

Contents

Chapter 1	1
Chapter 2	3
Chapter 3	8
Chapter 4	10
Chapter 5	12
Chapter 6	16
Chapter 7	19
Chapter 8	23
Chapter 9	26
Chapter 10	30
Chapter 11	33
Chapter 12	36
Chapter 13	45
Chapter 14	49
Chapter 15	54
Chapter 16	59
Chapter 17	62
Chapter 18	67
Chapter 19	73
Chapter 20	77
Chapter 21	84
Chapter 22	87
Chapter 23	90
Chapter 24	97
Chapter 25	101
Chapter 26	105
Chapter 27	111
Chapter 28	115
Chapter 29	120
Chapter 30	125

Solutions

Solutions to problems in Isaacs's *Algebra* book.

Chapter 1

- [1.1] Let G be a transitive Abelian permutation group. If it's not regular, then there's a point $x \in X$ with two distinct elements $g, h \in G$ with $xg = xh$. Then gh^{-1} fixes x . For any $y \in X$, let $k \in G$ be such that $xk = y$. Then

$$y(gh^{-1}) = xk(gh^{-1}) = x(gh^{-1})k = xk = y$$

where we've used that G is Abelian. Thus gh^{-1} fixes every point of X , and so is the identity: $g = h$. This contradiction shows G is regular.

- [1.2] We have to show each r_x and l_y is a bijection on G . But this is obvious, as

$$\begin{aligned} r_x^{-1} &= r_{x^{-1}} \\ l_y^{-1} &= l_{y^{-1}} \end{aligned}$$

Also, $(g)r_x r_y = (g)r_{xy}$ and $(g)l_x l_y = (g)l_{yx}$, so function composition is a binary operation for R and L , with inverses as noted above. Both r_1 and l_1 serve as the identity. Thus both R and L are permutation groups on the set G . The maps

$$\begin{aligned} x &\rightarrow r_x \rightarrow (1)r_x \\ y &\rightarrow l_{y^{-1}} \rightarrow [(1)l_{y^{-1}}]^{-1} \end{aligned}$$

give the required isomorphisms with G .

- [1.3] Let $l_y \in L$, and $r_x \in R$ and $g \in G$ be arbitrary. Then of course

$$(g)r_x l_y = ygx = (g)l_y r_x$$

Now let f be an arbitrary permutation of G that commutes with all R , and let $y = (1)f$. Then note that

$$(x)f = (1)r_x f = (1)fr_x = yx$$

and thus $f \equiv l_y$.

- [1.4]

(a) We work with the set $X = \{1, 2, 3\}$, and define $G = \{f, g\}$ where

$$\begin{aligned}(f(1), f(2), f(3)) &= (1, 1, 3) \\ (g(1), g(2), g(3)) &= (3, 3, 1)\end{aligned}$$

Then $f^2 = g^2 = f$, and $fg = g = gf$. So G is a group, but neither element is a permutation.

(b) Let $h \in G$ be an injective function. We want to show all elements of G are injective and surjective. If $e \in G$ is serving as the identity, then $he = h = eh$ and the fact that h is injective implies e is injective as well. But because $e^2 = e$, e must be surjective too: if $x \notin e(X)$, then from $e(x) \in e(X) = e^2(X)$, there's a $y \neq x$ with $y \in e(X)$ and $e(y) = e(x)$, contradicting injectivity. Finally, for any $g \in G$, we have $gg^{-1} = e = g^{-1}g$ and so each g must also be injective and surjective.

[1.5] Flipping, then rotating clockwise, is the same as rotating counterclockwise, then flipping. This is exactly the statement $trt = r^{-1}$, since $t = t^{-1}$. If n is odd, then $r^{-k} = tr^kt = r^k$ is impossible, since it implies $2k$ divides n . Likewise, tr^k can't be centralized by t , since that's equivalent to r^k being centralized by t . Thus no element of D_{2n} is centralized by t , so the group has trivial center.

[1.6] D_{24} has an element of order 6, as is easy to verify (thinking of it as the symmetries of a regular 12-gon). However, the rotation group of the cube has no element of order 6. Every rotation is through an axis, and that axis can go through a side or a diagonal. The former has order dividing 4, while the latter has order dividing 3.

[1.7] An element $g \in GL(n, q)$ takes a fixed basis to a basis, and it is uniquely determined (by linearity) by which basis. So if $\{e_i\}$ is the standard basis, then there are $(q^n - 1)$ choices for where to send e_1 [everything but 0]. $g(e_1)$ generates a subspace of order q , and to preserve linear independence, $g(e_2)$ cannot be in this subspace. Thus there are $q^n - q$ choices for where to send e_2 . Similar reasoning shows there are $q^n - q^i$ choices for where to send e_{i+1} , once $\{g(e_1), \dots, g(e_i)\}$ have been chosen. Thus the number of bases, and hence the number of elements of $GL(n, q)$, is given by

$$\prod_{i=0}^{n-1} (q^n - q^i)$$

[1.8] We have

$$\begin{aligned}(ab)^2 &= 1 \\ abab &= 1 \\ ab &= b^{-1}a^{-1} \\ ab &= ba\end{aligned}$$

Where the last line follows because b and a are involutions too.

[1.9] Here is the multiplication table:

	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

The above table shows we have an identity (1), as well as that composition is closed, and each element has an inverse (every row and column has a 1 in it). Associativity is a tedious check, but it works. Thus Q_8 is a group. The only nontrivial element that squares to the identity above is -1 , so it is the unique involution.

Chapter 2

[2.1] This is obvious if $H \leq K$ or $K \leq H$. But this has to be the case: otherwise, let $h \in H \setminus K$ and $k \in K \setminus H$. Then if $hk \in H$, we have $k \in H$; similarly if $hk \in K$. So $hk \notin H \cup K = G$, which is absurd.

[2.2] Choose the three elements x, y, xy . If x commutes with y we're done. If x commutes with xy , then $xy \in C_G(x)$, so that $y \in C_G(x)$, and x and y commute. Similarly if y commutes with xy . So in all cases, x commutes with y . Since there were arbitrary elements of G , it is an Abelian group.

[2.3]

(a) Because σ is an automorphism, we have

$$x^{-1}y^{-1} = \sigma(x)\sigma(y) = \sigma(xy) = y^{-1}x^{-1}$$

And this is equivalent to $xy = yx$, so G is Abelian.

(b) Consider the mapping $x \mapsto x^{-1}\sigma(x)$. This map is injective: otherwise,

$$\begin{aligned} x^{-1}\sigma(x) &= y^{-1}\sigma(y) \\ yx^{-1} &= \sigma(y)\sigma(x)^{-1} \\ &= \sigma(yx^{-1}) \end{aligned}$$

Since $\sigma(z) \neq z$ for all $z \neq 1$ in G , it must be that $y = x$. So we have an injective map on a finite group G , which is therefore surjective as well. Then for any $g \in G$, we can write it as $x^{-1}\sigma(x)$ for some $x \in G$, and we see that

$$\sigma(g) = \sigma(x^{-1}\sigma(x)) = \sigma(x)^{-1}x$$

Here we're using $\sigma^2 = 1$. This shows that $\sigma(g) = g^{-1}$, and so by part (a) G is Abelian.

[2.4] Take an element $g \neq 1$ in G , then we must have $\langle g \rangle = G$ since G is the only non-trivial subgroup. If g has order m , then for any prime p dividing m , $\langle g^p \rangle$ is a proper subgroup, so that $g^p = 1$ and G has order p .

[2.5] Take a $g \in G \setminus M$, so that $\langle g \rangle = G$. If g has order m , then for any prime p dividing m , we have that $\langle g^{m/p} \rangle$ is a subgroup of index p , hence maximal by Lagrange's theorem. Since there is only one maximal subgroup M , there is only one possibility for $[G : M]$, so there is only one prime dividing m .

[2.6] Let $g \in G \setminus H$. Then $\{H, gH\}$ are the left cosets, where gH contains all elements of G not in H . Similarly $\{H, Hg\}$ is the set of right cosets, and Hg contains all elements of $G \setminus H$. It must then be that $gH = Hg$ and so by theorem 2.25(iii) H is normal.

[2.7] If x is a non-generator for G , then for any maximal subgroup $M \leq G$, it must be that $\langle x, M \rangle \neq G$, since otherwise we would have $\langle M \rangle = G$, which is absurd. Since $M \leq \langle x, M \rangle \leq G$, we then have that $\langle x, M \rangle = M$ and $x \in M$. Since M was arbitrary, $x \in \Phi(G)$.

Conversely, let $x \in \Phi(G)$. Suppose S is a subset of G with $\langle x, S \rangle = G$, but $\langle S \rangle \neq G$. Then $\langle S \rangle \leq M$ for some maximal subgroup of M , which also contains x , so $\langle x, S \rangle \leq M \neq G$. This contradiction shows $\langle S \rangle = G$, and x is thus a non-generator.

[2.8]

- (a) Let T be a transversal for H in G . For every $s \in S$, define $t_s \in T$ as the element where $s \in Ht_s$, and replace each such t_s with s . This is still a transversal, since if s_1, s_2 both mapped to t_s , then $s_1s_2^{-1} \in H \cap K$, and because S is a transversal for $H \cap K$ in K , we would have $s_1 = s_2$.
- (b) If $T = S$ then $G \subset HS \subset HK$, so $G = HK$. Conversely, let $t \in T$ be given by $t = hk$. Then there's an $s \in S \subset T$ where $k = h^{-1}t \in (H \cap K)s$. Then $st^{-1} \in H$, and since T is a transversal, $t = s$. But t was arbitrary, so $T = S$.
- (c) This is a combination of the above two parts, since $[K : H \cap K] = |S|$ and $[G : H] = |T|$. Note we need $[G : H]$ finite, so that T (and thus S) are finite, allowing $|S| = |T|$ to imply $S = T$.
- (d) If $G = HK$ is finite, then from the previous part we have

$$\frac{|G|}{|H|} = \frac{|K|}{|H \cap K|}$$

and our desired formula holds by multiplying both sides of this by $|H|$.

[2.9] For $l \in L$ we have

$$Hl \subset K \iff l \in HK = K \iff l \in L \cap K$$

So $HL \cap K = H(L \cap K)$.

[2.10] Assume that $|H| \geq |K| \geq |L|$. Note that none of these three groups is contained in the other two, because of [2.1]. Suppose $[G : H] \geq 3$, so that $|H| \leq \frac{1}{3}|G|$. Then we would have

$$\begin{aligned} |G| &\leq |H| + |K| + |L| - 1 \\ &\leq \frac{|G|}{3} + \frac{|G|}{3} + \frac{|G|}{3} - 1 \\ &< |G| \end{aligned}$$

which is absurd. Here we are using that H is the biggest of the three subgroups. So we have $[G : H] = 2$. By [2.6] H is normal, and thus by Corollary 2.28 HK is a subgroup of G , with $H < HK \leq G$. Thus $G = HK$, and by part (c) of [2.8] we have $[K : H \cap K] = 2$, meaning $|K \setminus H| = \frac{1}{2}|K|$, and all of this holds for L as well. Then we have

$$\begin{aligned} |G| &\leq |H| + |K \setminus H| + |L \setminus H| \\ &= \frac{1}{2}|G| + \frac{1}{2}|K| + \frac{1}{2}|L| \\ |G| &\leq |K| + |L| \end{aligned}$$

And since $|L| \leq |K| \leq \frac{1}{2}|G|$, we must have equality throughout, so that

$$|L| = |K| = |H| = \frac{1}{2}|G|$$

[2.11] We have

$$\begin{aligned} [G : H \cap K] &= [G : H][H : H \cap K] \\ &= [G : K][K : H \cap K] \end{aligned}$$

By the gcd condition, we must have $[G : H]$ dividing $[K : H \cap K]$. By part (c) of [2.8] then, we must have $[G : H] = [K : H \cap K]$ so that $G = HK$.

[2.12]

(a)

$$[x, y][y, x] = x^{-1}y^{-1}xyy^{-1}x^{-1}yx = 1$$

(b)

$$\begin{aligned} [xy, g] &= y^{-1}x^1g^{-1}xyg \\ &= y^{-1}x^{-1}g^{-1}(xgyy^{-1}g^{-1}x^{-1})xyg \\ &= y^{-1}(x^{-1}g^{-1}xg)y(y^{-1}g^{-1}yg) \\ &= [x, g]^y[y, g] \end{aligned}$$

(c)

$$\begin{aligned} [x, y^{-1}, z]^y &= y^{-1}[y^{-1}, x]z^{-1}[x, y^{-1}]zy \\ &= x^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}zy \\ &= y^{-x}(xz)^{-1}yxz^y \end{aligned}$$

Writing all three of these out then we have

$$\begin{aligned} y^{-x}(xz)^{-1}yx[z^yz^{-y}](yx)^{-1}zy[x^zx^{-z}](zy)^{-1}xzy^x &= y^{-x}(xz)^{-1}[yx(yx)^{-1}][zy(zy)^{-1}]xzy^x \\ &= y^{-x}[(xz)^{-1}xz]y^x \\ &= y^{-x}y^x \\ &= 1 \end{aligned}$$

[2.13]

- (a) If $H \subset C_G(K)$, then for any $h \in H$ and $k \in K$, we have $[h, k] = 1$. Since these commutators generate $[H, K]$, we have $[H, K] = 1$. Conversely, if $[H, K] = 1$, then $[h, k] = 1$ for arbitrary h and k , again showing $H \subset C_G(K)$.
- (b) If $H \subset N_G(K)$, then for any $h \in H$ and $k \in K$, we have

$$[h, k] = k^{-h}k \in K$$

which shows $[H, K] \subset K$. Conversely, if $[H, K] \subset K$, then $k^{-h}k \in K$ for any $h \in H$ and $k \in K$, implying $k^h \in K$ and so $H \subset N_G(K)$.

- (c) By part (b), $[H, K] \subset H \cap K = 1$, and so by part (a) we have $H \subset C_G(K)$.

[2.14]

- (a) Since $[h, k] = [k, h]^{-1} \in [K, H]$ by [2.12] part (a), we have $[H, K] \subset [K, H]$. The same reasoning shows the reverse containment, so that $[H, K] = [K, H]$.
- (b) For $g, h \in H$ we have

$$[h, k]^g = [hg, k][g, k]^{-1} \in [H, K]$$

where the equality follows from [2.12] part (b). So the arbitrary $g \in N_G([H, K])$, and thus H normalizes $[H, K]$.

[2.15]

- (a) To see θ is well-defined, let $y \in Hx$, so that $y = hx$. Then

$$y^{-1}H = x^{-1}h^{-1}H = x^{-1}H$$

So θ is well-defined, and it has a well-defined inverse (by similar reasoning): $\theta^{-1}(zH) = Hz^{-1}$.

- (b) For this to be well-defined, for $y \in Hx$ we must have $x \in yH$, which implies $y \in xH$. Since y was arbitrary, we have $Hx \subset xH$, and the reverse containment follows from the well-definedness of ϕ^{-1} . So every left coset is a right coset, and by Theorem 2.25(iii) H is normal.

[2.16] Let $g \in G$ generate the quotient G/Z . Then every element of G belongs to some coset $g^n Z(G)$, so can be written as $g^n z$ with $z \in Z(G)$. But every element of this form is central, since it centralized by both $Z(G)$ and g . So G is Abelian.

[2.17] By Lagrange's theorem, the only subgroup orders are 1, 2, 4, and 8. The trivial subgroups are normal, and we shows in [1.9] that there is a unique subgroup of order 2, so that is normal. Every subgroup of order 4 has index 2, so by [2.6] it is also normal, and that covers all subgroups.

[2.18] Let $\{N_1, N_2, \dots, N_r\}$ be the normal π -subgroups of G , arranged by order: $|N_i| \leq |N_{i+1}|$. Note the cases of $r = 0$ and $r = 1$ are trivial. Then $N_i N_r$ is a normal subgroup of G by Corollary 2.31, and by [2.8] part (d) applied to $N_i N_r$, we have that $|N_i N_r|$ divides $|N_i| \cdot |N_r|$, which is a product of primes in π . In other words, $N_i N_r$ is a normal π -subgroup of G . By the choice of N_r we have

$$|N_r| \leq |N_i N_r| \leq |N_r|$$

so that $N_i N_r = N_r$. Since i was arbitrary, $N_i \leq N_r$ for all i , and N_r is the unique largest normal π -subgroup of G .

[2.19] As in the hint, taking $B = C$ in Theorem 2.11 gives $\phi(n)$ automorphisms of C with itself. If α and β are two automorphisms, with $C = \langle g \rangle$, then we have $\alpha(g) = g^a$ and $\alpha(g) = g^b$ for some integers a and b , and these completely determine the automorphism. Finally,

$$g^{\alpha\beta} = g^{ab} = g^{ba} = g^{\beta\alpha}$$

so $\alpha\beta = \beta\alpha$ and $\text{Aut}(C)$ is Abelian.

[2.20] Let C be cyclic of order n . Then for any divisor d of n , there is exactly one subgroup of order d in C , and it has $\phi(d)$ generators. Every element of C has order a divisor of n , so this gives a partition of C , and

$$n = |C| = \sum_{d|n} \phi(d)$$

[2.21] Because A is Abelian, $A \cap H \triangleleft A$, since all subgroups of A are normal. Because H normalizes both A and H , it also normalizes $A \cap H$. Thus both A and H are in $N_G(A \cap H)$, and then so is $G = AH$, meaning $A \cap H \triangleleft G$.

[2.22] Let $H = \{x + b \mid b \in \mathbb{Z}\}$, which is a subgroup (isomorphic to $\mathbb{Z}$). Let g be the element $x \mapsto 2x$. Then we have

$$g^{-1}Hg = \{x + 2b \mid b \in \mathbb{Z}\}$$

which is a proper subgroup of H (it misses $x \mapsto x + 1$ for example).

Chapter 3

[3.1] Define $\phi : G \rightarrow \text{Aut}(G)$ by $\phi(g)(x) = x^g$. This is a homomorphism, and the kernel is $Z(G)$. So we get the inner automorphisms are isomorphic to $G/Z(G)$. By [2.16], it's not possible for $G/Z(G)$ to be a nontrivial cyclic group.

[3.2] Suppose $G/Z(G) \cong Q_8$. Note that Q_8 has two cyclic subgroups of index 2, and hence by [2.16] G has two Abelian subgroups A and B of index 2, both of which are then normal. Their intersection $A \cap B = N$ is a normal subgroup of index 4 in G ; since it is centralized by both A and B and $G = AB$, we see that $N \leq Z(G)$, contradicting $[G : Z(G)] = 8$.

[3.3]

(a) Let K be the kernel of ϕ . Then

$$[\phi(G) : \phi(H)] = [G/K : H/(H \cap K)] = [G/K : HK/K] = [G : HK]$$

and since $[G : H] = [G : HK][HK : K]$, we have that $[\phi(G) : \phi(H)]$ divides $[G : H]$.

(b) $|\phi(H)| = [H : (H \cap K)]$ by the above, and this is a divisor of $|H|$.

[3.4]

(a) By part (a) of [3.3], we have that $[\phi(G) : \phi(H)]$ divides $[G : H]$, and thus is a π' number. By part (b) of the same exercise, $|\phi(H)|$ divides $|H|$, and so is a π number. Thus $\phi(H)$ is a Hall subgroup of $\phi(G)$.

(b) If $\phi(G)$ is a π group, then by part (a) $\phi(G) = \phi(H)$, so by the correspondence theorem $G = HN$. Conversely, if $G = HN$, then $\phi(G) = \phi(H)$, so again by part (a) $\phi(G)$ is a π group.

[3.5]

(a) Suppose N_1 and N_2 are normal subgroups of G such that G/N_i is a π group. Then $[G : N_1]$ and $[N_1N_2 : N_2]$ are π numbers, the latter because $N_1N_2/N_2 \leq G/N_2$. By the diamond theorem then

$$[G : (N_1 \cap N_2)] = [G : N_1][N_1 : N_1 \cap N_2] = [G : N_1][N_1N_2 : N_2]$$

is a π number, so $G/(N_1 \cap N_2)$ is a π group. By induction, if $\{N_i\}$ is the finite set of normal subgroups of G such that G/N_i is a π group, then $G/\cap N_i$ is also a π group, and clearly this normal subgroup is the smallest with that property.

(b) Let θ be a homomorphism to a π group. Since $\theta(G)$ is a π group, then $K = \ker(\theta)$ is a normal subgroup of G such that G/K is a π group. By part (a), we have $N \leq K$, so that

$$\theta \equiv \tau\bar{\theta}$$

where $\bar{\theta}$ is the canonical projection from G/N to $(G/N)/(K/N) \cong G/K$.

[3.6] To show this diagram is composed of two diamonds, we need to show $X = U \cap B$ and $A = UB$. For the first we have $X = U \cap V \subset A \cap V = B$, so that $X \subset U \cap B$. But $U \cap B \subset U \cap V = X$, so we have containment in both directions. For the second we already have $UB \subset A$; by Dedekind's lemma

$$A = UV \cap A = U(V \cap A) = UB$$

[3.7] We want to show $A \cap V = B$ and $A = UB$. If we show the first, we also get the second, since then

$$UB \subset A = UN \subset UB$$

To show the first, we have by Dedekind's lemma

$$A \cap V = NU \cap V = N(U \cap V) = NX = B$$

Here we use that N is normal to conclude that $\langle N, X \rangle = NX$.

[3.8] Let $K = \ker(\phi)$. Now if $g \in C_G(x)$, we have $[x, g] = 1$, and thus $[\phi(x), \phi(g)] = 1$, so that $\phi(C_G(x)) \subset C_H(\phi(x))$. If instead $\phi(g) \in C_H(\phi(x))$, then

$$[x, g] \in K \cap N = 1$$

so $g \in C_G(x)$, and we have containment in both directions: $C_G(x) = C_H(\phi(x))$.

[3.9] Define a homomorphism $\phi : N_G(H) \rightarrow \text{Aut}(H)$ by $\phi(g)(h) = h^g$. Then the kernel of this map is $C_G(H)$, so $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.

[3.10]

- (a) If G is metabelian, then there is $A \triangleleft G$ Abelian, with G/A Abelian as well. By Corollary 3.11, $G' \leq A$, and thus G' is Abelian, so that G'' is trivial. Conversely, if G'' is trivial, then G' is Abelian, and of course G/G' is always Abelian, so G is metabelian.
- (b) Suppose $A \triangleleft G$ makes G metabelian. Then G/AK , as a quotient of G/A , is Abelian, and $AK/K \cong A/(A \cap K)$ is Abelian as a quotient of A . Thus G/K is metabelian by the subgroup AK/K .
- (c) Since $H' \leq G'$ and thus $H'' \leq G'' = 1$, we have by part (a) that H is metabelian.

[3.11]

- (a) By [3.9], we have that $G/C_G(G'')$ is isomorphic to a subgroup of $\text{Aut}(G'')$, which by [2.19] is Abelian. Thus by Corollary 3.11, $G' \leq C_G(G'')$ and so $G'' \leq Z(G')$.
- (b) If G'/G'' is cyclic, then by part (a) and [2.16], G' is Abelian, so $G'' = 1$.

Chapter 4

[3.12] Let $\phi(x) = h$, and let $|x| = p^m d$, where d is relatively prime to p , and $|h|$ is a power of p . Then $\phi(x^d) = h^d$ is also a generator of $\langle h \rangle$, so choose r with $h^{dr} = h$. Now we have

$$\begin{aligned}\phi(x^{dr}) &= h \\ x^{dr} &\in \langle x^d \rangle\end{aligned}$$

Since $|x^d| = p^m$, we have that x^{dr} has p -power order.

[3.13] We work via induction of $|G|$, being trivial when G has order 1. Now if G has no proper nontrivial subgroups, then by [2.4] G has prime order, and any generator will have order p . Otherwise, let $1 < H < G$ be a proper nontrivial (normal) subgroup. Since $|G| = |H|[G : H]$, at least one of H and G/H has order divisible by p .

If H has order divisible by p , then by induction it has an element of order p , and thus so does G . If G/H has order divisible by p , then by induction it has an element of order p , and then by the previous problem G has an element of p -power order, which then also implies G has an element of order p .

[3.14] We work via induction on $|G|$, being trivial when G has order 1 or when $m = 1$. Let p be a prime dividing m , then by the previous problem, G has an element $h \in G$ of order p ; let $H = \langle h \rangle$. Since m/p divides $|G/H|$, by induction G/H has a subgroup M/H of order m/p . By the correspondence theorem, $M \leq G$ has order m .

Chapter 4

[4.1] Let $\mathcal{O}$ be the orbits of G_α on Ω , and let $\mathcal{P}$ be the orbits of G on $\Omega \times \Omega$. Define a map $\sigma : \mathcal{O} \rightarrow \mathcal{P}$ by

$$\sigma([\beta]) = [(\alpha, \beta)]$$

To see this is well-defined, note that if $\gamma = \beta g$ for $g \in G_\alpha$, then $(\alpha, \beta)g = (\alpha, \gamma)$. This is injective, since if there exists $x \in G$ with $(\alpha, \beta)x = (\alpha, \gamma)$, then $x \in G_\alpha$ so $[\beta] = [\gamma]$. Finally, it is surjective: for any (γ, δ) , choose $x \in G$ with $\gamma x = \alpha$. Then

$$\sigma([\delta x]) = [(\alpha, \delta x)] = [(\alpha x^{-1}, \delta)] = [(\gamma, \delta)]$$

[4.2] Let n be the number of orbits of G on $\Omega \times \Omega$. Note that the number of elements $g \in G$ fixes is equal to $\chi(g)^2$, since there are $\chi(g)$ choices for each of the two coordinates. By Cauchy-Frobenius then,

$$n = \frac{1}{|G|} \sum \chi(g)^2$$

If that sum is 2, then G is doubly transitive, because G has at least one orbit contained in the diagonal $\Delta = \{(\alpha, \alpha) : \alpha \in \Omega\}$, since $(\alpha, \alpha)g = (\alpha g, \alpha g) \in \Delta$. So if $n = 2$, then G

acts transitively on Δ (so transitively on Ω), and then also transitively on $\Omega \times \Omega \setminus \Delta$, as desired.

- [4.3] We let K act on the right cosets of H in G . Now HgK is the orbit of K acting on the element Hg . Since H^g is the stabilizer of Hg , we see this orbit has $[K : (K \cap H^g)]$ elements, each of size $|Hg| = |H|$, so we get

$$|HgK| = \frac{|H||K|}{|K \cap H^g|}$$

- [4.4] Let $C = \phi^{-1}(C_H(\phi(g)))$. Then $g \in C$ and $K = \ker(\phi) \leq C$. Now the conjugacy class of g in C is contained in Kg , because $\phi(c^{-1}gc) = \phi(g)$, since $\phi(c) \in C_H(\phi(g))$. Since the conjugacy class of g in C is bounded by $|K|$, we then have that

$$|C_G(g)| \geq |C_G(g) \cap C| = |C_C(g)| \geq [C : K] = |C_H(\phi(g))|$$

- [4.5] There are $|G|^2$ different pairs of elements from G . Fixing a first coordinate g , there are precisely $|C_G(g)|$ choices for the second coordinate so that the pair commutes. Then the probability is

$$\frac{1}{|G|^2} \sum_{g \in G} |C_G(g)| = \frac{1}{|G|} \left(\frac{1}{|G|} \sum_{g \in G} |C_G(g)| \right) = \frac{k}{|G|}$$

where we've used the Cauchy-Frobenius formula for k .

- [4.6] We let S_4 act on the cube by orientation-preserving isometries. Let the side of the cube facing us be called A , the back be called B , and the four other sides C_1 through C_4 . First consider rotation by a quarter turn through the axis formed by A and B , call that map σ . So we have an order 4 subgroup $\{1, \sigma, \sigma^2, \sigma^3\}$. The number of colorings fixed by these is $\{n^6, n^3, n^4, n^3\}$. Now consider a rotation that takes C_i to A , the side facing us. We can compose that rotation with each of the σ^j , and we see the number of fixed colorings is $\{n^3, n^2, n^3, n^2\}$. Finally consider the half turn that takes B to A , and then composing with a σ^j . The number of colorings fixed is $\{n^4, n^3, n^4, n^3\}$. By the Cauchy-Frobenius formula then, the number of distinct colorings is

$$\frac{n^6 + 3n^4 + 12n^3 + 8n^2}{24}$$

- [4.7] We let the cyclic group $C = \langle \sigma \rangle$ of order r act on the necklace by rotations. For every d dividing r , rotation by $\sigma^{r/d}$ divides the beads into $\frac{r}{d}$ orbits, so there are $n^{r/d}$ fixed colorings for that rotation, and this is true for any such element of order d in C . By the Cauchy-Frobenius formula then, together with the decomposition of a cyclic group based on element order, the number of distinct necklaces is

$$\frac{1}{r} \sum_{d|r} \phi(d) n^{r/d}$$

[4.8] If we consider coloring each element of Ω with one of x colors, then by the Cauchy-Frobenius formula, $f_{G,\Omega}(x)$ is the number of distinct colorings up to the action of G . This is clearly an integer. Note that a polynomial that takes integer values on infinitely many inputs must itself have integer coefficients, and so the **NOTE** of the problem is also true.

[4.9] Let G be a counterexample of minimal possible order. Then for any $g \notin Z(G)$, we must have that $|C_G(g)|$ is not divisible by p , otherwise by the minimality of $|G|$ we would have an element of order p in $C_G(g)$. Thus the conjugacy class of g must have order divisible by p . Since $|G| \equiv 0 \pmod{p}$, the class equation shows $|Z(G)| \equiv 0 \pmod{p}$ as well. Since $Z(G)$ is Abelian, [3.13] shows $Z(G)$ has an element of order p then, and this contradiction shows no counterexample exists.

Chapter 5

[5.1] Let $T \leq N$ be a Sylow p -subgroup of N , then $T \leq P$ for some Sylow subgroup P of G . But $P = S^g$ for some $g \in G$, so that by normality of N ,

$$T = P \cap N = S^g \cap N = S^g \cap N^g = (S \cap N)^g$$

Thus $S \cap N$ is itself a Sylow subgroup of N .

[5.2]

- (a) By [3.3], $\phi(P)$ is a p -subgroup of H , and $[H : \phi(P)]$ is not divisible by p , so $\phi(P)$ is a Sylow subgroup.
- (b) Let $L = \phi^{-1}(Q)$, so that $[G : L]$ is not divisible by p . Let P be a Sylow subgroup of L , which is then a Sylow subgroup of G as well. By part (a), $\phi(P)$ is a Sylow subgroup of H , contained in Q , so we have $\phi(P) = Q$.
- (c) The previous two parts show that ϕ is a surjective map from the Sylow p -subgroups of G to those of H .

[5.3] Let $P \leq H$ be a Sylow subgroup of H . Then there's a Sylow subgroup $S \leq G$ with

$$S \cap H = P$$

By picking such an S for each P , we get an injective map from the Sylow p -subgroups of H to those of G .

[5.4] Let $P \leq H$ be a Sylow p -subgroup of H , and choose a Sylow subgroup S of G such that $S \cap H = P$. Let $x \in Z(S)$ be non-trivial.. Then for $y \in P$ nontrivial, we have $x \in C_G(y) \subset H$, so that $S \subset C_G(x) \subset H$, and thus $S = P$. So for every prime p dividing $|H|$, we have that p does not divide $[G : H]$, and thus $|H|$ and $[G : H]$ are relatively prime.

[5.5] Let P be a Sylow p -subgroup of H , and S a Sylow p -subgroup of G with $S \cap H = P$. If

$P \neq S$, then $P < N_S(P) \leq N_G(P) \leq H$, and since $N_S(P)$ is a p -group, this contradicts P being a Sylow subgroup of H . So $P = S$.

[5.6] If p divides $|G|$, then let Ω be the set of Sylow p -subgroups of G . P acts on Ω , so that

$$|\Omega^P| \equiv |\Omega| \equiv 1 \pmod{p}$$

and thus there's a fixed Sylow subgroup Q .

If p does not divide $|G|$, then let q be any prime that does, and let Ω be the set of Sylow q -subgroups. Because $|\Omega|$ divides $|G|$, we have

$$|\Omega^P| \equiv |\Omega| \not\equiv 0 \pmod{p}$$

so there's a fixed Sylow q -subgroup Q .

[5.7] Suppose G doesn't have a normal Sylow p -subgroup. Then $n_p > p$ and divides q^2 , so since $q < p$ it must be that $n_p = q^2$. But we also have $q^2 = n_p \equiv 1 \pmod{p}$, so that p divides $q^2 - 1 = (q - 1)(q + 1)$. Again since $q < p$ this implies $p = q + 1$, and thus $\{p, q\} = \{3, 2\}$.

[5.8] Let $N = N_G(P)$, and suppose $g \in G$ normalized N . Then P^g is a Sylow p -subgroup of N , and hence $P^g = P$; this is exactly the condition that $g \in N$. Thus $N_G(N) = N$.

[5.9] We know the case of $|G| = p^3$ and $|G| = p^2q$ already (Corollary 5.22 and Theorem 5.27). So we can assume $p > q > r$ are distinct primes. Assume G is simple, then $n_p > p$ must divide qr , and since both q and r are smaller than p , we have $n_p = qr$. There are thus $qr(p - 1)$ elements of order p in G . Since $n_q > 1$ and $q > r$, there are at least r Sylow q -subgroups. That gives at least $r(q - 1)$ elements of order q in G , leaving at most

$$pqr - qr(p - 1) - r(q - 1) - 1 = r - 1$$

elements of order r , and that means there is only one Sylow r -subgroup, which is normal. This is the contradiction, and so G cannot be simple.

[5.10] We can remove all groups whose order has the form p^m , $p^a q$, and pqr (by Corollary 5.22, Theorem 5.27, and the previous problem). This leaves the following possible orders for a simple group:

- $|G| = 36$. There must be 4 Sylow 3-subgroups, and then Lemma 5.16 shows 36 would need to divide $4! = 24$, which is absurd.
- $|G| = 60$. This case is allowed by the problem (and we'll see A_5 is order 60 and simple).
- $|G| = 72$. There must be 4 Sylow 3-subgroups, and then Lemma 5.16 shows 72 would need to divide $4! = 24$, which is absurd.

- $|G| = 84$. The only possibility for $n_7 \equiv 1 \pmod{7}$ to divide 12 is $n_7 = 1$, so G isn't simple.
- $|G| = 90$. Since $n_5 \equiv 1 \pmod{5}$ needs to divide 18, it must be that $n_5 = 6$. This gives $6(5 - 1) = 24$ elements of order 5. Similarly $n_3 = 10$, and so there must be two Sylow 3-subgroups P and Q that intersect non-trivially (otherwise there would be $80 > 90 - 24$ elements of order 3 or 9). If $H = P \cap Q$, then $|H| = 3$ and its normalizer contains both P and Q , so has order at least

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = 27$$

Since $|N_G(H)|$ divides 90 and is divisible by 9, we have $|N_G(H)| = 45$ or 90. In the first case, $N_G(H)$ is normal in G ; in the second, H is normal in G . In both cases, G is not simple.

- $|G| = 100$. Isn't simple by [5.7].

[5.11] We show G has a subgroup of index 5, so that the right action on the cosets of that subgroup gives an injective homomorphism $G \rightarrow S_5$. This shows G is unique up to isomorphism, since any such subgroup of S_5 is normal, and if there are two (say G and H), then $G \cap H$ would be a nontrivial normal subgroup of the simple group G .

Now $n_2 \in \{3, 5, 15\}$. $n_2 = 3$ is ruled out by Lemma 5.16. If $n_2 = 5$, then the normalizer of a Sylow 2-subgroup is our subgroup of index 5. If $n_2 = 15$, then since $15 \not\equiv 1 \pmod{4}$, there are Sylow 2-subgroups P and Q with $|P \cap Q| = 2$, by Theorem 5.11. Since both P and Q are in $N_G(P \cap Q)$, we see that

$$|N_G(P \cap Q)| \geq \frac{|P| \cdot |Q|}{|P \cap Q|} = 8$$

and since $|N_G(P \cap Q)|$ divides G and is divisible by 4, we must have $|N_G(P \cap Q)| \geq 12$. However, this is the largest size it can have in G by Lemma 5.16. Thus $N_G(P \cap Q)$ is our subgroup of index 5.

[5.12] Suppose G is simple, so that $n_7 = 8$. If P is a Sylow 7-subgroup, then $N_G(P)$ has order 35. If Q is a Sylow 5-subgroup contained in $N_G(P)$, then it is normal there by Sylow's theorems. Thus 35 divides $|N_G(Q)|$, so that 8 divides n_5 . The only possibility is then $n_5 = 1$, so that Q is normal, and G is not simple.

[5.13] Clearly G as a set has order pq . We now show these maps are permutations on P , and that G is non-Abelian. First we have that

$$\phi(a, \sigma)^{-1} = \phi(a^{-1}, \sigma^{-1})$$

and of course $\phi(1, 1)$ is the identity, so that $G \subset S_P$. Now if $(xa)\sigma = (x\hat{a})\hat{\sigma}$ for all $x \in P$, we want to show $a = \hat{a}$ and $\sigma = \hat{\sigma}$. If $x = a^{-1}$, then we have

$$1 = (a^{-1}\hat{a})\hat{\sigma}$$

so that $a = \hat{a}$. Then since xa runs through P as x runs through P , we also have $\sigma \equiv \hat{\sigma}$.

Finally, note that if ι is the inversion map, then

$$(1)\phi(a, 1)\phi(1, \iota) = a^{-1} \neq a = (1)\phi(1, \iota)\phi(a, 1)$$

as long as $a \neq a^{-1}$, which we can do by taking a to generate P .

[5.14] If $n_p = 1$, then of course a subgroup of order p is normal. So suppose $n_p = p + 1$, the only other option. Then there are $(p + 1)(p - 1) = p^2 - 1$ elements of order p , so there are p elements of order not 1 or p . Let x be such an element. Since $x \notin C_G(P) \leq N_G(P) = P$, we know that $P \cap C_G(x) = \{1\}$, so that x has at least p conjugates. But there are only p elements that could have the same order as x , so that $|C_G(x)| = p + 1$. Since no element of order p is in $C_G(x)$, it must be exactly those elements not of order p in G , and that is clearly normal.

[5.15] Let $Q \leq P$, where P is a Sylow p -subgroup of G , which is a T.I. set by assumption (being a T.I. set is clearly invariant under conjugation, so it's fine if this P isn't the same P as in the problem). Suppose that

$$Q^h \cap Q \neq Q$$

for $h \in H$. Then $P^h \neq P$, so that

$$Q^h \cap Q \subset P^h \cap P = 1$$

[5.16] Let $\Omega = \{g \in G : g^p = 1\}$, and let S be a Sylow p -subgroup of G . S acts on Ω via conjugation, and so by the fundamental counting lemma

$$|\Omega| \equiv |\Omega^S| \pmod{p}$$

Now we have

$$\Omega^S = \Omega \cap C_G(S) = \{x \in Z(S) : x^p = 1\}$$

This last equality happens because if $x \in \Omega \cap C_G(S)$, then $\langle x, S \rangle$ is a p -subgroup of G , hence we must have $x \in S$. This shows that Ω^S is a subgroup of S , and it is non-trivial by Cauchy's theorem, since S (and hence $Z(S)$) is non-trivial. We thus have that $|\Omega| \equiv 0 \pmod{p}$, as desired.

[5.17] Suppose $S \leq G$ is not normal, and there is a maximal subgroup $S \leq M < G$; we can choose M so that it also contains $N_G(S) < G$. Let $r = [M : N_G(S)]$ and $s = [G : M]$. We have

$$r \equiv rs \equiv 1 \pmod{p}$$

and we know $s > 1$. If $r > 1$, then as in the hint, $[G : N_G(S)] = rs \geq (p + 1)^2 > kp + 1$, which is a contradiction. So $r = 1$ and $M = N_G(S)$. Now let $t = [M : S]$, so that

$$st = kp + 1 \equiv 1 \pmod{p}$$

Just as before then, since $s > 1$, we must have $t = 1$, so that $M = S$, and S is maximal.

[5.18] Since $Z(P) \neq 1$, the only possibility is $Z(P) = P$ (so P is Abelian) or $[P : Z(P)] = p$. But then by [2.16] P is also Abelian.

[5.19]

(a) We have $P \leq C_G(Z(P))$. For any Sylow q -subgroup Q of G with $q \neq p$, we have $Q \cap Z(P) = \{1\}$, and since both are normal, we also have $Q \leq C_G(Z(P))$. This implies $|G|$ divides $|C_G(Z(P))|$, so that $Z(P)$ is central in G .

(b) Let p be a prime dividing $|N|$. Then since G has a unique Sylow p -subgroup, we must have $N \cap P \triangleleft P$ non-trivial. By Theorem 5.21 $N \cap Z(P) \leq N \cap Z(G)$ is also non-trivial, the containment following from part (a).

[5.20] Let $C = C_P(A)$, and suppose that $C > A$, so that C/A is a non-trivial normal subgroup of P/A . By Theorem 5.21, this implies $C/A \cap Z(P/A)$ is non-trivial. Taking an element of order p in the intersection, the correspondence theorem gives a normal subgroup $B > A$ with $[B : A] = p$. Since $A \leq Z(C)$, [2.16] shows B is Abelian. This then contradicts the maximality of A , and so it must be that $C = A$.

Chapter 6

[6.1] Suppose x normalizes P and fixes two points $a \neq b$ in an orbit of P . Let $g \in P$ be such that $g(a) = b$, and note that g generates P . Also note that g is the only element of P that sends a to b ; otherwise, if $h \in P$ did the same, then $h^{-1}g$ would fix a , and if $h \neq g$ then it would generate P , showing a is fixed by P . This contradiction shows g is unique, and thus $g^x = g$, so that x centralizes $\langle g \rangle = P$.

[6.2] Suppose G is simple of order 760. By Sylow's theorems, G has 20 Sylow 19-subgroups. The action of G on these Sylow subgroups gives an embedding of G into A_{20} . Let P be a Sylow 19-subgroup and $g \in N_G(P)$ an element of order 2 (since $|N_G(P)| = 38$). If g centralized P , then G would have an element of order 38, which does not exist in S_{20} . So g fixes at least one point (corresponding to P), and by the previous problem g can fix at most one point in the orbits of P . But P has two orbits: it fixes itself, and permutes the remaining 19 Sylow subgroups. Thus g fixes exactly 2 points, and is the product of 9 transpositions, which means $g \notin A_{20}$. This contradiction shows G doesn't exist.

[6.3] The conjugacy class of x is smaller precisely when $C_G(x) \leq A_n$, with $G = S_n$. To see this, we know $|x^G| = [G : C_G(x)]$, and we also know $[C_G(x) : C_G(x) \cap A_n] \leq 2$. Since $[G : A_n] = 2$ the conjugacy class is smaller precisely when

$$C_G(x) = C_G(x) \cap A_n$$

Now suppose that $C_G(x) \leq A_n$. Then the cycle decomposition for x cannot have any even cycles, since such an even cycle c is not contained in A_n , but centralizes x . If there are two cycles of odd length k in the cycle decomposition of x , then there is a product σ of k transpositions that interchanges them, and hence centralizes x . Since $\sigma \notin A_n$, it must be that $s(k) \leq 1$.

Conversely, if the cycle decomposition of x has the desired structure function, then let g centralize x . Then g must send each cycle to itself. If c is a k -cycle, then g leaves the orbit of c invariant, and so its restriction to the orbit of c gives some of the cycle decomposition of g . Since g centralizes c , by [6.7] its restriction must be a power of c . Since this works for all cycles in the decomposition of x , g is a product of powers of cycles comprising x . Since each cycle is even by hypothesis, $g \in A_n$; since g was arbitrary, we see $C_G(x) \leq A_n$.

By the above, the classes that split in A_{10} are $1 \cdot 9$ and $3 \cdot 7$.

[6.4] We have

$$(1, 2, \dots, n)^{-k}(1, 2)(1, 2, \dots, n)^k = (k+1, k+2)$$

so by Lemma 6.16 we are done.

[6.5] Let $x = (1, 2, \dots, m)$ and $y = (1, 2, \dots, n)$. We show that $[x, y] = (2, 1, m+1)$. To that end, let $2 < i \leq m$ and $m+1 < j \leq n$. Using $[x, y] = x^{-1}y^{-1}xy$ we have

$$\begin{array}{ccccccc} 1 \mapsto & m \mapsto & m-1 \mapsto & m \mapsto & m+1 \\ 2 \mapsto & 1 \mapsto & n \mapsto & n \mapsto & 1 \\ m+1 \mapsto & m+1 \mapsto & m \mapsto & 1 \mapsto & 2 \\ i \mapsto & i-1 \mapsto & i-2 \mapsto & i-1 \mapsto & i \\ j \mapsto & j \mapsto & j-1 \mapsto & j-1 \mapsto & j \end{array}$$

[6.6] Use x and y as in the previous problem, and let $G = \langle x, y \rangle$. Consider disjoint subsets $\{B_1, \dots, B_k\}$ partitioning $\{1, \dots, n\}$ and such that G permutes these B_i . Since G is transitive, all B_i must have the same size, and let B be the one containing 1. We suppose $a \in B$ with $a \neq 1$, and show $B = \{1, \dots, n\}$, which implies G is primitive.

If $a > m$, then $(a)x = a$, and since then $a \in B \cap Bx$, we must have $B = Bx$. Since $(1)x = 2$, we must have $2 \in B \cap By$, so that $B = By$. Since y is transitive, we have $B = \{1, \dots, n\}$.

If $1 < a \leq m$, Then $(a)x^{-1}y = a$, and so as above $B = Bx^{-1}y$. Since $(1)x^{-1}y = m+1$, we have $m+1 \in B$, and we are in the same situation as the previous paragraph. So in all cases, G is primitive.

As noted after the problem, Jordan's theorem implies $G = A_n$ or $G = S_n$. We have $G \leq A_n$ precisely when $x, y \in A_n$, which happens precisely when both m and n are odd.

[6.7] There are $(n - 1)!$ ways to cyclically order n elements, and thus a has this many conjugates; hence

$$|C_G(a)| = \frac{n!}{(n - 1)!} = n$$

Since $a \in C_G(a)$ and $|a| = n$, we are done.

[6.8] We induct on $|T|$, the case T is empty being obvious. Suppose we know that $G = \langle T \rangle$ has at most $n - |T|$ orbits, and let $\tau = (a, b)$ be another transposition. If a and b are in the same G orbit, then $\langle T, \tau \rangle$ has the same orbits as G . If a and b are in different G orbits, then τ fuses them so that $\langle T, \tau \rangle$ has one less orbit than G . This completes the inductive step.

[6.9] Let $T = \{t_1, \dots, t_k\}$ as a set, so there are no duplicates, with $|T| = r$. By the previous problem, there are at least $n - r$ orbits of $G = \langle T \rangle$. Since $g \in G$, we know there are at most $n - m + 1$ orbits, so that

$$\begin{aligned} n - r &\leq n - m + 1 \\ m - 1 &\leq r \end{aligned}$$

[6.10] Let G act on G via right multiplication, and let g be a generator of a Sylow 2-subgroup of G , with order 2^k . If $|G| = 2^k m$ with m odd, then g has m orbits of length 2^k in this action, and so is an odd permutation. So if $\rho : G \rightarrow S_G$ is the regular representation, then $H = \rho^{-1}(A_G)$ is an index 2 subgroup of G .

Note that H is normal in G , and also has cyclic Sylow 2-subgroups (since subgroups of cyclic groups are cyclic). By induction on k , H has a characteristic subgroup K of order m . Since K consists precisely of the elements of odd order in G , it is also characteristic in G .

[6.11] Let G act on the cosets of M . If $Mxt = Mx$, then $xtx^{-1} \in M$, contradicting the problem statement. Thus t fixes no coset, and hence acts as a product of $[G : H]$ transpositions. It is thus acting as an odd permutation, and as in the previous problem, G has a normal subgroup of order 2.

[6.12] Let $s = (a, b)$, and choose k such that $g^k = (a, b, \dots)$. Relabing $a \mapsto 1, b \mapsto 2$, etc., we have by [6.4] that

$$S_p = \langle s, g^k \rangle = \langle s, g \rangle$$

This last equality relies on p being prime.

[6.13] If $n < 3$, then A_n is trivial. When $n = 3$, $|A_n| = 3$ so is of course Abelian. Suppose $\sigma \in Z(A_n)$ for $n > 3$, and suppose $(a)\sigma = b$ with $a \neq b$. If c, d are distinct elements besides a and b , then we have

$$\begin{aligned} (b)\sigma^{(a,b,c)} &= c \\ (b)\sigma^{(a,b,d)} &= d \end{aligned}$$

Since $\sigma^{(a,b,c)} = \sigma^{(a,b,d)} = \sigma$, we have a contradiction. So $Z(A_n)$ is trivial.

Chapter 7

[7.1] Let N be a normal subgroup of $G = U \times V$. Since $\pi_1(N) \leq U$ is a normal subgroup, if the image is nontrivial, then $\pi_1(N) = U$, so that $NV = G$. If $N \cap U$ is trivial, then $N \leq C_G(U) = V$, which is a contradiction. Since U is simple, we must have $N \cap U = U$. Similar reasoning shows what happens with $\pi_2(N)$ and V . We thus have three possible normal subgroups: U , V , and G . If both $\pi_1(N)$ and $\pi_2(N)$ are trivial, then of course N is trivial as well.

[7.2] If $\phi : M \rightarrow N$ is an isomorphism, then

$$D = \{(g, \phi(g)) : g \in M\}$$

is a diagonal subgroup. Conversely, if a diagonal subgroup D exists, then we have

$$M \cong G/N \cong DN/N \cong D/(N \cap D) \cong D \cong D/(M \cap D) \cong DM/M \cong G/M \cong N$$

[7.3] Let $\phi_i : G \rightarrow G/M_i$ be the canonical homomorphism. Then

$$\prod \phi_i : G \rightarrow \prod G/M_i$$

is a homomorphism, whose kernel is $D = \cap M_i$.

[7.4] Let $\{N_i\}$ be all the normal subgroups such that $G/N_i \in \mathcal{X}$, and let $N = \cap N_i$. By (iii) $\prod G/N_i$ is in $\mathcal{X}$, and by (i-ii) and the previous problem $G/N \in \mathcal{X}$. Clearly N is the unique minimal such normal subgroup.

[7.5]

(a) Choose a maximal subset R of the M_i such that their product K is a direct product. If $M \in \{M_i\} \setminus R$, then we cannot have $M \cap K$ trivial, since by Theorem 7.5 MK would be a direct product, contradicting maximality of R . Since M is a minimal normal subgroup, we must have $M \cap K = M$. Since M was arbitrary, we see that $N \leq K$, and of course $K \leq N$, so that $N = K$ is a direct product.

(b) Part (a) shows N is a direct product of some subset R of the M_i . If $M \notin R$, then for every factor N_j of N , by minimality we have $N_j \cap M = \{1\}$. Thus M is central in N , contradicting the fact it is nonabelian. So no such M exists.

[7.6] By the previous problem, the socle is a direct product of some subset of minimal normal subgroups. By Theorem 7.8 each of these factors is a direct product of simple groups, so that by Lemma 7.11 the socle is a direct product of simple groups.

[7.7] Suppose $D < L$ for some subgroup L of G . Then

$$L = DN \cap L = D(N \cap L)$$

shows that $L \cap N$ is non-trivial, and since M centralizes N , we see that both L and M normalize $L \cap N$, so that $G = LM$ normalizes $L \cap N$. Since N is simple, $L \cap N = N$. Similarly, $L \cap M = M$, so that $L = G$.

[7.8] Let $\phi : U/M \rightarrow V/N$ be an isomorphism, with $\alpha : U \rightarrow U/M$ and $\beta : V \rightarrow V/N$ the canonical homomorphisms. Define $G \subset U \times V$ as

$$G = \{(u, v) : \phi\alpha(u) = \beta(v)\}$$

Of course $(1, 1) \in G$, and if (a, b) and (c, d) are in G , then from

$$\phi\alpha(a^{-1}c) = \phi\alpha(a^{-1})\phi\alpha(c) = \beta(b^{-1})\beta(d) = \beta(b^{-1}d)$$

we have that $(a, b)^{-1}(c, d) \in G$, so that G is a subgroup.

Now define $M_0 = G \cap U$ and $N_0 = G \cap V$, so that clearly $M_0 \cap N_0$ is trivial. From the definition of G , we have

$$M_0 = M \times \{1\}$$

$$N_0 = \{1\} \times N$$

So clearly $M_0 \cong M$ and $N_0 \cong N$. Finally define the map $\psi : G \rightarrow U/M$ via

$$\psi(u, v) = \alpha(u)$$

This is a surjective map, since for any $u \in U$ we know that $\beta^{-1}\phi\alpha(u)$ is non-empty. The kernel is precisely those elements (u, v) with $u \in M$. This implies $\beta(v) = 1$, so that $v \in N$. In particular, the kernel is $M \times N = M_0N_0$, as desired.

[7.9] Let $\phi : M \rightarrow N$ be an isomorphism. Let $H = U \times V$ and define a normal subgroup $R \triangleleft H$ by

$$R = \{(u, v) : \phi(u) = v\}$$

Since ϕ is a homomorphism, R is a subgroup; it's normal since it's central. We will let

$$G = H/R$$

$$K = UR/R$$

$$L = VR/R$$

Obviously K and L are normal in G , with $KL = G$. Since ϕ is an isomorphism, we have $R \cap U = R \cap V = \{1\}$, so that $K \cong U$ and $L \cong V$.

Now note that $UR = U \times N$ and similarly $VR = M \times V$. Since M and N are central, we have $[UR, VR] = \{1\}$, so the same is true for $[K, L]$. Finally, $UR \cap VR = M \times N$. Define a map $\psi : M \times N \rightarrow N$ by

$$\psi(m, n) = \phi(m)n^{-1}$$

Since M and N are Abelian, this is a homomorphism, and is clearly surjective. The kernel is precisely R , so we have

$$K \cap L = (UR \cap VR)/R \cong N \cong M$$

[7.10] Write $G_1 \cong G$ as the normal subgroup of the semidirect product, and $G_2 \cong G$ as the complement acting via conjugation on G_1 . Let

$$H = \{(g, g^{-1}) : g \in G\} \subset G_1 \rtimes G_2$$

We have $(1, 1) \in H$, and also

$$(g, g^{-1})(x, x^{-1}) = (gxg, g^{-1}x^{-1}) = (xg, (xg)^{-1}) \in H$$

Finally, $(g, g^{-1})^{-1} = (g^{-1}, g) \in H$, so H is a subgroup. We also have

$$\begin{aligned} (x, y)^{-1}(g, g^{-1})(x, y) &= (x^{-y}, y^{-1})(g, g^{-1})(x, y) \\ &= (x^{-y}g^y, (gy)^{-1})(x, y) \\ &= (x^{-y}g^y x^{gy}, g^{-y}) \\ &= (g^y, g^{-y}) \end{aligned}$$

Thus $H \triangleleft G_1 \rtimes G_2$. The above calculation also shows that G_1 (where $y = 1$) centralizes H , and of course $G_1 \cap H$ is trivial. Since

$$(g, x) = (gx, 1)(x^{-1}, x) \in G_1 H$$

we have that $G_1 \rtimes G_2 = G_1 \times H$. To finish, the map $\psi : H \rightarrow G$ sending $(g, g^{-1}) \mapsto g^{-1}$ is an isomorphism, by the product calculation in H above.

[7.11] If $P = Z(P) \rtimes Q$, Then $Z(Q)$ is centralized by both Q and $Z(P)$, hence is central in P ; in other words, $Z(Q) \leq Z(P) \cap Q$, which only makes sense if $Z(Q) = 1$, so that Q is trivial and P is Abelian.

[7.12]

- (a) Since $G = NH$, it's enough to show that for $n \in N$ nontrivial, $H \cap H^n$ is trivial. Suppose that $h \in H \cap H^n$. Then from $n h n^{-1} \in H$ we have that $n^h \in Hn$; since $n^h \in N$, this implies $n^h = n$, so that (since $n \neq 1$) $h = 1$.
- (b) We know from part (a) that $H^n \cap H^k = \{1\}$ for $n \neq k \in N$. This implies $N_G(H) = H$ and so there are $|N|$ conjugates, all intersecting trivially. That implies that

$$\left| \bigcup_{n \in N} H^n \right| = |N| \cdot |H| - (|N| - 1)$$

Since $H^n \cap N = (H \cap N)^n = \{1\}$, we then have that

$$N \cup \bigcup_{n \in N} H^n = G$$

by counting elements.

[7.13] We assume $G \neq \{1\}$ and thus via [5.6] we know there's a Sylow q -subgroup $Q \leq G$ fixed by the action of P . Since $QP > P$, maximality implies $G = Q$. Since P fixes the characteristic subgroup $Z(Q) \neq \{1\}$, again maximality shows $Q = Z(Q)$, so that G is an Abelian q -group.

[7.14] Let $g \in G \setminus A$, and let m be the least integer with $g^m \in A$. Choose $a_g \in A$ with $a_g^m = g^m$, so that ga_g^{-1} has order m , and

$$\langle ga_g^{-1} \rangle \cap A = \{1\}$$

If we pick $\{g_1, \dots, g_n\}$ to represent the cyclic factors of the finite Abelian group G/A , then the above shows $U = \langle g_1 a_{g_1}^{-1}, \dots, g_n a_{g_n}^{-1} \rangle$ is a subgroup isomorphic to G/A and trivially intersecting A , so that $G = A \times U$.

[7.15]

(a) Let $G = A \times B$, and suppose $(ab)^n = a^n b^n \in A$. This implies $b^n = 1$, so that

$$a^n = (ab)^n$$

and thus A is pure.

(b) Let $g^n \in U$. By hypothesis, there's a $u \in U$ with $u^n g^{-n} = (ug^{-1})^n \in A$. Since A is pure, there's $a \in A$ with $a^n = (ug^{-1})^n$. Thus

$$(ua^{-1})^n = u^n a^{-n} = g^n$$

so that U is pure (since $A \leq U$).

(c) The proof of [7.14] only relied on A being pure, so works here too.

[7.16] The key fact is that for $e \geq 1$, we have

$$g(e) - g(e-1) = |\{e_i \mid e_i \geq e\}|$$

To prove this, note that

$$g(e) = \sum_i \min(e_i, e)$$

since if $(g_1, \dots, g_n)^{p^e} = 1$, then $g_i^{p^e} = 1$ for each i ; that holds for every element in $Z_{p^{e_i}}$ if $e_i \leq e$, and holds for exactly p^e elements in $Z_{p^{e_i}}$ if $e_i \geq e$. Thus

$$g(e) - g(e-1) = \sum_i \min(e_i, e) - \min(e_i, e-1)$$

and the only terms that contribute a non-zero entry are when $e_i \geq e$, in which case it contributes exactly 1. We then have

$$\begin{aligned} (g(e) - g(e-1)) - (g(e+1) - g(e)) &= |\{e_i \mid e+1 > e_i \geq e\}| \\ &= f(e) \end{aligned}$$

[7.17] Define $\phi_i : Z_m \rightarrow Z_{m_i}$ by sending a generator to a generator, say g to g_i . We then have

$$\prod \phi_i : Z_m \rightarrow \prod Z_{m_i}$$

The kernel of this map consists of elements g^k such that $k \equiv 0 \pmod{m_i}$ for all m_i . By the relatively prime assumption, this implies m divides k , so that $g^k = 1$. Thus our product map is injective, and order considerations show it is in fact an isomorphism.

Chapter 8

[8.1] Suppose $M \leq G$ with $H \triangleleft M$. By the Frattini argument,

$$M = N_G(P)H = H$$

with the last equality following since $N_G(P) \leq H$.

[8.2]

(a) Since N is not contained in M , $M < MN$ so that $G = MN$. Since G is solvable, N is Abelian, and thus $M \cap N$ is normalized by both M and N , hence $M \cap N \triangleleft G$. Minimality implies $M \cap N = \{1\}$.

(b) Note that for $m \in M$ we have

$$C_M(N)^m = C_M(N^m) = C_M(N)$$

Since N centralizes $C_M(N)$, we have $C_M(N) \triangleleft G$. Since M is core-free, $C_M(N)$ is trivial.

(c) N is Abelian, so $N \leq C_G(N)$. But if $mn \in C_G(N)$, then $m \in C_M(N)$, which is trivial by part (b). So $C_G(N) = N$.

(d) If K is another minimal normal subgroup, then $K \cap N$ is trivial, so that $K \leq C_G(N) = N$, and thus K cannot exist.

[8.3] If G is nilpotent, then it is a product of Sylow subgroups:

$$G = \prod Q_p$$

for primes p dividing $|G|$. So if $|x|$ and $|y|$ are coprime, then we can write

$$\begin{aligned} x &= \prod x_p \\ y &= \prod y_p \end{aligned}$$

where if $x_p \neq 1$ then $y_p = 1$ and vice versa. This is true since otherwise p divides both $|x|$ and $|y|$. Thus x and y commute factorwise.

Conversely, let x be an element of a Sylow p -subgroup P of G . If $y \in Q$ for a Sylow q -subgroup of G (with $p \neq q$), then $y \in C_G(x)$. This is true for all $y \in Q$ and $x \in P$, so that $Q \leq C_G(P) \leq N_G(P)$. Since obviously $P \leq N_G(P)$, order considerations show $N_G(P) = G$. This is true for any Sylow subgroup, so G is nilpotent.

- [8.4] If M and N are normal solvable subgroups of G , then $N \triangleleft MN$ is solvable, while $MN/N \cong M/(M \cap N)$ is solvable as a quotient of M , so MN is solvable as well. Thus by induction, the product of all normal solvable subgroups of G is the largest normal solvable subgroup.
- [8.5] Note that $\phi(G)$ is solvable, and hence $\phi(G)/\phi(N)$ is solvable. As an image of G/N , it is perfect as well by Lemma 8.2. Thus $\phi(G)/\phi(N)$ is trivial, so $\phi(G) = \phi(N)$.
- [8.6] $G/Z(G)$ is solvable and nontrivial; let $N/Z(G)$ be a minimal normal subgroup of $G/Z(G)$. Then $N/Z(G)$ is an elementary Abelian p -group, so it has a nontrivial center $C/Z(G)$, which is nilpotent, since $C/Z(G)$ is a quotient of $C/Z(G)$ and is thus Abelian. Hence $C \leq F(G)$ and since $C \neq Z(G)$ we have the strict inequality we want.
- [8.7] Note that $H = C_G(F(G)) \triangleleft G$. If it's Abelian, then of course $H \leq F(G)$. If it's non-Abelian, then the previous problem shows $Z(H) < F(H)$. Since $F(H)$ is normal and nilpotent, we then have

$$H \cap F(G) \leq Z(H) < F(H) \leq H \cap F(G) \quad (1)$$

The strict inequality is thus a contradiction, and H must be Abelian (and in particular $H \leq F(G)$).

- [8.8] Let $U \leq H$ be a Sylow p -subgroup of H , and let $S \leq G$ be a Sylow p -subgroup of G containing U . Similarly define $V \leq K$ and $T \leq G$. We can write $S^g = T$, with $g = hk$. Then S^h contains $U^h \leq H$ and $V^{k^{-1}} \leq K$. Thus by Lemma 8.22 we have

$$S^h = U^h V^{k^{-1}}$$

- [8.9] We prove this by induction on $|G|$. If $N \leq \Phi(G)$, then G is nilpotent by Theorem 8.24, so we can take $H = G$. If N is not contained in $\Phi(G)$, then there's a maximal subgroup $M \leq G$ not containing N , so that $G = MN$. By induction, since $M/(M \cap N)$ is nilpotent, there's a nilpotent subgroup $H \leq M$ with

$$M = H(N \cap M) = HN \cap M$$

with the last equality following by Dedekind's lemma. We then have $M, N \leq HN$, so $G = HN$.

- [8.10] Let G be a finite nilpotent group. Then we can write

$$1 = Z_0 < Z_1 < \cdots < Z_n = G$$

where Z_{i+1}/Z_i is central in G/Z_i . Thus every subgroup of Z_{i+1}/Z_i is normal in G/Z_i ; since each Z_{i+1}/Z_i is a finite Abelian group, we can refine this series to

$$1 = Z_0 < N_{1,1} < N_{1,2} < \cdots < Z_1 < N_{2,1} < \cdots < Z_2 < \cdots < Z_n = G$$

where the factors are finite cyclic. This means G is supersolvable.

[8.11] Write

$$1 = N_0 < N_1 < \cdots < G$$

for a normal series of G with cyclic factors. Choose the largest i with $N_i \leq M$; let $L = N_i$ and $K = N_{i+1}$. Then $L \leq M$, $MK = G$, and K/L is cyclic. We now work in G/L , writing $\hat{S}$ for the image of S in G/L . First we have that $\hat{M} \cap \hat{K}$ is a maximal subgroup of $\hat{K}$: if $\hat{M} \cap \hat{K} < \hat{H} \leq \hat{K}$, by Dedekind's lemma we would have

$$\hat{H} = \hat{H}(\hat{M} \cap \hat{K}) = \hat{H}\hat{M} \cap \hat{K} = \hat{K}$$

where the last equality happens because $\hat{H}\hat{M}$ is a subgroup of $\hat{G}$ properly containing $\hat{M}$, and thus is all of $\hat{G}$. [It's a subgroup because all subgroups of $\hat{K}$ are characteristic, hence normal in $\hat{G}$.] Since $\hat{K}$ is cyclic, a maximal subgroup must have prime index p . We then have

$$[G : M] = [\hat{G} : \hat{M}] = [\hat{M}\hat{K} : \hat{M}] = [\hat{K} : \hat{M} \cap \hat{K}] = p$$

[8.12]

- (a) Let P be a Sylow p -subgroup of G . If P is not normal, then let $N_G(P) \leq M \leq G$ for M a maximal subgroup. Then $[G : M] = q$ for some prime q , and

$$1 \equiv [G : N_G(P)] = [G : M][M : N_G(P)] \equiv q \cdot 1 \pmod{p}$$

This is a contradiction since $q < p$, thus P is normal in G .

- (b) We can prove this by induction on $|G|$. From part (a), there's a normal Sylow subgroup $P \triangleleft G$; since the maximal subgroups of G/P come from the maximal subgroups of G containing P , by induction G/P is solvable. Since P is nilpotent (hence solvable), G is solvable too.

[8.13] For $x, y \in H$ and $z \in K$ we have by [2.12]

$$[x, z]^y = [xy, z][y, z]^{-1}$$

which proves that H normalizes $[H, K]$. Since $[h, k]^{-1} = [k, h]$, a similar argument shows K normalizes $[H, K]$, and thus $\langle H, K \rangle$ normalizes (and contains) $[H, K]$.

[8.14] As in the hint, $\Gamma = G \rtimes H$ is such that $K \triangleleft \Gamma$ and thus $H \leq C_\Gamma(K) \triangleleft \Gamma$. So $[g, h] = h^{-g}h \in C_\Gamma(K)$, while since $H \leq N_\Gamma(G)$, we also have $[g, h] \in G$. Thus

$$[G, H] \leq G \cap C_\Gamma(K) = C_G(K) \leq K$$

We then have that $[H, G, H] = [G, H, H] \leq [K, H] = 1$, so by the Three Subgroups lemma $[H, H, G] = 1$. Since H acts faithfully, we must have $[H, H] = 1$, so that H is Abelian.

[8.15] Since G is nilpotent, we must have $[N, G, \dots, G] \leq [G, G, \dots, G] = 1$ for some number k of G on the right. Choose $k > 0$ to be minimal so that $[N, G, \dots, G] = 1$, and let $R = [N, G, \dots, G]$ with $k-1$ G . Then $R \neq \{1\}$ and $R \leq N$ since N is normal. But $[R, G] = 1$ so that $R \leq Z(G)$ as well, and we're done.

[8.16] Write

$$1 = N_0 < N_1 < \dots < N_n = G$$

for a normal series of G with cyclic factors, and let M be a minimal normal subgroup of G . We proceed by induction on n , the case $n = 0$ being trivial. If $M \leq N_1$, then of course M is cyclic since N_1 is cyclic. If M is not contained in N_1 , then $M \cap N_1 = \{1\}$ and then $M \cong MN_1/N_1$ is a normal subgroup of G/N_1 . If we can show this is a minimal normal subgroup, then by induction M is cyclic.

By the Correspondence theorem, we need to show if $K \triangleleft G$ with $N_1 \leq K \leq MN_1$, then $K = N_1$ or $K = MN_1$. Since $MK = MN_1$, by Dedekind's lemma we can show

$$K = N_1 M \cap K = N_1 (M \cap K)$$

If $N_1 < K$ then this implies $M \cap K > \{1\}$ so by minimality of M we have $M \cap K = M$ and so $K = MN_1$.

[8.17] Let E be a finite elementary Abelian p -group. Then $\Phi(E) = \{0\}$. To see this, let $E = C_p^n$ and let $x \neq 0$ be an element with $x_i \neq 0$. Then $M_i = \{y \in E : y_i = 0\}$ is a subgroup of index p in E , hence maximal, and it does not contain x .

Now let $\{M_1, \dots, M_m\}$ be the maximal subgroups of P . Then $M_j \triangleleft P$ is normal, and P/M_j is cyclic of order p . By [7.3], $P/\Phi(P)$ is isomorphic to a subgroup of $\prod (P/M_i)$, and hence is an elementary Abelian p -group. If $N \leq \Phi(P)$ is normal in P , and P/N is elementary Abelian, then by the first paragraph

$$\Phi(P)/N = (\cap M_i)/N = \cap (M_i/N) = \{1\}$$

so that $N = \Phi(P)$.

Chapter 9

[9.1] By Burnside's Transfer Theorem, we have $G = K \rtimes P$ for a complement K . Since P is central, it is normal as well, so that G is actually the direct product $K \times P$.

[9.2]

- (a) Let $x \in G$, $a \in A$, and ν be the transfer map. Let T be a transversal for A in G . $S = T^x$ is also a transversal for $A^x = A$, and since A is normal, $t^{-1}at \in A$ for all $t \in T$. Then we have

$$\nu(a)^x = \prod_{t \in T} (t^{-1}at)^x = \prod_{s \in S} s^{-1}a^x s = \nu(a^x) = \nu(a)^{\nu(x)} = \nu(a)$$

where the last equality relies on A being Abelian. So $\nu(a) \in Z(G)$.

- (b) The condition implies A is a Hall subgroup. From [3.4] we have $\nu(G) = \nu(A)$, and from part (a) we have $\nu(A) \leq A \cap Z(G)$. Meanwhile, if $a \in A \cap Z(G)$, choose integers m, n with

$$mo(a) + n[G : A] = 1$$

which is possible since $o(a)$ divides $|A|$ so is coprime to $[G : A]$. Then

$$\nu(a^n) = a^{n[G:A]} = a^{1-mo(a)} = a$$

so we have $A \cap Z(G) \leq \nu(A)$.

- (c) We know from part (b) that $\nu(G) = A \cap Z(G) \triangleleft G$, and of course $\ker(\nu) \triangleleft G$. For $a \in A \cap Z(G)$ we have $\nu(a) = a^{[G:A]} \neq 1$, so that $\nu(G) \cap \ker(\nu) = \{1\}$. Since we of course have $[G : \ker(\nu)] = \nu(G)$, we have shown $G = \nu(G) \times \ker(\nu)$.

[9.3] As in the hint, first assume $P \triangleleft G$. Then we are in the case of part (b) of the previous problem, so we can write $G = \nu(P) \times \ker(\nu)$. Let $P = \langle x \rangle$, and write $x = (a, b)$ with $a \in \nu(P) \leq P$ and $b \in \ker(\nu)$. Since $x, a \in P$ we must have $b \in P$, and thus

$$x = x^r x^s$$

with $x^r \in \nu(P)$ and $x^s \in \ker(\nu)$. We cannot have p dividing both r and s , so in particular either $P \leq \nu(P)$ or $P \leq \ker(\nu)$. Since by assumption

$$1 < G' \cap P \leq \ker(\nu) \cap P$$

we must have $P \leq \ker(\nu)$, which is contained in G' by the Focal Subgroup theorem. Thus p cannot divide $[G : G']$.

In the general case, we have $P \triangleleft N_G(P)$. From Corollary 9.15, we have $1 < P \cap N'_G(P)$. So by the previous paragraph we must have $P \leq N'_G(P) \leq G'$ as well.

[9.4] This problem is not true. Let $K = C_4 \times C_4$, and let $A \leq \text{GL}(2, 4)$ be a non-Abelian group of automorphisms of K of order 6. The semidirect product $G = K \rtimes A$ is a counterexample. Specifically, let $K = \langle u, v \rangle$ and $A = \langle x, y \rangle$ with

$$x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

In this case $P = \langle x, K \rangle$ is a Sylow 2-subgroup, and $N_G(P) = P$. We also have

$$\begin{aligned} G' &= \langle y, K \rangle \\ P' &= \langle uv^{-1} \rangle \\ Z(P) &= \langle uv \rangle \end{aligned}$$

Now $z = uv \in P \cap Z(N) = Z(P)$, but $z \notin P'$. However, $z \in K \leq G'$.

- [9.5] Suppose $P = Q \times C$ was a Sylow 2-subgroup of the finite simple group G . Consider the transfer map $\nu : G \rightarrow P/P'$. Now P has three elements x, y, xy of order 2, with $x \in Q$ and $y \in C$. All three are in $Z(P)$, so by Burnside's Lemma their fusion is controlled in $N_G(P)$. But x is the only involution in $Z(P) \cap P' \triangleleft N_G(P)$, so x is not conjugate to either y or xy . Let T be a transversal for P in G ; by the Transfer Evaluation Lemma, choose $T_0 \subset T$ for y , so that we have

$$\nu(y) = \prod_{t \in T_0} t^{-1} y^{n_t} t \pmod{P'}$$

But $x \in P'$, so that $y \equiv xy \pmod{P'}$, and we must have $t^{-1} y^{n_t} t \in \{1, y, xy\}$. Since $\sum n_t = [G : P]$ is odd, there are an odd number of $n_t = 1$. Thus we have

$$\nu(y) = y \pmod{P'}$$

But $y \notin P'$, so that $y \notin \ker(\nu)$, and this implies G/G' is non-trivial, contradicting that G is simple.

- [9.6] As in the hint, let M be a maximal subgroup of G and let P and Q be nontrivial Sylow subgroups of M for the primes p and q . Now M is nilpotent, so $P, Q \triangleleft M$. Since $P \cap Q = \{1\}$, we have $P \leq C_G(Q)$. So if $x, y \in P$ are conjugate in G , they are conjugate in $N_G(Q)$ by Burnside's Transfer Lemma. Since G is simple, we must have $N_G(Q) \leq M$, since otherwise $M < N_G(Q)$ and we'd have $Q \triangleleft G$. Thus x and y are conjugate in M . We then have

$$\text{Foc}_G(P) = \text{Foc}_M(P) = P \cap M' = P' < P$$

This means the transfer map $G \rightarrow P/P'$ is not trivial, contradicting G being simple. Thus M must be a p -group.

- [9.7] Suppose $M^g = N$. Then both P and P^g are contained in $N_G(N)$, so there's an element $n \in N_G(N)$ with $P^{g^n} = P$. Thus $gn \in N_G(P)$ and $M^{g^n} = N^n = N$.

- [9.8] Write Z for $Z(P)$. Suppose $Z^g \leq P$. Then $Z \triangleleft P^{g^{-1}}$ by hypothesis, so $Z^g \triangleleft P$. By the previous exercise, Z and Z^g are conjugate in $N_G(P)$. But $Z \triangleleft N_G(P)$ so $Z^g = Z$.

[9.9]

- (a) Let $x^g = y$. Then both W and W^g are contained in $C_G(y)$, and in particular both are contained in Sylow p -subgroups of $C_G(y)$. Choose $c \in C_G(y)$ such that W^{g^c} and W are contained in the same Sylow subgroup of $C_G(y)$, and hence contained in the same

Sylow subgroup Q of G . Finally, choose $h \in G$ with $Q^h = P$. Since W is weakly closed, we have

$$W^{gch} = W^h = W$$

so that $W^{g^c} = W$, and $gc \in N_G(W)$, with $x^{g^c} = y^c = y$.

(b) From part (a) we have

$$G' \cap P = \text{Foc}_G(P) = \text{Foc}_N(P) = N' \cap P$$

[9.10] Let P be of class at most 2, and note this means $P' \leq Z(P) \leq P$, so that every subgroup of P containing $Z = Z(P)$ is normal in P . Suppose Q is another Sylow p -subgroup containing Z , and let $M = P \cap Q$. From what was just said, $P \leq N_G(M)$; meanwhile, normalizers grow in Q , so $P < N_G(M)$ and thus $M \triangleleft G$, contradicting simplicity of G . Thus Z is only contained in P . Since $P = N_G(Z)$ by simplicity and maximality, we have by [9.8] and [9.9]

$$\text{Foc}_G(P) = P'$$

This shows the transfer map $G \rightarrow P/P'$ is non-trivial, contradicting simplicity. Thus P must be class at least 3.

[9.11] As in the hint, let T be a transversal for H in G , let

$$Y = \{tx(t \cdot x)^{-1}\}$$

for a finite set X with $G = \langle X \rangle$, and define $K = \langle Y \rangle$, so that K is finitely generated and contained in H . We show T is also a transversal for K in G , implying (since $K \leq H$) that $K = H$, as desired.

Let $x \in X$ and $t \in T$, and note that

$$Ktx = K(t \cdot x)$$

from the definition of Y . Thus $\{Kt : t \in T\}$ is invariant under x , and hence under $G = \langle X \rangle$. Since G acts transitively on the right cosets of K , these must be all of them.

[9.12] Let $[G : Z(G)] = m$. Then the transfer map $g \mapsto g^m$ is a homomorphism into the Abelian group $Z(G)$, and hence G' is in the kernel: every $h \in G'$ is such that $h^m = 1$. Let T be a transversal for $Z(G)$ in G . Then we compute for $x, y \in Z(G)$ and $s, t \in T$

$$[xs, yt] = [x, yt]^s [s, yt] = [x, t]^s [x, y]^{ts} [s, t] [s, y]^t = [s, t]$$

since all commutators involving an element of $Z(G)$ are trivial. Thus $G' = \langle [s, t] : s, t \in T \rangle$ is a finitely generated group (since T is finite). Since $[G' : G' \cap Z(G)] \leq [G : Z(G)]$, by the previous problem $G' \cap Z(G)$ is a finitely generated Abelian group where every element has order dividing m . This means $G' \cap Z(G)$ is finite, and hence G' is finite.

[9.13]

- (a) Suppose x and y are conjugate in G , with $x^g = y$. Then $y \in H \cap H^g$, so either $y = 1$ or $g \in H$. Thus no two non-trivial elements of H are conjugate in G , unless they're conjugate in H already, so there's no fusion.
- (b) If $x \neq 1 \in H$ and $x^g = x$, then $x \in H \cap H^g$, so $g \in H$. Thus $C_G(x) \leq H$, and [5.4] shows H is a Hall subgroup.
- (c) From parts (a) and (b), the Focal Subgroup Theorem shows $\nu(H) \leq \nu(G)$ is nontrivial, where $\nu : G \rightarrow H/H'$ is the transfer map. Since $\nu(G)$ is an image of G/G' , and H/H' is a π -group, we must have some prime in π dividing $[G : G']$.
- (d) Let $N = O^\pi(G)$, the minimal normal subgroup such that G/N is a π -group. [3.4] already shows that $G = HN$, so we just need to show $H \cap N$ is trivial. But if $n \in N$ is such that

$$(N \cap H) \cap (N \cap H)^n = N \cap H \cap H^n \neq \{1\}$$

then since H is a Frobenius complement in G , we must have $n \in H$. So $H \cap N$ is a Frobenius complement in N . If $H \cap N$ is non-trivial, then solvability of H and part (c) shows $[N : N']$ is divisible by some prime in π . Then $O^\pi(N) < N$ while $O^\pi(N) \triangleleft G$, contradicting the minimality of N . Hence $H \cap N$ is trivial as desired.

Chapter 10

- [10.1] For any endomorphism ϕ of G , we have $\phi([a, b]) = [\phi(a), \phi(b)]$. Thus $\phi(G') \subset G'$, and so for any set X of endomorphisms we have G' is an X -subgroup.
- [10.2] Let $u \in D_8$ be a non-central involution. Then with $g \in D_8$ and $C_2 = \langle c \rangle$, define the endomorphism x as

$$\begin{aligned} g^x &= g \\ (gc)^x &= g^x u \end{aligned}$$

Since $c \in Z(G)$, but $c^x = u \notin Z(G)$, $Z(G)$ is not an X -subgroup.

- [10.3] If there exists an X -composition series for G with Abelian factors, each subgroup of the series is normal in G , and hence G is solvable by definition. Note that there is an X -composition series since G is of finite length.

Conversely, suppose G is solvable. We proceed by induction on the derived length of G , the case of $G = \{1\}$ being trivial. By [10.1] G' is a normal X -subgroup of G , so there is an X -composition series containing G' as a member. All factors above G' are Abelian. By induction, all factors below G' are Abelian as well. By the Jordan-Holder theorem, every X -composition series then for G has Abelian factors.

- [10.4] Let N_1 and N_2 be two normal subgroups of G such that G/N_i is an S -group. If $K/N_i \triangleleft$

G/N_i , then Corollary 10.4 and the Jordan-Holder theorem shows both K/N_i and G/K is an S -group. Define $N = N_1 \cap N_2$, and note

$$(G/N)/(N_1/N) \cong G/N_1$$

$$N_1/N \cong N_1N_2/N_2$$

Thus both the groups on the left are S -groups, since the groups on the right are. By Corollary 10.4 (applied to N_1/N) and Jordan-Holder again, G/N is an S -group as well. Inductively, if we define N as the intersection of all such N_i (there are finitely many), then G/N is still an S -group, so N is clearly the unique minimal such normal subgroup.

Now if both N_1 and N_2 are S -groups, then as before, from

$$N_1N_2/N_2 \cong N_1/(N_1 \cap N_2)$$

we have that the group on the left is an S -group, since the one on the right is. Then again by Corollary 10.4 and the Jordan-Holder theorem, N_1N_2 is an S -group. Just as above, inductively if we define N as the product of all such N_i , then N is an S -group, and is clearly the unique maximal such normal subgroup.

[10.5] Let $1 = G_0 < G_1 < \cdots < G_k < G$ be a chief series for G , such that every factor is either a p -group or a p' -group, as in (i). Since G_r/G_{r-1} is a p -group or a p' -group, all (normal) subgroups are also p -groups or p' -groups. A composition series for G_r/G_{r-1} is then as in (ii). Piecing these together (using Corollary 10.4), we have a composition series for G where each factor is a p -group or p' -group, so (i) implies (ii).

Conversely, let $1 = G_0 < G_1 < \cdots < G_k < G$ be a composition series as in (ii). Let $\mathcal{P}$ be the set of all finite simple groups that are p -groups (there is only one), and let $\mathcal{P}'$ be the set of all finite simple groups that are p' -groups. As in the previous exercise, let N_p be smallest normal subgroup such that G/N_p is a $\mathcal{P}$ -group, and $N_{p'}$ the smallest normal subgroup such that $G/N_{p'}$ is a $\mathcal{P}'$ -group. Since G/G_k is either a simple p -group or simple p' -group, we have either N_p or $N_{p'}$ is a proper normal subgroup of G (contained in G_k). Write N_k for this characteristic subgroup. By Corollary 10.4 and Jordan-Holder, N_k has a composition series as in (ii). Thus the same reasoning constructs a characteristic subgroup $N_{k-1} < N_k$, which is then normal in G . Continuing this way, we eventually reach a normal series

$$1 = N_0 < N_1 < \cdots < N_k < G$$

where each factor is either a p -group or a p' -group. Now with $X = G$ acting by conjugation, inductively refine this to a chief series by considering $N_r/N_{r-1} \triangleleft G/N_{r-1}$ and using Corollary 10.4. Just as in the previous paragraph, the factors of this X -composition series (which is just a chief series for G) are subquotients of the factors N_r/N_{r-1} , and hence are all p -groups or p' -groups. Thus (ii) implies (i).

[10.6] If G is solvable, then it has a composition series where each factor is simple and Abelian, hence cyclic of prime order. Thus condition (ii) from the previous exercise is satisfied for all primes p . Now suppose condition (ii) is satisfied for all primes, and consider a

composition series for G . No factor can have order divisible by two different primes p and q , since then G is not p -solvable (nor q -solvable). Thus each factor is a simple p -group, hence cyclic of prime order. Thus all factors are Abelian and G is solvable.

[10.7] This is just the Jordan-Holder theorem when $X = G$ is acting by conjugation. For any two chief series, the factors are X -isomorphic, and a factor is central precisely when X acts trivially on it.

[10.8] If G has a normal p -complement N , build a chief series containing N . Then all the factors below N are p' -groups, and the factors above N give a chief series for G/N , a p -group. Since minimal normal subgroups of p -groups are central, all the factors above N are central.

Now assume G does not have a normal p -complement, and choose $N \triangleleft G$ maximal such that $H = G/N$ does not have a p -complement. Let K be a minimal normal subgroup of H . We must have $|K|$ divisible by p , since otherwise a normal p -complement in H/K corresponds to a normal p -complement in H . Assume K is central, so that by minimality $|K| = p$. Let P be any p -subgroup of H , and let $g \in N_H(P)$ be such that $o(g)$ is coprime to p . Then in H/K , gK centralizes PK/K by Frobenius's theorem. For every $x \in P$ then, we have

$$x^g = xk$$

for some $k \in K$. Since k is central, repeated application shows $x^{g^i} = xk^i$, and thus g^p centralizes x . Since $o(g)$ is coprime to p , this means $g \in C_H(x)$. Since x was arbitrary, $g \in C_H(P)$. Thus $N_H(P)/C_H(P)$ is a p -group, so again by Frobenius's theorem, H has a normal p -complement. This contradiction shows K is not central in H .

Thus if $1 < \cdots < N < K < \cdots < G$ is a chief series for G containing N , then K/N has order divisible by p , but is not central.

[10.9] Write $N = \prod_{j=1}^b N_j$ and $M = \prod_{k=1}^a M_k$ for indecomposable X -groups, and we proceed by induction on $a + b$. Via factor replacement on N_1 we have that

$$G = H_1 \times \prod_{j=2}^b N_j \times \prod_{k=1}^a M_k$$

where we've renumbered the H_i so that the factor we pull out is H_1 . Now we have

$$L := \prod_{j=2}^b N_j \times \prod_{k=1}^a M_k = C_G(H_1) = \prod_{i=2}^n H_i$$

where the last equality follows as in the problem's hint. From the above equality we also have that H_1 and N_1 centralize L . We have an isomorphism $N_1 \rightarrow G/L \cong H_1$ given by projection. Let $n \in N_1$ map to $h \in H_1$ under this map. If $n \neq h$, then $nh^{-1} \in L$ and it centralizes L , so that $nh^{-1} \in Z(G) = 1$. So we must have $n = h$, and thus $N_1 \leq H_1$. Since the isomorphism is surjective, we actually have $N_1 = H_1$. Replacing G by L , by induction on $a + b$ we see that M and N are products of the H_i .

Chapter 11

[11.1] Note that the poset of subgroups of G/G' , via the correspondence theorem, also satisfies both chain conditions. Thus G/G' is an Abelian group that is both Noetherian and Artinian. By Theorem 11.3 then, G/G' has finite composition length. Since the only simple Abelian groups are finite, this implies G/G' is finite. By induction on the derived length of G , G' is finite as well (note that the poset of subgroups of G' is a subset of the poset for G), so that G is finite.

[11.2]

- (a) If X is an initial segment of L , then we can write $X = L^a$ for some $a \in L$. Then if $x \in X$ and $y \notin X$, then

$$y \geq a > x$$

So X is a cut.

- (b) Suppose every proper cut is an initial segment, and let $P \subset L$ be any nonempty subset. Define

$$X = \bigcap_{a \in P} L^a$$

By part (a) this is an intersection of cuts, hence a cut. Since $X \cap P = \emptyset$, we see that X is proper, so by hypothesis, $X = L^b$ for some $b \in L$. If $a \in P$ is such that $a < b$, then $a \in X$, and in particular, $a \in L^a$, which is absurd. Thus $b \leq a$ for all $a \in P$. But if $b \notin P$, then by definition $b \in X = L^b$, which is also absurd. Thus $b \in P$ and $b \leq a$ for all $a \in P$, so P has a minimal element.

Conversely, assume L is well-ordered, and let X be a proper cut. Then $L \setminus X$ is nonempty, so has a minimal element a . Then $X \subset L^a$, but if $y < a$, then $y \notin L \setminus X$, so $y \in X$, and so we have $X = L^a$ as desired.

[11.3] Let $\mathcal{L}$ be the poset of all linearly ordered subsets of P , ordered by containment. Then the union of any chain in $\mathcal{L}$ is also a linearly ordered subset of P , so we can apply Zorn's lemma to $\mathcal{L}$ to get a maximal linearly ordered subset of P .

[11.4] Suppose P is linearly ordered, and let A be an antichain with $a, b \in A$. Then we have either $a \leq b$ or $b \leq a$, so $a = b$, and A has at most one element.

Now suppose every antichain has at most one element. If $x, y \in P$ are incomparable, then $\{x, y\}$ is an antichain. Thus x must be comparable to y , so P is linearly ordered.

[11.5] Let P be the set of all finite intersections of maximal X -subgroups of M . Since M is Artinian, there is a minimal element of P , say $K = K_1 \cap \cdots \cap K_n$. It must be the case this intersection is $\{0\}$; if not, by hypothesis there would be a maximal X -subgroup L not containing K , and then $K \cap L$ would be a smaller finite intersection.

So $\cap K_i = \{0\}$, and we have M/K_i is simple for each K_i . By Corollary 11.13 then, M is completely reducible.

[11.6] Let $A \leq M$ be an X -subgroup of M isomorphic to S . Then $\phi(A)$, as a quotient of A , is either $\{0\}$ or isomorphic to A . Either way, $\phi(A)$ is contained in the S -isotypic component of N . Since A was arbitrary, this shows the S -isotypic component of M is mapped into the S -isotypic component of N .

[11.7] We must assume S is finite ($\mathbb{Q}$ as a vector space over itself is an infinite counterexample). Then let p be a prime dividing $|S|$. Then the set of elements of order p in S is nonempty (Cauchy's theorem), and is X -invariant (since it's invariant under any endomorphism of S). Thus the subgroup consisting of elements with order dividing p is a non-trivial X -subgroup of S , and so is all of S .

[11.8] Assume G is not finitely generated. Let $\mathcal{S}$ be the set of all subgroups $H \leq G$ such that $\langle H \cup Y \rangle \neq G$ for all finite subsets $Y \subset G$. By assumption, $\{1\} \in \mathcal{S}$, so it is non-empty. Let $\{H_\alpha\} \subset \mathcal{S}$ be a linearly ordered subset of $\mathcal{S}$. Now all the H_α are proper subgroups, so by hypothesis so is $H = \cup H_\alpha$. If $\langle H \cup Y \rangle = G$ for some finite subset $Y \subset G$, then from

$$\langle H \cup Y \rangle = \bigcup \langle H_\alpha \cup Y \rangle$$

the hypothesis again implies there is some α with $\langle H_\alpha \cup Y \rangle = G$, contradicting $H_\alpha \in \mathcal{S}$. So $H \in \mathcal{S}$, and Zorn's lemma then gives a maximal element $M \in \mathcal{S}$. But this is a contradiction: since $\langle M \cup g \rangle \neq G$ for any $g \in G \setminus M$, and since

$$\langle M \cup g \cup Y \rangle = \langle M \cup (g \cup Y) \rangle$$

we see that $\langle M \cup g \rangle > M$ also belongs to $\mathcal{S}$, contradicting maximality. Thus G is finitely generated.

[11.9] Let $\{B_\alpha\} \subset \mathcal{P}$ be a linearly ordered subset of linearly independent sets of V . Then $B = \cup B_\alpha$ is also linearly independent: for any finite subset $\{b_1, \dots, b_n\} \subset B$, there is a B_α containing all the b_i , and so we know they are linearly independent. Since any one-element subset of V is linearly independent, $\mathcal{P}$ is non-empty, and so by Zorn's lemma there is a maximal linearly independent set X of V . Then for any $v \in V \setminus X$, $X \cup \{v\}$ must be linearly dependent, so there exists constants with

$$av + \sum a_i x_i = 0$$

We must have $a \neq 0$, since otherwise the x_i would be linearly dependent. Thus we can write v as a linear combination of elements of X , so X spans V .

[11.10] If M is Noetherian and completely reducible, then Theorems 11.11 and 11.12 show M can be written as a finite sum of simple X -subgroups. Conversely, suppose M is Noetherian and can be written as a sum of simple X -subgroups, say $M = \sum S_\alpha$ for some indexing set $\mathcal{A}$. Let

$$\mathcal{B} = \{\sum S_\beta : \beta \subset \mathcal{A}, |\beta| < \infty\}$$

Then there is a maximal element $N \in \mathcal{B}$. If some $S_\alpha \not\subset N$, then $(N + S_\alpha) \in \mathcal{B}$ contradicts maximality. Thus all $S_\alpha \subset N$, so that $M = \sum S_\alpha \subset N$. In other words, M is a finite sum of simple X -subgroups. By Theorem 11.12 again, M is completely reducible.

[11.11]

- (a) We know $F \cap M \triangleleft M$, and since F is nilpotent, normalizers grow. Thus we have $M < N_G(F \cap M)$, so by maximality $F \cap M \triangleleft G$. Suppose $F \cap M < N \leq F$ with $N \triangleleft G$. Then by Dedekind's lemma

$$F = G \cap F = NM \cap F = N(M \cap F) = N$$

Thus $F/(F \cap M)$ is G -simple. Since $G/(F \cap M)$ is solvable (as G is), and $F/(F \cap M)$ is a minimal normal subgroup, it is Abelian.

- (b) By part (a), for every maximal subgroup $M \leq G$ not containing F , $F/(F \cap M)$ is G -simple. Let $\mathcal{M}$ be the maximal subgroups not containing F , and $\mathcal{C}$ the maximal subgroups containing F . Then by hypothesis

$$\{1\} = \Phi(G) = \bigcap_{C \in \mathcal{C}} C \cap \bigcap_{M \in \mathcal{M}} M \supset F \cap \bigcap_{M \in \mathcal{M}} M = \bigcap_{M \in \mathcal{M}} (F \cap M)$$

If $\mathcal{M} = \{M_1, \dots, M_n\}$, then write $K_i = F \cap M_i$. We thus have a finite set of G -subgroups of F , the $\{K_i\}$, such that the quotient of each is G -simple, and their intersection is trivial. Since F embeds in $\prod (F/K_i)$, and each factor is Abelian by part (a), F is Abelian. Then Corollary 11.13 shows F is completely reducible as a G -group.

[11.12]

Write $K = \mathbf{F}(G) \cap G'$. By the previous exercise, $\mathbf{F}(G)$ is Abelian, and there is a normal subgroup $A \triangleleft G$ with $\mathbf{F}(G) = AK$ and $A \cap K = \{1\}$. Since $A \cap G'$ is trivial, we have for $a \in A$ and $g \in G$ that

$$[g, a] \in A \cap G' = \{1\}$$

Thus A is central, so $A = \{1\}$ and $\mathbf{F}(G) = K \leq G'$.

[11.13]

First consider the case of a finite simple Abelian G -group S . Since S is finite, it has an N -composition series, so let $T \leq S$ be a simple N -subgroup. Then T^g is also a simple N -subgroup for all $g \in G$ (isomorphic to T with $n \cdot t^g = (ngn^{-1} \cdot t)^g$), and thus

$$X = \sum_{g \in G} T^g$$

is an N -subgroup of S that is a sum of simple N -subgroups. But X is a G -subgroup, and so by simplicity we must have $X = S$. Then S is a finite sum of simple N -subgroups.

Now consider the case A is completely reducible as a G -group, so that by Theorem 11.12 we can write

$$A = \bigoplus_{i=1}^n S_i$$

for simple G -groups S_i . By the previous paragraph, each of these is a finite sum of N -simple N -subgroups, so A is also such a finite sum. Again by Theorem 11.12, A is completely reducible as an N -group.

Chapter 12

[12.1] Let R be a division ring. If $rs = 0$, and $s \neq 0$, then

$$0 = (rs)s^{-1} = r(ss^{-1}) = r1 = r$$

Conversely, suppose R is a finite ring where $rs = 0$ implies either $r = 0$ or $s = 0$. Pick an element $u \in R$ with u nonzero. Consider left multiplication on R by u . If $ur = us$, then $u(r - s) = 0$, and thus $r = s$. In other words, this left multiplication is injective, and so since R is finite it is surjective. There is thus an element $v \in R$ with $uv = 1$. Similarly we can find a left inverse of u by multiplying on the right. Since u was arbitrary, every nonzero element of R has an inverse.

[12.2] The argument in the previous problem that (i) implies (ii) used no finiteness conditions. For the proof that (ii) implies (i), we replace the finiteness of R by the finite dimensionality; it is then still true that being injective (and F -linear) implies being surjective, and the rest of the proof remains the same.

[12.3] Let $S \subset R$ be a unitary subring, and $r \in R$ with $rS = 0$. Since $1 \in S$, this implies $r = r1 = 0$. Conversely, suppose $rS = 0$ implies $r = 0$ for a generic subring S . Let $e \in S$ be its unit, so that $e^2 = e$. Then for any $s \in S$, we have

$$(e - 1)s = (e - 1)es = (e^2 - e)s = 0$$

Thus $(e - 1)S = 0$, so that $e = 1$, and S is unitary.

[12.4] For an integer $m \in \mathbb{Z}^+$, define $mr = r + r + \cdots + r$ (m times). If m is negative, define it as $(-m)(-r)$. And of course $0r = 0$, where the left 0 is from $\mathbb{Z}$ and the right 0 is from R . Now to define the multiplication on $R \times \mathbb{Z}$, we say that

$$(r, m)(s, n) = (rs + ms + nr, mn)$$

To show this is a (unital) ring, note that

$$\begin{aligned}
 (r, m)((s, n)(t, p)) &= (r, m)(st + nt + ps, np) \\
 &= (rst + nrt + prs + mst + mnt + mps + npr, mnp) \\
 &= (rs + ms + nr, mn)(t, p) \\
 &= ((r, m)(s, n))(t, p) \\
 (r, m)((s, n) + (t, p)) &= (r, m)(s + t, n + p) \\
 &= (r(s + t) + m(s + t) + (n + p)r, m(n + p)) \\
 &= ((rs + ms + nr) + (rt + mt + pr), mn + mp) \\
 &= (r, m)(s, n) + (r, m)(t, p) \\
 ((s, n) + (t, p))(r, m) &= (s + t, n + p)(r, m) \\
 &= ((sr + ms + nr) + (tr + mt + pr), nm + pm) \\
 &= (s, n)(r, m) + (t, p)(r, m) \\
 (r, m)(0, 1) &= (r, m) \\
 &= (0, 1)(r, m)
 \end{aligned}$$

Finally, the set $I = \{(r, 0) : r \in R\}$ is a two-sided ideal, and

$$(r, 0)(s, 0) = (rs, 0)$$

so that I is ring-isomorphic to R .

[12.5]

- (a) Note that for $a \in R$, aI is a right ideal of R as well. If $aI \not\subset I$, then by maximality we must have $aI = R$. So for some $x \in I$ we have $ax = 1$, and thus

$$0 = (1 - ax)a = a - axa = a(1 - xa)$$

So if J is the right annihilator of a , we have $1 - xa \in J$. Since J is a right ideal, $J \subset I$, and since $xa \in I$, we would have $1 \in I$, which is a contradiction. Thus $aI \subset I$. Since this is true for all $a \in R$, I is a two-sided ideal.

- (b) Let $a \in R \setminus I$. If a doesn't have a right inverse, then aR is a right ideal, so that $a \in aR \subset I$, which is a contradiction. So there exists $b \in R$ with $ab = 1$. Now we can't have $b \in I$ (since by part (a) it's a left ideal), so by the same reasoning there exists $c \in R$ with $bc = 1$. Then $a = c$ so that $ba = 1$ and a is invertible.

- (c) Let J be a left ideal of R . Then J cannot contain any elements of $R \setminus I$, since by part (b) they're all invertible. Thus $J \subset I$, so that I is the unique maximal left ideal of R .

[12.6]

Let $a \in I$ and suppose $ab = 1$. We can't have b is a unit, since then a is too. So $b \in I$ as well. Then

$$a(1 - b) = a - ab = a - 1$$

so that $a = (a - 1)(1 - b)^{-1}$, where $(a - 1), (1 - b) \notin I$ since that would imply $1 \in I$. Thus a is the product of units, and hence a unit itself. This contradiction shows b does not exist. Similarly, a has no left inverses. Thus aR and Ra must consist only of non-inverses, so both are contained in I . This shows I is an ideal of R . Since every left/right ideal consists of non-units, I is the unique maximal left/right ideal, and the previous problem then says R is local.

[12.7] R is clearly a subring of $\mathbb{Q}$, since if p does not divide n and s , then it doesn't divide ns , so that

$$\frac{m}{n} + \frac{r}{s} = \frac{ms + nr}{ns} \in R$$

And similarly for multiplication. The nonunits of R are precisely those with numerator divisible by p . This set is closed under addition, since

$$\frac{ap}{n} + \frac{bp}{s} = \frac{(sa + nb)p}{ns}$$

By the previous problem, R is local.

[12.8]

- (a) Define the map $\delta : FG \rightarrow F$ on the basis G by $\delta(g) = 1$, and extending F -linearly. This is a vector space homomorphism, so we only need to check it preserves the ring product of FG :

$$\delta(ag)\delta(bh) = ab = \delta(abgh)$$

Here $a, b \in F$ and $g, h \in G$. Since every element of FG looks like $\sum a_i g_i$ and we already know δ is F -linear, this shows it is a ring homomorphism. It is clearly unique because it is uniquely determined (F -linearly) by what it does on the basis G .

- (b) Clearly $\delta(1 - g) = 0$, so that $1 - g \in \Delta$ for all $g \in G$. Let's now show that every element of Δ is a linear combination of the $(1 - g)$ with $g \neq 1$, and that they are F -linearly independent.

If $\sum a_i g_i \in \Delta$, then we must have

$$0 = \delta(\sum a_i g_i) = \sum \delta(a_i g_i) = \sum a_i$$

We can thus write $\sum a_i g_i = \sum -a_i(1 - g_i)$, so that $\{(1 - g) : g \in G\}$ spans Δ . Suppose now that we could write

$$\sum a_i(1 - g_i) = 0$$

with each $g_i \neq 1$. Then the coefficient of g_i , which is a_i , is 0, and hence all the a_i are zero. Thus $\{(1 - g) : g \in G \setminus \{1\}\}$ is an F -basis for Δ .

[12.9] Suppose S has an element $s \in S$ with finite additive order m . If p is a prime dividing $m = pn$, then $ns \neq 0$ has finite order p . Let P be the set of elements in S with additive

order dividing p . Note that $ns \in P$ so it is non-empty. For $a, b \in P$ and $r \in S$, we have

$$\begin{aligned} p(a+b) &= pa + pb \\ &= 0 \\ p(ra) &= r(pa) \\ &= 0 \\ p(br) &= (pb)r \\ &= 0 \end{aligned}$$

Thus P is a nonzero ideal of S , so that $S = P$ and every nonzero element of S has additive order p .

[12.10] We apply the "usual" formula for an inverse, relying on the fact r is nilpotent:

$$(1-r)^{-1} = \sum_{i=0}^{\infty} r^i = 1 + r + r^2 + \cdots + r^{n-1}$$

Multiplying these on the left and right shows it is an actual inverse.

[12.11] If $r, s \in R$ are nilpotent (say of orders m and n), then $(ra)^m = r^m a^m = 0$ for any $a \in R$. Meanwhile, every term in the binomial expansion of $(r+s)^{m+n}$ contains either a multiple of r^m or s^n , so it is also 0. Thus the nilpotent elements form an ideal when R is commutative.

For a counterexample with non-commutativity, consider $A, B \in M_2(\mathbb{R})$, with

$$\begin{aligned} A &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ B &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

We have $A^2 = B^2 = 0$, but $(A+B)^2 = I$.

[12.12] [We alter the problem to discuss "nonzero" ideals.] When G is finite, the augmentation ideal of [12.8] is finite dimensional. Now suppose $I \leq FG$ is a finite F -dimensional nonzero ideal. Then we can write I with a finite F -basis, say $\{b_1, \dots, b_n\}$, with each expressible as an element of FG :

$$b_i = \sum a_{ij} g_{ij}$$

Let $S = \{g_{ij}\}$, which is a finite subset of G , so that I is contained in the F -span of S . Relabel S as $\{s_1, \dots, s_n\}$, and let $\sum a_i s_i$ be a nonzero element of I , say with nonzero coefficient a_1 . Let $g \in G$ be arbitrary, then from the fact that $gs_1^{-1}I \subset I \subset \langle S \rangle_F$, we can write

$$\sum a_i g s_1^{-1} s_i = \sum b_i s_i$$

Since G is linearly independent, this implies the coefficient of each element of G is equal on both sides of this equation. In particular, since $gs_1^{-1}s_1 = g$, we see that the coefficient on the right-hand side for g is non-zero, so that $g \in S$. Thus $S = G$ and G is finite.

Finally, if G is finite, let $x = \sum g$ be the sum of all elements of G . Then the set $J = \langle x \rangle_F$ is a one-dimensional subspace, and we claim it is actually an ideal:

$$(\sum a_i g_i) bx = \sum a_i bx = (\sum a_i b) x$$

where we've used that $g_i x = x$, since multiplication by g_i just permutes the elements of G . Similar reasoning shows that J is also a right ideal, and hence is an ideal of FG .

[12.13] Of course $eRe \subset eR$. Now define the map $eR \rightarrow eRe$ by $x \mapsto xe$. This is clearly an additive homomorphism, and also respects multiplication:

$$(eres)e = (ere)(ese)$$

Suppose $er \in eR$ is such that $ere = 0$. Then $(er)^2 = 0$ so that $er = 0$ (since R has no nonzero nilpotents). So our map is injective. But R is finite, so then eR and eRe are finite as well, so that we must have $eR = eRe$.

[12.14] Let D be a division ring, and let $A = D$ as an Abelian (additive) group, and $X = D$ acting via multiplication on the left. By Corollary 12.11, A is a simple X -group. Now for any $d \in D$, we have that right multiplication ρ_d (given by $(a)\rho_d = ad$) is an element of $\text{End}_X(A)$, since

$$(ba)\rho_d = bad = b(a)\rho_d$$

If $\phi \in \text{End}_X(A)$ is an arbitrary endomorphism, let $(1)\phi = d$. Then for $a \neq 0$ we have

$$d = (1)\phi = (a^{-1}a)\phi = a^{-1}(a)\phi$$

And thus $(a)\phi = ad$ for all $a \in A$. This means $\phi \equiv \rho_d$. So the map $d \mapsto \rho_d$ is surjective, and since $\rho_d(1) = d$, it is clearly injective. We also have

$$\begin{aligned} \rho_d + \rho_x &= \rho_{d+x} \\ \rho_d \rho_x &= \rho_{dx} \end{aligned}$$

And thus the map $D \rightarrow \text{End}_X(A)$ is an isomorphism.

[12.15] Let $y, z \in C(X)$, and $x \in X$ be arbitrary. Then

$$(y + z)x = yx + zx = xy + xz = x(y + z)$$

shows $C(X)$ is closed under addition. We also have

$$(yz)x = yxz = x(yz)$$

so that $C(X)$ is closed under multiplication. Finally, $0, 1 \in C(X)$ clearly, and from $xy = yx$ with $y \neq 0$ we have $y^{-1}x = xy^{-1}$, so $C(X)$ is closed under nonzero inverses, and is a division ring.

[12.16] If R is an F -algebra, then $F \cdot 1 \subset Z(R)$ is isomorphic to F (since F has no nonzero ideals). Conversely, suppose the central unitary subring S exists, with $S \cong F$. Then for $s \in S$, we have

$$s(ab) = (sa)b = a(sb)$$

so that R is an F -algebra. [That R is an F -vector space and uses the same addition comes from $F \cong S \subset R$.]

[12.17] $Z(R) \subset R$ is a unitary subring. Let $I \leq Z(R)$ be a nonzero ideal. Then $IR = RI$ is a nonzero ideal of R , so by simplicity $IR = R$. In particular, there is $i \in I$ and $r \in R$ with $ir = ri = 1$. Since then $r = i^{-1}$, we also have $r \in Z(R)$, so that $1 = ir \in I$, implying $I = Z(R)$. So $Z(R)$ is a simple commutative ring: a field.

If $R = M_n(F)$, then clearly $aI \in Z(R)$, where I is the identity element and $a \in F$. If $A \in Z(R)$, then we have

$$\sum a_{ij}e_{kj} = e_{ki}A = Ae_{ki} = \sum a_{jk}e_{ji}$$

Since the $\{e_{ki}\}$ form an F -basis of R , this equality means the coefficients of each matrix unit on each side are equivalent. If $i \neq j$ and $a_{ij} \neq 0$, then the coefficient of e_{kj} on the left-hand side is nonzero, but there is no e_{kj} on the right side. So for $A \in Z(R)$ we must have $a_{ij} = 0$ for $i \neq j$. So the above equation simplifies to

$$\sum a_{ii}e_{ki} = e_{ki}A = Ae_{ki} = \sum a_{kk}e_{ki}$$

And so $a_{ii} = a_{kk}$ for all i and k . That is, $A = a_{11}I$, and thus $Z(R)$ is isomorphic to F .

[12.18] Let $\alpha \in F$. Define $\alpha m = m(\alpha 1)$. Note that we then have

$$\alpha(ma) = (ma)\alpha 1 = m(a\alpha 1) = m(\alpha a) = m(\alpha 1a) = (m\alpha 1)a = (\alpha m)a$$

We also have an F -vector space structure on M :

$$\alpha(m + n) = (m + n)\alpha 1 = m\alpha 1 + n\alpha 1 = \alpha m + \alpha n$$

Finally, this is unique, since if $\alpha(ma) = m(\alpha a)$, then choosing $a = 1$ we see that $\alpha m = m(\alpha 1)$.

[12.19] For $m \neq 0$ in M , the map $a \mapsto ma$ is a surjective F -linear map from A to M by the previous problem; since A is finite dimensional, so then is M . Now if $\alpha \in \text{End}_A(M)$, then for $\lambda \in \mathbb{C}$ we have

$$\alpha(\lambda m) = \alpha(m(\lambda 1)) = \alpha(m)\lambda 1 = \lambda \alpha(m)$$

so that α is $\mathbb{C}$ -linear. There is thus an eigenvalue ζ of this linear map on the finite-dimensional vector space M . $m \mapsto \zeta m$ is of course an endomorphism of M , since $\zeta(ma) = (\zeta m)a$ by the previous problem. Define a new map by

$$\beta(m) = \alpha(m) - \zeta m$$

We have $\beta \in \text{End}_A(M)$, which is a division ring by Schur's lemma. But if $n \in M$ is an eigenvector associated to ζ for α , then $\beta(n) = 0$. This implies $\beta \equiv 0$, and so $\alpha(m) = \zeta m$ for all $m \in M$.

[12.20] The previous problem shows that $\text{End}_A(M) \cong \mathbb{C}$. Since A is commutative, we also have $\rho_a \in \text{End}_A(M)$ for every $a \in A$, where $\rho_a(m) = ma$. Thus $ma = \lambda_a m$ for some $\lambda_a \in \mathbb{C}$. So if $m \neq 0$ in M , then $\mathbb{C}m$ is an A -submodule, so by simplicity is all of M , so that M is one-dimensional.

[12.21] Let A be the $\mathbb{C}$ -algebra generated by X and the scalar matrices. Then A is commutative and finite-dimensional. Let $M = \mathbb{C}^n$ be an A -module. Then every A -submodule of M is a $\mathbb{C}$ vector subspace, so M is Artinian/Noetherian. Let $S \leq M$ be a simple A -submodule. By the previous problem, S is one-dimensional over $\mathbb{C}$: $S = \mathbb{C}v$ for some $v \in M$. Then for every $x \in X \subset A$, we have

$$vx = \lambda_x v$$

for some $\lambda_x \in \mathbb{C}$, so that v is a common eigenvector for all elements of X .

[12.22] (a) Since R is Artinian and Noetherian, it has a finite composition length (as a module over itself). Let that length be k . Then R^n has composition length nk . So if $R^n \cong R^m$, then $nk = mk$, so that $n = m$.

(b) When I is an ideal of R , then $I^n \leq R^n$ is an R submodule. So $R^n/I^n \cong (R/I)^n$ is an R module, with I acting trivially, so is really an R/I module. So if $R^n \cong R^m$, then $(R/I)^n \cong (R/I)^m$ as R/I modules. When I is a maximal ideal, R/I is a field, and these are vector spaces of dimensions n and m . So in this case $n = m$.

[12.23] First note we can treat $B = (B, 0)$ and $C = (0, C)$ as R -modules, with right R -submodules corresponding exactly to right ideals. Suppose B and C are right Artinian as rings; then they are right Artinian as R -modules. Then if $R = B \oplus C$, we have both B and $R/B \cong C$ are Artinian, so by Theorem 11.6 R is Artinian. Conversely, if R is Artinian, so are its submodules B and C , and so B and C are Artinian as rings. The same line of reasoning works for Noetherian.

[12.24] (a) R is clearly closed under addition. Meanwhile, we have

$$\begin{pmatrix} b & 0 \\ a & c \end{pmatrix} \begin{pmatrix} \hat{b} & 0 \\ \hat{a} & \hat{c} \end{pmatrix} = \begin{pmatrix} b\hat{b} & 0 \\ a\hat{b} + c\hat{a} & c\hat{c} \end{pmatrix}$$

Thus R is closed under multiplication. Since B and C are unitary, the identity matrix is in R , so it is a ring.

Finally, I is an ideal because

$$\begin{pmatrix} 0 & 0 \\ \hat{a} & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ a & c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \hat{a}b & 0 \end{pmatrix}$$

$$\begin{pmatrix} b & 0 \\ a & c \end{pmatrix} \begin{pmatrix} 0 & 0 \\ \hat{a} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ c\hat{a} & 0 \end{pmatrix}$$

(b) Consider the map $R \rightarrow B \oplus C$ given by sending

$$\begin{pmatrix} b & 0 \\ a & c \end{pmatrix} \mapsto (b, c)$$

Part (a) shows this is a ring homomorphism, and is surjective. The kernel is precisely I .

(c) Consider the map $\phi : I \rightarrow A_B$ given by sending

$$\begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} \mapsto a$$

This is an additive isomorphism. The map $b \mapsto \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$ is an isomorphism by part (a). This gives an action of B on the right of I , and part (a) shows ϕ is a B -module homomorphism as well. Part (a) in fact shows that right R -submodules of I are precisely the right B -submodules. Thus I is right Artinian/Noetherian precisely when A_B is.

(d) The same reasoning (*mutatis mutandis*) in the previous part, with C acting on the left, works as well for ${}_C A$.

(e) As fields, all of A, B, C are Artinian/Noetherian rings. Since $A = B$, we have that A_B is clearly Artinian/Noetherian as a B -module. Thus by part (c), I is a right Artinian/Noetherian R -module. Since $R/I \cong B \oplus C$, the previous problem shows R/I is right Artinian/Noetherian as well, as an R/I (and hence R) module. By Theorem 11.6 then, R is right Artinian/Noetherian.

However, ${}_C A$ is not Artinian/Noetherian as a C module, since it is infinite dimensional over C . Thus by part (d) I is not a left Artinian/Noetherian submodule of R . This implies R itself is not left Artinian/Noetherian.

[12.25] Let $\zeta = \sum a_g g$ be an element of $Z(FG)$. Then for any $h \in G$, we have

$$\zeta = h^{-1} \zeta h = \sum a_g g^h$$

Since G is linearly independent over F , equating coefficients above shows $a_g = a_{g^h}$ for all $g \in G$. In particular, since h was arbitrary, for any conjugacy class $C \subset G$, the coefficients of each element of C in ζ are equal.

Let $\{C_0, C_1, \dots, C_m\}$ be the conjugacy classes of G . From the above,

$$\zeta_i = \sum_{g \in C_i} g$$

is in $Z(FG)$, and any element of $Z(FG)$ can be written as an F -linear combination of the ζ_i . Clearly $Z(FG)$ is closed under addition and multiplication by F , and since the conjugacy classes of G are disjoint (and G is linearly independent over F), we have the $\{\zeta_i\}$ are linearly independent, and hence form an F -basis for $Z(FG)$.

[12.26] Write $1 = \sum e_i$, where $e_i \in I_i$. Then for any $x \in I_i$, we have

$$x = x1 = x(e_1 + \dots + e_n) = xe_i$$

and similarly with multiplication on the left. The final equality above uses that $xe_j \in I_i \cap I_j = \{0\}$. Thus each e_i is an identity element for its respective ideal. Note that for any $r, s \in R$, we have that

$$\begin{aligned} rs &= (re_1 + \dots + re_n)(e_1s + \dots + e_ns) \\ &= \sum re_ie_is \\ &= \sum rse_i \end{aligned}$$

by the same reasoning: $re_ie_js \in I_i \cap I_j = \{0\}$. Here we have also used that e_i is a unity for I_i to reduce

$$re_ie_is = re_is = (re_is)e_i = re_i(se_i) = rse_i$$

The expressions in parentheses above are elements of I_i .

Now define a map $\phi : R \rightarrow \oplus I_i$, by sending $r \mapsto \oplus re_i$. This is surjective, an additive homomorphism, and preserves the identity. It is injective because $\sum e_i = 1$, and by the previous paragraph it is a multiplicative homomorphism. Thus this is a ring isomorphism.

[12.27] Every element of R can be written as $\sum_{i,j} e_{ij}a_{ij}$ for $a_{ij} \in D$, so to show I_i is a right ideal, it's enough show for any $x \in I_i$, we have $xe_{jk}a_{jk} \in I_i$. But we have

$$xe_{jk}a_{jk} = x_{ij}e_{ik}a_{jk} = x_{ij}a_{jk}e_{ik}$$

and that's in I_i . To show I_i is simple, let y be an arbitrary element of I_i and let x be a nonzero element in an R -submodule of I_i ; suppose $x_{ik} \neq 0$ for some k . Then

$$y = \sum_j y_{ij}e_{ij} = \sum_j (x_{ik}x_{ik}^{-1}y_{ij})e_{ij} = x \sum_j e_{kj}(x_{ik}^{-1}y_{ij})$$

Thus any nonzero submodule of I_i is all of I_i , so it is simple.

[12.28] Suppose $x^2 + y^2 + z^2 = -1$ for $x, y, z \in F$. Then

$$(1 + xi + yj + zk)(1 - xi - yj - zk) = 1 + x^2 + y^2 + z^2 = 0$$

Thus $\mathbb{H}(F)$ has zero divisors, so cannot be a division ring. Conversely, if $\mathbb{H}(F)$ is not a division ring, then by [12.2] there are nonzero elements $r, s \in \mathbb{H}(F)$ with $rs = 0$. Let $r = a + bi + cj + dk$, and define $\bar{r} = a - bi - cj - dk$. Then $\bar{r}r = a^2 + b^2 + c^2 + d^2$. If this is a nonzero element of F , then $\bar{r}r$ is invertible, and hence from $\bar{r}rs = 0$ we have $s = 0$, which contradicts our assumption. So we must have that $\bar{r}r = 0$. One of the $\{a, b, c, d\}$ is non-zero (since r is non-zero); assume without loss of generality it is a . Then dividing $\bar{r}r$ by a^2 , we have

$$\left(\frac{b}{a}\right)^2 + \left(\frac{c}{a}\right)^2 + \left(\frac{d}{a}\right)^2 = -1$$

[12.29] Let $e \in S$ be the unit of S . Define $T = \{r \in R \mid er = re = r\}$, and note that $S \subset T$. In fact, for any subring $X \subset R$ such that $S \subset X$ is a unitary subring, it must be that $X \subset T$. So to complete the solution, we will show T is a ring. Obviously e functions as its identity. For $r, s \in T$ we also have

$$e(r + s) = er + es = r + s = re + se = (r + s)e$$

to show T is closed under addition. T is also closed under multiplication:

$$e(rs) = (er)s = rs = r(se) = (rs)e$$

[12.30]

(a) We have $x(1 - yx) = x - (xy)x = x - x = 0$. Thus $1 - yx \neq 0$ is a right annihilator of x .

(b) Suppose $x^n a = 0 \neq x^{n-1} a$. Then we must have

$$x^{n+1} ya = x^n (xy) a = x^n a = 0 \neq x^{n-1} a = x^{n-1} (xy) a = x^n ya$$

So ya annihilates x^{n+1} but not x^n .

(c) If $yx \neq 1$, then parts (a) and (b) give an infinite ascending sequence of right ideals (this is by induction, the base case for part (b) being $n = 1$). Since R is right Noetherian, that is impossible. So we must have $yx = 1$.

Chapter 13

[13.1] Let J be a maximal right ideal of R containing I , and let $U = R/J$ be a simple right R -module. Then $\text{ann}_R(U)$ is an ideal of R , and if we show $I \leq \text{ann}_R(U)$, then maximality shows $I = \text{ann}_R(U)$. So let $x \in I$ and let $u \in U$, represented as Jy for some $y \in R$. Then $yx \in I \leq J$, so $ux = 0$.

[13.2] If I is a primitive ideal of R , let it be $\text{ann}_R(U)$ for some simple module U . Let $u \in U$ be non-zero, and $J \geq I$ be $\text{ann}_R(u)$. J is a maximal ideal of R by Lemma 13.1. But if $y \in J$ and $r \in R$, then $ury = (uy)r = 0$. Since $uR = U$, we see that $y \in I$, implying $J \leq I$ so that $J = I$ is maximal.

[13.3] Suppose $a \in J(R)$, so that $ba \in J(R)$ as well, such that ba is quasiregular by Theorem 13.4. Since $a(1 - ba) = a - aba = 0$, and $(1 - ba)$ is invertible, we have that $a = 0$.

[13.4]

(a) Let $v \in V$ be non-zero, and write $v = (a_1, \dots, a_n)$, assuming $a_i \neq 0$ for some i . Then

$$(b_1, \dots, b_n) = v \sum_j a_i^{-1} b_j e_{ij}$$

Thus for the arbitrary $v \neq 0$, we have $vR = V$, and so V is simple.

(b) let $\phi : V \rightarrow V$ be an R -module homomorphism, and let $v_1 = (1, 0, \dots, 0)$. If we let $\phi(v_1) = (a_1, \dots, a_n)$, then from

$$\phi(v_1) = \phi(v_1 e_{11}) = \phi(v_1) e_{11} = (a_1, 0, \dots, 0) = a_1 v_1$$

we have that $\phi(v_1 r) = (a_1 v_1) r = a_1 (v_1 r)$, and since $v_1 R = V$ it must be that ϕ is just multiplication (on the left) by $a_1 \in D$. Conversely, for any $a \in D$, left multiplication is an element of $\text{End}_R(V)$, since

$$(av)r = a(vr)$$

Thus E is precisely left multiplication by elements of D .

[13.5]

(a) Consider the additive subgroups $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in R \right\}$ and $B = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} : b \in R \right\}$. The following shows $A \leq S$ is a right ideal, and $B \leq S$ is a left ideal:

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & 0 \\ r & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} c & 0 \\ r & d \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & db \end{pmatrix}$$

Now for any $x_a \in A \cap J(S)$ (having a in the upper left corner), we know that x_a is quasiregular, so that in particular $1 - a$ is invertible. The set $\hat{A} = \{a \in R : x_a \in A \cap J(S)\}$ is a right ideal of R , with all elements quasiregular, and hence $\hat{A} \leq J(R)$. All that's left to do is show that if some $y \in J(S)$, then if a is the upper-left corner of y , we have $x_a \in A \cap J(S)$, since this implies $a \in J(R)$. For that we have

$$x_1 y = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ r & b \end{pmatrix} = x_a$$

The preceding arguments work just as well for B swapping "left" and "right".

(b) We have

$$\begin{pmatrix} a^{-1} & 0 \\ x & b^{-1} \end{pmatrix} \begin{pmatrix} a & 0 \\ r & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ r & b \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ x & b^{-1} \end{pmatrix}$$

where $x = -b^{-1}ra^{-1}$.

(c) Note that

$$J = \begin{pmatrix} J(R) & 0 \\ R & J(R) \end{pmatrix} \leq S$$

is an ideal of S . For each $x \in J$, we have that $I - x$ has invertible elements along the diagonal, so by part (b) $I - x$ is invertible in S . Thus every element of J is quasiregular, so $J \leq J(S)$.

Note this problem shows, in the language of part (c), that $J = J(S)$.

[13.6] We work by induction on $|G|$, the case of $|G| = 1$ being obvious. For $|G| > 1$, let $z \in Z(G)$ be an element of order p , generating a central subgroup Z . Consider the ring homomorphism $A \rightarrow F(G/Z)$ given by sending group elements to their representatives in G/Z . Suppose $\sum a_g g$ is in the kernel of this map; then for every $g \in G$, we have

$$\sum_{h \in gZ} a_h = 0$$

If we relabel the coefficients above as a_i for gz^i , then it is straightforward to see (using $\sum a_i = 0$)

$$(1 - z) \sum_{i=0}^{p-1} \left(\sum_{j=0}^i a_j \right) gz^i = \sum_{k=0}^{p-1} a_k gz^k$$

Doing this for each coset of Z shows that every element in the kernel is a multiple of $(1 - z)$, so that the kernel must in fact be $(1 - z)A$. Since $(1 - z)^p = 0$ and z is central, we have by Corollary 13.5 that $(1 - z) \in J(A)$, so that our whole kernel is in $J(A)$. By Corollary 13.2 then, the image of $J(A)$ is equal to $J(F(G/Z))$. The induction hypothesis shows $J(F(G/Z))$ has codimension 1, and so then too does $J(A)$.

[13.7] We know from [12.7] that L_p is local. So there is only one maximal ideal of L_p consisting of all non-units, and so $J(L_p)$ (as an intersection of the maximal ideals) is precisely these non-units.

[13.8]

- (a) This is untrue; see [13.5] to see that if S is the lower triangular matrices of $M_2(\mathbb{R})$, then $J(S)$ consists of all matrices with zeroes everywhere except the lower left. Meanwhile $M_2(\mathbb{R})$ is simple and has trivial Jacobson radical.
- (b) This is also untrue; let $S = \mathbb{Z}$ and $R = L_p$ from the previous problem. Then $J(S) = \{0\}$ while $p\mathbb{Z} \subset J(R)$.

[13.9]

- (a) Assume $Ue \neq \{0\}$. Let $ue, ve \in Ue$ with $ue \neq 0$. Since U is simple, we know there is an $r \in R$ with $uer = ve$. Then

$$(ue)(ere) = (ue)(re) = (ve)e = ve$$

Thus $(ue)eRe = Ue$ and Ue is simple.

- (b) Suppose $ere \in eRe$ annihilated each simple eRe module. If U is any simple R module, then from part (a) we know $(Ue)(ere) = 0$. Since e is idempotent, this means $U(ere) = 0$. Because U was an arbitrary simple R module, we have $ere \in J(R)$. Thus $J(eRe) \subset J(R)$.

[13.10] Since e is the identity of eRe , the previous problem implies $J(eRe) \subset eJ(R)e$. Now suppose $x \in eJ(R)e \subset J(R)$. Then x is quasiregular, so that there exists $y \in R$ with $(1-x)y = 1 = y(1-x)$. Then we have

$$(e-x)(eye) = eye - exye = e(y-xy)e = e$$

Here we have used $ex = x = xe$. Similarly, we see that $(eye)(e-x) = e$. Thus eye is an inverse for $(e-x) \in eRe$. Since $eJ(R)e$ is an ideal of eRe , and we've just shown it contains all quasiregular elements, we have $eJ(R)e \subset J(eRe)$.

[13.11] If $\dim(V) = n < \infty$, then $R \cong M_n(D^{op})$ by Lemma 13.19, so is of course simple. If $\dim(V)$ is infinite, consider the subset $I \subset R$ of elements $\alpha \in R$ where $\alpha(V)$ is contained in a finite dimensional subspace of V . Note that I is a proper additive subgroup of R . If $\beta \in R$, then from $\alpha\beta(V) \subset \alpha(V)$ we see that I is a right ideal; if $\alpha(V) \subset W$ with $\dim(W) < \infty$, then $\beta\alpha(V) \subset \beta(W)$ with the latter finite-dimensional, so I is a left ideal as well. Thus I is a proper ideal of R , so R is not simple.

[13.12]

- (a) Since R is primitive, it has a faithful simple module U . Since a submodule of $R^\bullet$ is just a right ideal, Lemma 13.25 shows all minimal right ideals of R are isomorphic to U , and hence to each other.
- (b) Let J be a minimal right ideal of R , which by part (a) is a faithful simple module for R . Then $JI \subset J$ is a right R -module, so by simplicity and faithfulness we must have $J = JI$. But since I is an ideal, $JI \subset I$.

[13.13] Let $s+x = 1$ with $s \in S$ and $x \in J(R)$. Also let $e \in S$ be its unit. Then

$$\begin{aligned} e &= e(s+x) \\ &= s+ex \\ e(1-x) &= s \\ &= (1-x) \end{aligned}$$

Since $1-x$ is invertible, this shows $e = 1$, so S is unitary.

[13.14] Define U as

$$U = \{u \in eR \mid uRe = \{0\}\}$$

Note that for $u \in U$ and $r \in R$, we have $(ur)Re \subset uRe = \{0\}$, so $ur \in U$ and U is a right R -submodule. Since $ue = 0$ for any $u \in U$, and $U \subset eR$, we of course have $U^2 = \{0\}$. What's left to show is that eR/U is simple.

To that end, let $er, es \in eR \setminus U$. There is thus an $a \in R$ with $erae \neq 0$. Since eRe is a division ring, there's an inverse $x \in eRe$ to this element, and then

$$(er)(aexs) = (erae)x(s) = es$$

This shows that for any two non-zero elements in eR/U , there's an element of R taking one to the other, and thus eR/U is simple.

[13.15] Let $V = XR$ be the submodule of U generated by X . The hypothesis of the problem then shows that V maps onto U/UJ , so by the correspondence theorem $U = V + UJ$. By Nakayama's lemma, $V = U$.

[13.16] If $x \in U(R)$, then there exists $y \in R$ with $xy = 1 = yx$, and that still holds in $R/J(R)$, so we have a well-defined map from $U(R)$ to $U(R/J(R))$. Now let $x + J(R)$ be a unit in $R/J(R)$, so that there exists $y \in R$ with $1 - xy \in J(R)$. Since this element is quasi-regular, there is a $z \in R$ with

$$1 = (1 - (1 - xy))z = xyz$$

so that x has a right inverse. Similarly it has a left inverse, so $x \in U(R)$ and x maps (of course) to $x + J(R)$.

[13.17] Let M be a simple A -module, which (as a quotient of A) is finite-dimensional as a $\mathbb{C}$ vector space. (Note M exists because any minimal right ideal of A is simple.) By [12.19] we see that $\text{End}_A(M) \cong \mathbb{C}$. Because A is simple, its image in $\text{End}(M)$ is isomorphic to A . Then since A is Artinian, by the double centralizer theorem, we have

$$M_n(\mathbb{C}) \cong \text{End}_{\mathbb{C}}(M) \cong A$$

where $n = \dim_{\mathbb{C}}(M)$.

Chapter 14

[14.1] We prove this by induction on $|X|$, the case X being empty the trivial base case. Now suppose $|X| = n + 1$, and let $x_0 \in X$ with $X_0 = X \setminus \{x_0\}$. The inductive hypothesis implies $X_0 \subset J$ with J nilpotent, and of course $I = \langle x_0 \rangle$ is nilpotent because x_0 is and R is commutative. Suppose $I^m = \{0\} = J^n$. Then for $a \in I$ and $b \in J$ we have

$$(a + b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}$$

and in each of those terms on the right-hand side, either $k \geq m$ and/or $m + n - k \geq n$. So every term is zero, and thus $(a + b)^{m+n} = 0$. Since a and b were arbitrary, this shows $(I + J)^{m+n} = \{0\}$, and since $X \subset I + J$ we are done.

[14.2] Assume x is such that $Ix = \{0\}$ but $xI \neq \{0\}$. Then R being semiprime implies for the right ideal xI that

$$\{0\} \neq (xI)^2 = x(Ix)I = \{0\}$$

this contradiction shows every right annihilator is a left annihilator; the reverse argument shows we have two-way containment, hence equality.

[14.3]

- (a) We define the a_i inductively, with $a_1 = a$. Suppose we've defined a_i for $i \leq n$. Since R is semiprime and $a_n \neq 0$, we know that $a_n R a_n \neq \{0\}$, so we can take $a_{n+1} \in a_n R a_n$. By construction a_{n+1} is in $a_n R a_n$, and the inductive hypothesis implies for $j < n$ that

$$a_{n+1} \in a_n R a_n \subset (a_j R a_j) R (a_j R a_j) \subset a_j R a_j$$

so our induction is complete.

- (b) Suppose $a_i \in I$ and $a_j \in J$, and without loss of generality assume $i < j$. Then we know $a_j \in a_i R a_i \subset I$. So we have a_j in both I and J . Then $a_j R a_j \subset IJ$ so that $a_{j+1} \in IJ$.
- (c) Suppose $A, B \supset P$, so that by maximality $A \cap S$ and $B \cap S$ are non-empty. By the previous part, $AB \cap S \neq \emptyset$, but since P is disjoint from S , this implies $AB \not\leq P$. This is the contrapositive definition of being a prime ideal.

[14.4] Suppose first the intersection of prime ideals is zero. If P is an arbitrary prime ideal, and I is nilpotent, then $I^n = \{0\} \leq P$, so that by primeness $I \leq P$. Since P was arbitrary, I is contained in every prime ideal, so we have $I = \{0\}$. Thus R is semiprime.

Conversely, let R be semiprime. For $0 \neq a \in R$, build the set S as in the previous problem. If an ascending chain $\{I_\alpha\}$ of ideals intersects S trivially, then $\cup I_\alpha$ is an ideal that also intersects S trivially. Zorn's lemma then implies a maximal such ideal P such that $P \cap S = \emptyset$. The previous problem shows P is prime, and $a \in S$, so $a \notin P$. Since a was an arbitrary nonzero element, we see that the intersection of all prime ideals contains no nonzero elements, and is thus $\{0\}$.

[14.5]

- (a) Let $M = R_1 \times \{0\} \leq R^\bullet$ be a submodule of the regular module, and similarly define N . Since $J = \{0\} \times R_2 \leq R$ acts trivially on M , and is an ideal of R , we see that M is really a module over $R/J \cong R_1$, and as such it is isomorphic to the regular module $R_1^\bullet$, hence Artinian. Similarly, N is a module over R_2 and is Artinian. Then $R^\bullet$ is the sum of two Artinian submodules, hence Artinian.

- (b) Let $I = R_1 \times \{0\}$ and $J = \{0\} \times R_2$ be ideals of R . Let $K \leq R$ be an ideal with $K^2 = \{0\}$. The map $R \rightarrow R/I$ sends K to an ideal of $R/I \cong R_2$ which is nilpotent; since R_2 is semiprime, we see that the image of K is zero, so that $K \leq I$. Similarly $K \leq J$, and thus $K \leq I \cap J = \{0\}$. So R is semiprime.

[14.6] By Theorem 14.2, $J(R)$ is nilpotent. If $M \leq R$ is a maximal ideal, then the image of $J(R)$ in R/M is also nilpotent. But the only ideals of R/M are the trivial ones, so the image of $J(R)$ must be the zero ideal; in other words, $J(R) \leq M$. Since this holds for all maximal ideals, we can count the maximal ideals of R by counting them in $R/J(R)$. This is a Wedderburn ring, so by Lemma 14.16 it has only finitely many ideals, so certainly only finitely many maximal ideals.

[14.7] Suppose first that e is not primitive, so we can write $e = f + g$ for two orthogonal idempotents f and g . Then note $f = ef \in eR$, and similarly $g \in eR$, so that $fR + gR \leq eR$. Of course, since $f + g = e$, we see that $fR + gR = eR$. Also, if $x = fr = gs$, then

$$0 = (fg)s = fx = f(fr) = fr = x$$

Thus $fR \cap gR = \{0\}$, and $eR = fR \oplus gR$ shows it is decomposable.

Conversely, suppose $eR = M \oplus N$, and let $e = m + n$. Since $m \in eR$ and e is idempotent, we know that

$$m = em = (m + n)m = m^2 + nm$$

But then $m - m^2 = m(1 - m) = nm$ is in $mR \subset M$ and $nR \subset N$, so is 0; that is, $m = m^2$. From the equation above this implies $nm = 0$. Similarly, $n = n^2$ and $mn = 0$. So m and n are orthogonal idempotents with $e = m + n$, so e is not primitive.

[14.8] Let e be an idempotent, and we show it is the finite sum of mutually orthogonal primitive idempotents. Since R is Artinian, it is also Noetherian (Theorem 14.11). Since eR is a finitely generated R -module, it is also Artinian and Noetherian (Corollary 11.8), so has finite composition length (Theorem 11.3). This means we can write eR as a finite direct sum of indecomposable right ideals contained in eR (Lemma 10.9).

Now we mimic the proof for the previous problem. Write $eR = M_1 \oplus \cdots \oplus M_k$ for indecomposable right ideals M_i . Let $e = \sum m_i$ for $m_i \in M_i$. We know that

$$m_i = em_i = \left(\sum m_j\right) m_i = m_i^2 + \sum_{j \neq i} m_j m_i$$

Then $0 = (m_i - m_i^2) - \sum_{j \neq i} m_j m_i$. By the direct sum decomposition, we have $m_i = m_i^2$ and $m_j m_i = 0$ for $j \neq i$. This works for all i , so we see that our decomposition has expressed e as a sum of mutually orthogonal idempotents.

The final piece is to show $M_i = m_i R$, since then the previous problem shows then that each of the m_i is primitive. To that end, note that since $m_i R \leq M_i$ and M_i is indecomposable, the Peirce decomposition (Lemma 14.8) shows we cannot have $m_i R < M_i$.

[14.9] Let $\hat{U} = (U + J(R))/J(R) \leq R/J(R)$. Then $R/J(R)$ is a Wedderburn ring, so by Lemma 14.16 there is an ideal $\hat{V} \leq R/J(R)$ such that $\hat{U} + \hat{V} = R/J(R)$, and $\hat{U} \cap \hat{V} = \{0\}$. Up in R , this means there's an ideal V containing $J(R)$ such that $(U + J(R)) + V = R$ and $(U + J(R)) \cap V \leq J(R)$. Since $J(R) \leq V$, this means $U + V = R$, and since $U \leq U + J(R)$, we also have $U \cap V \leq J(R)$.

[14.10] Let $1 = u_1 + v_1$ be a representation of $1 \in R$. Also, let $r = u_r + v_r$ be a representation of the inverse of v in R/U : $1 - rv \in U$. Then we have for $x = 1 - (u_1 + v_r)(u_1 + v)$ the following equivalent expressions:

$$\begin{aligned} 1 - (u_1 + v_r)(u_1 + v) &= (1 - v_r v) - (v_r u_1 + u_1 v + u_1^2) \\ 1 - (u_1 + v_r)(u_1 + v) &= (1 - u_1^2) - (v_r u_1 + u_1 v + v_r v) \end{aligned}$$

Since $1 - rv \in U$, that implies $1 - v_r v \in U$; thus the first line above shows $x \in U$. Since also $1^2 = u_1^2 + (u_1 v_1 + v_1 u_1 + v_1^2)$, we see that $1 - u_1^2 \in V$; thus the second line above shows $x \in V$. So we have $x \in U \cap V \subset J(R)$, and hence $(u_1 + v_r)(u_1 + v)$ is invertible. This means that $u_1 + v$ has a left inverse. Similarly, by reversing the product order in the expression for x , we see it has a right inverse, and thus $u_1 + v$ is invertible, as desired.

[14.11] If $u \in R$ is invertible, so that $vu = 1 = uv$, then $\overline{vu} = 1 = \overline{uv}$ in R/I , so the units of R map to units of R/I . Now suppose $\bar{x} \in R/I$ is invertible. Choose an ideal J such that $I + J = R$ and $I \cap J \leq J(R)$, by [14.9]. Then the previous problem shows there is some $y \in I$ with $x + y$ invertible in R . But $\bar{x} + \bar{y} = \bar{x}$ and we're done.

[14.12] Since $R/J(R)$ is Wedderburn, Theorem 14.13 shows there's an $a \in R$ with $\bar{a} \in R/J(R)$ idempotent, and $K/J(R) = \bar{a}(R/J(R))$. Since $K = I + J(R)$, we can suppose $a \in I$. Note that $aI \leq I$ is a right ideal. If we can show $K = aI + J(R)$, then the minimality implies $aI = I$ and hence by Lemma 14.32 we have $I = eR$ for an idempotent $e \in R$.

Let $x \in K$ be arbitrary, and note we can write $\bar{x} = \bar{a}\bar{r} = \bar{a}\bar{a}\bar{r}$ in $K/J(R)$ from what we showed above (remembering that $\bar{a}$ is idempotent). Thus

$$x \in aaR + J(R) \subset aI + J(R)$$

Since x was arbitrary, and $aI + J(R) \leq I + J(R) = K$, we have containment both ways, and thus $K = aI + J(R)$.

[14.13] First, suppose $SI \neq 0$. Then there is some $s \in S$ with $sI \neq 0$, and since this is a submodule and S is simple, we have $sI = S$. The map $\theta : I \rightarrow S$ given by $\theta(x) = sx$ is a surjective homomorphism.

Conversely suppose we have this surjective homomorphism $\theta : I \rightarrow S$. Corollary 14.33 shows $I = eR$ for an idempotent e . Let $s = \theta(e)$. We can't have $s = 0$, since then $\theta(I) = \theta(e)R = \{0\}$. But then we have

$$0 \neq s = \theta(e) = \theta(ee) = \theta(e)e = se$$

So $s \in SI$.

[14.14] We prove the following, which implies the problem statement: if U is of finite composition length and I is a minimally potent right ideal of R , then U has $I/M(I)$ as a composition factor if and only if $UI \neq 0$. This suffices because every simple module is a quotient $I/M(I)$ for some minimally potent right ideal, by Theorem 14.31 and Corollary 14.37.

If U has two submodules $N \leq W$ with $W/N \cong I/M(I)$, then $WI \not\subseteq N$ by the previous problem, so we must have $UI \neq 0$.

To prove the converse, we induct on the composition length of U . The case where U is simple is exactly the previous problem. Now let $\ell(U) = n + 1$, and assume our result is true for composition lengths $\leq n$.

If $UI \neq 0$, then let $N \leq U$ be a maximal submodule. If $NI \neq 0$, then the inductive hypothesis shows N (and hence U) has a composition factor isomorphic to $I/M(I)$. If $NI = 0$, but $(U/N)I \neq 0$, then we're back in the simple case of the previous problem, showing $U/N \cong I/M(I)$. If $NI = (U/N)I = 0$, then with $I = eR$, we have $Uee \subset Ne = \{0\}$. Since e is idempotent, we have $Ue = \{0\}$, but then $UI = UeR = \{0\}$, a contradiction.

[14.15] It seems likely that we need to assume R is right Artinian, so we do that.

- (a) Note that $IA, IB \subset I$, but since $R = A + B$, we have in fact $IA + IB = I$. Since $IA \subset A$ and $IB \subset B$, this is actually a direct sum decomposition: $I = IA \oplus IB$. But I is minimally potent, hence indecomposable, so either $IA = 0$ or $IB = 0$. In the first case $I = IB \subset B$, and the second case similarly yields $I \subset A$.
- (b) By the previous problem, for A and B to have a composition factor in common, there would have to be a minimally potent ideal I with $AI \neq 0$ and $BI \neq 0$. By part (a), either $I \subset A$ or $I \subset B$. In the first case, $BI \subset A \cap B = \{0\}$, and the second case yields a similar result. Thus A and B have no composition factor in common.

[14.16] Let $u_x \in U$ be the matrix with x in the upper-right corner, and similarly define $v_x \in V$, for $x \in K$. We have

$$\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & xd \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & xd \end{pmatrix}$$

This shows U and V are right ideals, and that the map $u_x \mapsto v_x$ is an R -module isomorphism. Note there can't be any non-zero right ideals J contained in V : $v_x v_y = v_{xy}$, so if $v_x \in J$ with $x \neq 0$, then since K is a field, all of V is contained in J . Now $v_1^n = v_1$ for all $n > 0$, so V cannot be nilpotent, and so it is minimally potent. But $u_x u_y = 0$ for every $u_x, u_y \in U$, so $U^2 = 0$ and U is nilpotent.

Chapter 15

[15.1]

- (a) If $\theta : G \rightarrow G/N$ is the canonical homomorphism, and Ψ is the representation of G/N affording the character ψ , then $\theta\Psi$ is a representation of G . If χ is the character afforded by this representation, we have

$$\chi(g) = \text{Tr}(\Psi(\theta(g))) = \text{Tr}(\Psi(Ng)) = \psi(Ng)$$

- (b) Now that we know χ is a character of G , we can just compute its inner product with itself ($T \subset G$ is a transversal of N in G):

$$\begin{aligned} \langle \chi, \chi \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \psi(Ng) \overline{\psi(Ng)} \\ &= \frac{|N|}{|G|} \sum_{t \in T} \psi(Nt) \overline{\psi(Nt)} \\ &= \frac{1}{[G : N]} \sum_{x \in G/N} \psi(x) \overline{\psi(x)} \\ &= \langle \psi, \psi \rangle_{G/N} \end{aligned}$$

Since this inner product is 1 precisely when χ is irreducible, we are done.

[15.2]

Let X be a representation of G affording χ . As in the proof of Lemma 15.17, we know N is contained in $\ker(\chi) = \ker(X)$, and thus there is an induced homomorphism Ψ on G/N , with $\Psi(Ng) = X(g)$. We can now compute the character of this representation on G/N :

$$\psi(Ng) = \text{Tr}(\Psi(Ng)) = \text{Tr}(X(g)) = \chi(g)$$

[15.3]

The previous two problems have established there is an one-to-one correspondence between $\mathcal{N}$ and $\text{Irr}(G/N)$, given by mapping $\chi \in \mathcal{N}$ to the character ψ of G/N , with $\psi(Ng) = \chi(g)$.

- (a) Of course, by definition N is contained in the kernel of every character in $\mathcal{N}$. Suppose $g \in G$ was contained in the kernel of every element of $\mathcal{N}$. Then Ng is contained in the kernel of every element of $\text{Irr}(G/N)$, and hence $Ng = N$; that is, $g \in N$.

- (b) We have

$$\sum_{\chi \in \mathcal{N}} \chi(1)^2 = \sum_{\psi \in \text{Irr}(G/N)} \psi(N)^2 = |G/N| = [G : N]$$

[15.4] First, suppose $z \in Z(\chi)$ for every $\chi \in \text{Irr}(G)$. Then we have from Lemma 15.17 that $zK \in Z(G/K)$ for $K = \ker(\chi)$ for every such χ . By Corollary 15.18, the intersection of all these K is trivial, and thus we have a canonical injective homomorphism $G \rightarrow \prod_{\chi \in \text{Irr}(G)} G / \ker(\chi)$. Since z ends up in the center of this product, it certainly commutes with all elements of (the embedded) G , so that $z \in Z(G)$.

Conversely, let $\chi \in \text{Irr}(G)$, and X be a representation affording χ . By Lemma 15.10, X maps $\mathbb{C}G$ onto $M_n(\mathbb{C})$. Thus for $z \in Z(G)$, $X(z)$ commutes with all of $M_n(\mathbb{C})$, and hence it is a scalar matrix ϵI . We thus have $|\chi(z)| = n = \chi(1)$ so that $z \in Z(\chi)$.

[15.5] If G is Abelian, then $\mathbb{C}G$ is Abelian. Let $\chi \in \text{Irr}(G)$ and X be a representation affording χ . Since $X : \mathbb{C}G \rightarrow M_n(\mathbb{C})$ is onto by Lemma 15.10 (with $n = \chi(1)$), we must have that $M_n(\mathbb{C})$ is Abelian. Hence $n = 1$ and the arbitrary character χ is linear.

Conversely, suppose $\chi(1) = 1$ for all $\chi \in \text{Irr}(G)$. Then $g \in Z(\chi)$ for all $g \in G$. By the previous problem, since χ was arbitrary, we have that $Z(G) = G$, so that G is Abelian.

[15.6] If χ is a linear character of G , then $G' \leq \ker(\chi)$ since $M_1(\mathbb{C}) = \mathbb{C}^*$ is Abelian. Meanwhile, if $G' \leq \ker(\chi)$, then by [15.2] we have an induced character on G/G' , which must be linear by the previous problem. Thus we have that $\mathcal{L}$, the linear characters of G , are precisely those with $G' \leq \ker(\chi)$. By [15.3] part (b) we have that (noting $\chi(1)^2 = 1$ for a linear character) $[G : G'] = |\mathcal{L}|$.

[15.7] We write $\chi = \sum \alpha_i \psi_i$ as a linear combination of irreducible characters, and compute

$$\langle \chi, \chi \rangle = \sum \alpha_i^2$$

relying on the fact the $\{\psi_i\}$ are an orthonormal set. Because our group is Abelian, we have $\psi_i(1) = 1$ for all i , and hence $\chi(1) = \sum \alpha_i$. Since χ is a character, the α_i are non-negative integers, so that $\alpha_i^2 \geq \alpha_i$ for all i , and we are done.

[15.8] Let $D = H \rtimes C$, where $H = \langle h \rangle$ is cyclic of order n , and $C = \langle c \rangle$ is cyclic of order 2, with $h^c = h^{-1}$. There are thus $\frac{n+1}{2}$ conjugacy classes contained in H : 1 for the identity, and then $\frac{n-1}{2}$ of size 2, all looking like $\{a, a^{-1}\}$. Since c is self-centralizing, it has $[D : C] = n$ conjugates, so the elements of $D \setminus H$ form one conjugacy class, and we have $\frac{n+3}{2}$ altogether.

Because $[c, h] = h^2$, and n is odd, we see that $H \leq D'$. Of course, D/H is Abelian (of order 2), so $H = D'$. By [15.6], D has 2 linear characters. The other $\frac{n-1}{2}$ irreducible characters have degree at least 2; but

$$2 + \frac{n-1}{2} \cdot 2^2 = 2n$$

and thus by Corollary 15.7 it must be that all non-linear irreducible characters of D have degree exactly 2.

[15.9] Let θ° be the extension of θ to G , sending everything in $G \setminus H$ to 0. For $x \in G$ and $h \in H$, note that $hxh^{-1} \in H$ precisely when $x \in H$, and thus (since θ is a class function on H) we

always have $\theta^\circ(hxh^{-1}) = \theta^\circ(x)$. This allows us to write (with T a right transversal of H in G):

$$\begin{aligned}\theta^G(x) &= \frac{1}{|H|} \sum_{g \in G} \theta^\circ(gxg^{-1}) \\ &= \frac{1}{|H|} \sum_{h \in H} \sum_{t \in T} \theta^\circ(htxt^{-1}h^{-1}) \\ &= \frac{1}{|H|} \sum_{h \in H} \sum_{t \in T} \theta^\circ(txt^{-1}) \\ &= \sum_{t \in T} \theta^\circ(txt^{-1})\end{aligned}$$

Since $|\theta(h)| \leq \theta(1)$, we certainly have $|\theta^\circ(x)| \leq \theta(1)$. Thus

$$|\theta^G(x)| = \left| \sum_{t \in T} \theta^\circ(txt^{-1}) \right| \leq \sum_{t \in T} |\theta^\circ(txt^{-1})| \leq |T|\theta(1) = \theta^G(1)$$

For equality to hold (so that $x \in Z(\theta^G)$), we must have $|\theta^\circ(txt^{-1})| = \theta(1)$ for each $t \in T$. In particular, for $t \in T \cap H$, we then have

$$|\theta^\circ(txt^{-1})| = |\theta^\circ(x)| = \theta(1) > 0$$

so that $x \in H$.

[15.10] We first prove a result about the different ways to write an element $g \in G = HK$ as a product hk . To that end, let the group $H \times K$ act on the set HK on the right, via

$$x \cdot (h, k) = h^{-1}xk$$

Then this action is transitive, and the stabilizer of $1 \in HK$ is the diagonal subgroup D of $(H \cap K) \times (H \cap K)$. Thus the ways to write $g = hk$ are given by the right coset $D(h^{-1}, k)$, which has $|D| = |H \cap K|$ elements, and in particular all the ways to write g are as $(h\alpha^{-1})(\alpha k)$ for $\alpha \in H \cap K$.

Now let $x \in K$, and we compute:

$$\begin{aligned}\phi^G(x) &= \frac{1}{|H|} \sum_{g \in G} \phi^\circ(gxg^{-1}) \\ &= \frac{1}{|H| \cdot |H \cap K|} \sum_{h \in H} \sum_{k \in K} \phi^\circ(hkxk^{-1}h^{-1}) \\ &= \frac{1}{|H| \cdot |H \cap K|} \sum_{h \in H} \sum_{k \in K} \phi^\circ(kxk^{-1}) \\ &= \frac{1}{|H \cap K|} \sum_{k \in K} \phi^\circ(kxk^{-1})\end{aligned}$$

Now since $kxk^{-1} \in K$, we know that $kxk^{-1} \in H$ if and only if $kxk^{-1} \in H \cap K$, and thus $\phi^\circ(kxk^{-1}) = \phi_{H \cap K}^\circ(kxk^{-1})$. So the above expression is nothing more than $\phi_{H \cap K}^K(x)$, as desired.

[15.11] Let X be a representation affording the character χ , with $n = \chi(1)$. Since χ is irreducible, we know by Lemma 15.10 that $X : \mathbb{C}G \rightarrow M_n(\mathbb{C})$ is onto, and thus $X(z)$ is a scalar matrix, say $\epsilon_z I$, for every $z \in Z(G)$. For $g \in G$ then, we have

$$|\chi(gz)|^2 = |\text{Tr}(X(gz))|^2 = |\text{Tr}(X(g)X(z))|^2 = |\text{Tr}(\epsilon_z X(g))|^2 = |\epsilon_z \text{Tr}(X(g))|^2 = |\chi(g)|^2$$

where the last equality follows because ϵ_z is a root of unity. If T is a transversal of H in G , such that $T \subset Z(G)$, then we can thus compute

$$\begin{aligned} \langle \chi, \chi \rangle_G &= \frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2 \\ &= \frac{1}{|G|} \sum_{h \in H} \sum_{t \in T} |\chi(ht)|^2 \\ &= \frac{1}{|G|} \sum_{h \in H} \sum_{t \in T} |\chi(h)|^2 \\ &= \frac{1}{|H|} \sum_{h \in H} |\chi(h)|^2 \\ &= \langle \chi_H, \chi_H \rangle_H \end{aligned}$$

Since χ_H is a character of H , and $\langle \chi, \chi \rangle_G = 1$ by hypothesis, we see that χ_H is irreducible.

[15.12]

(a) We have

$$\langle \chi, \chi \rangle_G = \frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2 \geq \frac{1}{|G|} \sum_{h \in H} |\chi(h)|^2 = \frac{1}{n|H|} \sum_{h \in H} |\chi(h)|^2 = \frac{1}{n} \langle \chi_H, \chi_H \rangle_H$$

(b) If H is Abelian, then we know from [15.7] that

$$\chi(1) = \chi_H(1) \leq \langle \chi_H, \chi_H \rangle_H \leq n \langle \chi, \chi \rangle_G = n$$

with the last equality following because $\chi \in \text{Irr}(G)$.

(c) We ignore the case $|G| = 1$ since that's trivially true. If equality holds in the above, then we must have $\langle \chi_H, \chi_H \rangle_H = n$. Equality must also hold in part (a), and from the fact $|\chi(g)|^2 \geq 0$ for all $g \in G$, we know that $\chi(g) = 0$ for $g \notin H$. If we set N to be the subgroup (of H) generated by elements $h \in H$ with $\chi(h) \neq 0$, then N is the union of conjugacy classes (since χ is a class function), hence normal. It is also contained in H , hence Abelian. It is not trivial, since otherwise we would have $\chi(g) = 0$ for all

non-trivial $g \in G$, so that χ is a multiple of the permutation character, which is not irreducible for non-trivial G .

However, the problem statement is wrong, in that H need not be normal in G . A counterexample is when G is of order 54, written as a semidirect product $P \rtimes C$, with P a non-Abelian group of order 27 and exponent 3, and C a group of order 2 acting on P . Specifically, let

$$P = \langle x, y, z \mid x^3 = y^3 = z^3 = 1, [x, y] = z, [x, z] = [y, z] = 1 \rangle$$

Then $C = \langle c \mid c^2 = 1 \rangle$ with the non-trivial c acting by swapping x and y . This also means $z^c = z^2$. The presentation above also shows $x^y = xz$ and $y^x = yz^2$. If we let $H = \langle x, z \rangle$, then H is elementary Abelian of order 9. Let χ be the character of H with $\chi(z) = \lambda$ and $\chi(x) = 1$, with λ a primitive third root of unity. It can be checked that χ^G is actually irreducible, of degree $6 = [G : H]$. However, H is not normal in G , because $x \in H$ but $x^c = y \notin H$. In this case, the N constructed in the solution above is $\langle z \rangle = Z(P)$.

To see the statement about χ^G , note that since $P \triangleleft G$, we have $\chi^G(g) = 0$ for $g \notin P$. Now every element of P can be written as $x^\alpha y^\beta z^\gamma$ with $0 \leq \alpha, \beta, \gamma < 3$. Let $S \cup T$ be a transversal for H in G , with $S = \{1, y, y^2\}$ and $T = \{c, cy, cy^2\}$. Since S fixes y , and $y \notin H$, it can be checked that

$$\sum_{s \in S} \chi^\circ(s^{-1} x^\alpha y^\beta z^\gamma s) = \begin{cases} 0 & \beta \neq 0 \\ \lambda^\gamma + \lambda^{\alpha+\gamma} + \lambda^{2\alpha+\gamma} & \beta = 0 \end{cases}$$

Since c swaps x and y , a similar statement holds for T and α :

$$\sum_{t \in T} \chi^\circ(t^{-1} x^\alpha y^\beta z^\gamma t) = \begin{cases} 0 & \alpha \neq 0 \\ \lambda^{2\gamma} + \lambda^{\beta+2\gamma} + \lambda^{2\beta+2\gamma} & \alpha = 0 \end{cases}$$

Of course, if $\alpha \neq 0$, then $\lambda^\gamma + \lambda^{\alpha+\gamma} + \lambda^{2\alpha+\gamma} = 0$ (and a similar statement holds for β). Meanwhile, if $\alpha = 0$, then the above sum is just $3\lambda^\gamma$. Together with the fact that $\lambda^\gamma + \lambda^{2\gamma} = -1$ when $\gamma \neq 0$, we finally have

$$\chi^G(x^\alpha y^\beta z^\gamma) = \sum_{r \in S \cup T} \chi^\circ(r^{-1} x^\alpha y^\beta z^\gamma r) = \begin{cases} 0 & \alpha \neq 0 \neq \beta \\ 0 & \alpha = 0, \beta \neq 0 \\ 0 & \alpha \neq 0, \beta = 0 \\ -3 & \alpha = 0 = \beta, \gamma \neq 0 \\ 6 & \alpha = \beta = \gamma = 0 \end{cases}$$

We can then compute

$$\langle \chi^G, \chi^G \rangle = \frac{1}{|G|} \sum_{g \in G} \chi^G(g) = \frac{6^2 + (-3)^2 + (-3)^2}{54} = 1$$

so that χ^G is irreducible.

[15.13] Let $[G : H] = n$. Then from part (b) of the previous problem, we have $\chi(1) \leq n$ for all $\chi \in \text{Irr}(G)$. Thus we have

$$|G| = \sum_{\chi \in \text{Irr}(G)} \chi(1)^2 \leq n^2 |\text{Irr}(G)|$$

This shows $|\text{Irr}(G)| \geq |H|^2/|G|$; since $|\text{Irr}(G)|$ is the number of conjugacy classes, we're done.

Chapter 16

[16.1] Consider the map $\phi : \mathbb{Z}[x] \rightarrow \mathbb{C}$ given by sending $x \mapsto \alpha$. If we can show $R = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$ is a ring, then R is in the image of ϕ , but $\phi(x) \in R$, so we actually have R is the image of ϕ as desired.

R is clearly closed under addition, and it inherits associativity and distributivity from $\mathbb{C}$. So we only need to show it's closed under products. But

$$(a + b\alpha)(c + d\alpha) = (ac + bdn) + (ad + bc)\alpha \in R$$

[16.2] For $a + bi\sqrt{5} = r \in R$, we have $|r|^2 = a^2 + 5b^2 \in \mathbb{Z}$. Note that $|r| = 1$ implies $r = \pm 1$ (in particular r is a unit), and there are no $r \in R$ with $|r|^2 \in \{2, 3\}$.

Since $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, we can show R is not a UFD by showing these are two distinct irreducible decompositions of 6. We have

$$\begin{aligned} |2|^2 &= 4 \\ |3|^2 &= 9 \\ |1 + i\sqrt{5}|^2 &= 6 \\ |1 - i\sqrt{5}|^2 &= 6 \end{aligned}$$

So all of these are irreducible. For example, if $1 + i\sqrt{5} = uv$, then since the norm is multiplicative, we must have $|u|^2$ and $|v|^2$ divide 6. From the previous paragraph that implies one has norm 6, and thus the other has norm 1, so is a unit.

To finish showing R is not a UFD, we need to show these primes aren't associates (related by units). But 2 has the smallest norm, so can't be divisible by any of the other elements, so we're done.

[16.3] We know we can write $\alpha = a/b$ for $a, b \in R$. Let

$$\begin{aligned} a &= up_1p_2 \cdots p_m \\ b &= vq_1q_2 \cdots q_n \end{aligned}$$

If q_1 divides a , then it divides one of the p_i , which we can assume is p_1 . By uniqueness of factorizations, we can modify the unit u so that $p_1 = q_1$. We then proceed with a/p_1 and b/q_1 , continuing this process until none of the remaining q_i divide a . Suppose after this process $p_i = q_i$ for $i \leq k$. Define

$$\begin{aligned}\hat{a} &= up_{k+1} \cdots p_m \\ \hat{b} &= vq_{k+1} \cdots q_n\end{aligned}$$

Then since $\hat{a}\hat{b} = b\hat{a}$, we see that $\alpha = \hat{a}/\hat{b}$, and these are coprime.

[16.4] Write $\alpha = a/b$ where a and b are coprime, as in the last problem. If $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c + 0$, then from $f(\alpha) = 0$ we have (after clearing denominators)

$$0 = a^n + c_{n-1}ba^{n-1} + \cdots + c_0b^n = a^n + b(\cdots)$$

This implies b divides a^n . If p is a prime dividing b , then p divides a , contradicting our coprime assumption. So no prime divides b , and it is then a unit, so $\alpha = ab^{-1} \in R$.

[16.5] Suppose for contradiction that the irreducibles of $F[x]$ all had degree at most n . Since there are only finitely many polynomials in $F[x]$ of degree at most n (this uses that F is finite), we can form their product $p(x)$, which is still a polynomial. Then $p(x) + 1$ is not divisible by any irreducible, but it has positive degree, so it cannot be a unit. This contradicts $F[x]$ being a UFD, so there must be irreducibles of arbitrarily high degree.

[16.6] Let I be an ideal of R ; we want to show it is principal. We prove this by induction on the number of generators of I , the base case of I already principal being trivial. Assuming the induction hypothesis, let I be generated by $n + 1$ generators, with all ideals generated by at most n generators being principal. If $a, b \in I$ are two of those generators, write both as products of primes, and let c be the product of the common primes (as in [16.3]). Then by hypothesis there exists u and v such that

$$\left(\frac{a}{c}\right)u + \left(\frac{b}{c}\right)v = 1$$

But then $au + bv = c$, and since c divides both a and b , we have $(a, b) = (c)$. Thus I can be generated by n elements (replace a and b by c), and so by induction I is principal.

[16.7]

(a) Write $\alpha = a/b$ for coprime a and b (as in [16.3]). Then Lemma 16.29 implies there exists $u, v \in R$ with $au + bv = 1$. This implies

$$\frac{1}{b} = \alpha u + v \in S$$

- (b) Let I be an ideal of S . Since $I \cap R$ is an ideal of R , it is principal, say generated by $r \in R$. Let $J = (r) \leq S$, so that $J \leq I$. Now if $a/b \in I$, we have $a = (a/b)b \in I \cap R$, so that $a \in J$. But then $a(1/b) \in J$ by part (a), so that $I \leq J$ and we're done.

[16.8] Write $a = bx$ and $b = ay$. Thus $a = axy$ and $a(1 - xy) = 0$. If M is the unique maximal ideal of R , then if $1 - xy \in M$, we must have $xy \notin M$ (since otherwise $1 \in M$), so that xy is a unit, implying y is also a unit, and we're done. If instead $1 - xy \notin M$, then it's a unit, and hence $a(1 - xy) = 0$ implies $a = 0$. This means $b = 0$, and so of course $b = 1a$, and we're again done.

[16.9] $f(x)$ and $g(x)$ are clearly continuous. We have $f = gh$ and $g = fh$ with

$$h(x) = \begin{cases} -1 & -1 \leq x \leq -\frac{1}{2} \\ 2x & -\frac{1}{2} \leq x \leq \frac{1}{2} \\ 1 & \frac{1}{2} \leq x \leq 1 \end{cases}$$

Suppose $g = uf$ for $u(x)$ a unit; this means $u(x)$ is never zero, so by continuity it is always positive or always negative. If it's always positive, then we would have $g(-1) = u(-1)f(-1) < 0$, which is a contradiction. A similar contradiction holds (for $g(1)$) if $u(x)$ is assumed always negative.

[16.10] Write $f(X) = a(X)b(X)$ with $a, b \in E[X]$. By Gauss's Lemma, we can write $f(X) = A(X)B(X)$ for $A, B \in F[Y][X] = F[X, Y]$, with $A(X) = \alpha \cdot a(X)$ and $B(X) = \beta \cdot b(X)$ for $\alpha, \beta \in E$. Since $\deg_Y f = 1$, it must be that one of $A(X)$ or $B(X)$ has no Y terms. Then $A(X)$ divides both $g(X)$ and $h(X)$ in $F[X]$, so it is in fact a constant in F . Then $a(x)$ is a constant in E . This shows $f(x)$ is irreducible in $E[X]$.

[16.11]

- (a) Since $\theta(b)$ is invertible in S , We certainly have $\{\theta(a)/\theta(b) \mid a \in P, b \notin P\} \subset Q$. But the former is an ideal of S containing $\theta(P)$, so is equal to Q . To see it's an ideal, note

$$\begin{aligned} \theta(a)/\theta(b) + \theta(c)/\theta(d) &= \theta(ad + bc)/\theta(bd) \\ \theta(a)/\theta(b) \cdot \theta(c)/\theta(d) &= \theta(ac)/\theta(bd) \end{aligned}$$

and $ad + bc, ac \in P$ since it's an ideal, and $bd \notin P$ since $b, d \notin P$ and P is prime.

- (b) If $a, b \in R$ with $ab = 0$ and $b \notin P$, then $a \in P$ because P is prime. This shows $\ker(\theta) \leq P$. Now suppose $\theta(a)/\theta(b) \in Q$ is invertible in S . That means we have $r \in R$ and $d \in M$ such that $\theta(ar) = \theta(bd)$. But $ar \in P$ and $bd \notin P$, and that contradicts the fact $ar - bd \in \ker(\theta) \leq P$. So no element of Q is invertible. Meanwhile, an element $\theta(r)/\theta(d)$ with $r, d \notin P$ is invertible, with inverse $\theta(d)/\theta(r)$. So Q is the ideal of all non-units, and hence the unique maximal ideal.

[16.12]

- (a) Let $x \in R$ be its unit, so that $x^2 = x$. In E , this implies $x = 0$ or $x = 1$, and R is not the zero ring, so $x = 1$ and R is unitary.

- (b) Consider the set $F = \{rs^{-1} \mid r, s \in R, s \neq 0\} \subset E$. This is a subring of E via the usual ideas (and unitary by part (a)):

$$\begin{aligned} rs^{-1} + uv^{-1} &= (rv + us)(sv)^{-1} \\ rs^{-1} \cdot uv^{-1} &= (ru)(sv)^{-1} \end{aligned}$$

Every nonzero element of F is invertible in E (and that inverse is contained in F), so F is a field. Its construction shows it is a field of fractions for R . To show F is unique, note that for any subfield $K \leq E$ that contains R , it must necessarily also contain F . Thus F is the unique smallest subfield of E containing R .

- [16.13] Let $\tau \in S_n$. Define a map $\phi : R \rightarrow R$ by sending X_i to $X_{\tau(i)}$ and fixing F pointwise. This is a ring homomorphism, since it just sends $f(X_1, \dots, X_n) \mapsto f(X_{\tau(1)}, \dots, X_{\tau(n)})$. It is an isomorphism since it's invertible (just use τ^{-1}). By Theorem 16.24, ϕ extends to a (unique) isomorphism $\sigma : E \rightarrow E$, which fixes F and permutes the X_i .

Chapter 17

[17.1]

- (a) The map $\alpha \mapsto \alpha^p$ is an additive group homomorphism since $(\alpha + \beta)^p = \alpha^p + \beta^p$. It is then injective since $\alpha^p = 0$ implies $\alpha = 0$. If F is finite, the map must also be surjective.
- (b) Suppose $X = \alpha^p$ for $\alpha \in F(X)$. This implies

$$\begin{aligned} X &= \frac{f(X)^p}{g(X)^p} \\ &= \frac{f(X^p)}{g(X^p)} \\ Xg(X^p) &= f(X^p) \\ p \deg(g) + 1 &= p \deg(f) \end{aligned}$$

And this last line is impossible (modulo p). Thus X is not a p th power in $F(X)$, so it is not a perfect field.

[17.2]

Let $L \supset E$ be a field containing a root α of $f(x)$. If $f(x)$ is not irreducible over $E[x]$, then it is the product of several irreducibles all of degree $< p$, so that $[E[\alpha] : E] < p$. If $[E : F]$ is not divisible by p , then neither is

$$[E[\alpha] : E] \cdot [E : F] = [E[\alpha] : F] = [E[\alpha] : F[\alpha]] \cdot [F[\alpha] : F]$$

And this is a contradiction because $[F[\alpha] : F] = \deg(f) = p$. This contradiction shows p does divide $[E : F]$.

[17.3]

- (a) Let $K \supset L$ contain $\beta \in K$ such that $f(\beta) = 0$. If we write $g(x) \in F[x]$ as the minimal polynomial of α , then $f(x)$ divides $g(x)$ in $E[x]$, so $g(\beta) = 0$. Thus β is algebraic over F .
- (b) Let K as above be a splitting field for $f(x)$. Then part (a) shows the roots $\alpha_0, \alpha_1, \dots$ are algebraic over F , and thus $M := F[\alpha_0, \alpha_1, \dots]$ is a finite extension of F . But the coefficients are combinations of these roots, and so live in M , and hence are algebraic over F .

[17.4] Let $L \supset E$ be a splitting field for $f(x)$ over E . Then if $\alpha \in L$ is a root of $f(x)$, we can let $g(x) \in E[x]$ be the minimal polynomial for α over E . Since $f(\alpha) = 0$, part (b) of the previous problem shows all the coefficients of $g(x)$ are algebraic over F . Since $F \subset E$ is totally transcendental, this implies all the coefficients of $g(x)$ are in F , so that $g(x) \in F[x]$. Since $g(x)$ divides $f(x)$, irreducibility implies $g(x) = cf(x)$ for some $c \in F$. Since $g(x) \in E[x]$ is irreducible, this shows $f(x)$ is irreducible over $E[x]$ as well.

[17.5] Write $g(x) = f(x)h(x)$ for $h(x) \in E[x]$. We have

$$\begin{aligned} f(x) &= \sum_{i=0}^k a_i x^i \\ g(x) &= \sum_{i=0}^m b_i x^i \\ h(x) &= \sum_{i=0}^n c_i x^i \end{aligned}$$

We must have $m = n + k$. Now the coefficient of x^{n+k} in $g(x) = f(x)h(x)$ is then $b_m = a_k c_n$. This shows that $c_n = b_m / a_k \in F$. Suppose we've shown that $c_j \in F$ for $n \geq j > r$. Then the coefficient of x^{r+k} in $g(x)$ is

$$b_{r+k} = c_r a_k + (c_{r+1} a_{k-1} + \dots + a_{r+k-n} c_n)$$

The expression in parentheses is in F , and so is b_{r+k} and $a_k \neq 0$. This implies $c_r \in F$, and we can continue this process all the way to $r = k$ to conclude that $h(x) \in F[x]$.

[17.6]

- (a) Since both α and $\alpha\epsilon$ are roots of $f(x)$, we see that $\mathbb{Q}[\alpha, \epsilon] \subset E$. Meanwhile, $\{\alpha\epsilon^k\}$ for $0 \leq k < p$ are all the roots of $f(x)$, so we must actually have equality: $E = \mathbb{Q}[\alpha, \epsilon]$.
- (b) Let $g(x) = x^{p-1} + x^{p-2} + \dots + 1$. Since

$$x^p - 1 = (x - 1)g(x)$$

and $\epsilon^p = 1$, we know that $g(\epsilon) = 0$. As noted, $g(x)$ is irreducible, so it must be the minimal polynomial for ϵ over $\mathbb{Q}$.

- (c) Because both $\mathbb{Q}[\alpha] \subset E$ and $\mathbb{Q}[\epsilon] \subset E$, we know that both p and $p - 1$ divide $[E : \mathbb{Q}]$. These are relatively prime, so $p(p - 1)$ divides $[E : \mathbb{Q}]$. The chain of fields

$$\mathbb{Q} < \mathbb{Q}[\alpha] < \mathbb{Q}[\alpha][\epsilon] = E$$

shows $[E : \mathbb{Q}] \leq p(p - 1)$, because the minimal polynomial of ϵ over $\mathbb{Q}[\alpha]$ divides $g(x)$, so has degree at most $p - 1$. From what was shown before, we must have equality: $[E : \mathbb{Q}] = p(p - 1)$.

[17.7] Let $L \supset F$ be a splitting field for $f(x)$. If $f(\alpha) = 0$ for $\alpha \in L$, then since $f(x) = (x - \alpha)^p$, we see that $L = F[\alpha]$. The minimal polynomial $g(x) \in F[x]$ for α divides $f(x)$, and $[L : F] = \deg(g)$.

If $f(x) = g(x)h(x)$ for $h(x) \in F[x]$, then the only possible roots for $h(x)$ are α (since roots of $h(x)$ are roots of $f(x)$). So if $h(x)$ is non-constant, it must be divisible by $g(x)$. Unique factorization then shows we actually have

$$f(x) = cg(x)^d$$

for some $c \in F$. Because this implies d and $\deg(g)$ divide $\deg(f) = p$, either $d = 1$ (so $f(x)$ is irreducible), or $\deg(g) = 1$, and $L = F$.

[17.8] Choose $E \subset \mathbb{C}$ such that $E \supset F$ is a splitting field for $f(x)$. If $\alpha \in E$ is such that $f(\alpha) = 0$, then note that $f(\alpha\epsilon^k) = 0$ for $0 \leq k < p$. Since $\epsilon \in F$, we have $E = F[\alpha]$. If $g(x) \in F[x]$ is the minimal polynomial for α , then $[E : F] = \deg(g)$.

If $f(x) = g(x)h(x)$ for $h(x) \in F[x]$, then the only possible roots for $h(x)$ look like $\alpha\epsilon^k$. So if $h(x)$ is non-constant and has root $\alpha\epsilon^r$, then the irreducible polynomial $g(\epsilon^{-r}x)$ must divide $h(x)$. Unique factorization then shows we actually have

$$f(x) = cg(\epsilon^{-r_1}x) \cdots g(\epsilon^{-r_m}x)$$

for some $c \in F$. Because this implies $\deg(g)$ divides $\deg(f) = p$, we must have either $\deg(g) = p$ (so that $f(x)$ is irreducible) or $\deg(g) = 1$ (so that $E = F$).

[17.9]

- (a) Note that

$$2 = (\alpha - \sqrt{3})^3 = \alpha^3 + 9\alpha - \sqrt{3}(3\alpha^2 + 3)$$

And this then implies

$$\sqrt{3} = \frac{\alpha^3 + 9\alpha - 2}{3(\alpha^2 + 1)} \quad (\star)$$

Since $\alpha \in \mathbb{R}$, we know the denominator above is nonzero. This shows that $\sqrt{3} \in \mathbb{Q}[\alpha]$, and so of course then $\sqrt[3]{2} = \alpha - \sqrt{3} \in \mathbb{Q}[\alpha]$. The other containment direction is obvious, so $\mathbb{Q}[\sqrt{3}, \sqrt[3]{2}] = \mathbb{Q}[\alpha]$.

- (b) Squaring both sides of the equation $(\star)$ above, and then clearing denominators, we see that α is a root of the polynomial

$$f(x) = x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23 \in \mathbb{Q}[x]$$

This shows that $[\mathbb{Q}[\alpha] : \mathbb{Q}] \leq 6$. Since both $\mathbb{Q}[\sqrt{3}]$ and $\mathbb{Q}[\sqrt[3]{2}]$ are subfields of $\mathbb{Q}[\alpha]$, and since they have degrees 2 and 3 over $\mathbb{Q}$ respectively, we know both 2 and 3 divide $[\mathbb{Q}[\alpha] : \mathbb{Q}]$. We thus have $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 6$, and since $f(x)$ has degree 6, is monic, and has α as a root, it must be the minimal polynomial for α over $\mathbb{Q}$, and hence is irreducible.

[17.10]

- (a) We have that $\alpha^2 - 2 = \sqrt{2}$, and hence (squaring both sides) that α is a root of

$$f(x) = x^4 - 4x^2 + 2$$

By Eisenstein's criterion (with prime 2) we know that $f(x)$ is irreducible, so that it's the minimal polynomial for α over $\mathbb{Q}$.

- (b) Note that $\beta = \sqrt{2 - \sqrt{2}}$ is also a root of $f(x)$, since $(\beta^2 - 2)^2$ is also equal to 2. So the roots of $f(x)$ are then $\{\pm\alpha, \pm\beta\}$. But we have that $\alpha\beta = \sqrt{2}$ so that

$$\beta = \frac{\sqrt{2}}{\alpha} = \frac{\alpha^2 - 2}{\alpha} \in \mathbb{Q}(\alpha)$$

And this shows that the splitting field $E = \mathbb{Q}[\alpha]$, so that $[E : \mathbb{Q}] = \deg(f) = 4$.

[17.11]

- (a) We show containment $F(\alpha)(\beta) \subset F(\beta)(\alpha)$, the reverse containment following via symmetry. Now $F(\alpha)(\beta)$ is by definition the smallest subfield of E that contains both $F(\alpha)$ and β . But $F(\beta)(\alpha)$ contains $F(\beta)$, and since $F \subset F(\beta)$, it also contains $F(\alpha)$.
- (b) We will show that if β is algebraic over $F(\alpha)$, then α is algebraic over $F(\beta)$; the reverse direction follows by symmetry. So suppose β is the root of a polynomial in $F(\alpha)[x]$; we can then write

$$p_m(\alpha)\beta^m + \cdots + p_0(\alpha) = 0$$

where the p_i are rational functions of α . After clearing denominators, we can assume that each $p_i(x) \in F[x]$. Consider then the polynomial

$$f(x, y) = p_m(x)y^m + \cdots + p_0(x) \in F[y, x]$$

$\deg_y(f) = m > 0$ so that f is not the zero polynomial. Because β is transcendental over F , the map $F[y, x] \rightarrow F[\beta, x]$ given by setting $y = \beta$ is an isomorphism, and $f(x, \beta) \neq 0$. Finally, note that at least one of the p_i must be non-constant, since otherwise we would have β algebraic over F , which contradicts our hypotheses. Thus α is a root of the polynomial $f(x, \beta) \in F(\beta)[x]$, so is algebraic over $F(\beta)$.

[17.12]

- (a) Since α is a root of $f(X) = X^n - \alpha^n \in F(\alpha^n)[X]$, we know that $[F(\alpha) : F(\alpha^n)] \leq n$. To show this is an equality, we show that $f(X)$ is irreducible. We note that $\alpha^n \in F[\alpha^n]$ is a prime element, because $F[\alpha^n]/\langle \alpha^n \rangle \cong F$, a field (this follows from α^n being transcendental, so $F[\alpha^n] \cong F[x]$); the ideal $\langle \alpha^n \rangle$ is thus maximal. By Eisenstein's criterion, $f(X)$ is irreducible.
- (b) First we compute $[F(\alpha, \beta^m) : F(\alpha^n, \beta^m)]$. Note that β^m is transcendental over F by Corollary 17.8. Now α is transcendental over $F(\beta^m)$; if not, by the previous problem we would have β^m algebraic over $F(\alpha)$, meaning β is algebraic over $F(\alpha)$, which contradicts our hypotheses. So part (a) of this problem, together with the previous problem, shows

$$[F(\alpha, \beta^m) : F(\alpha^n, \beta^m)] = [F(\beta^m)(\alpha) : F(\beta^m)(\alpha^n)] = n$$

Now we compute $[F(\alpha, \beta) : F(\alpha, \beta^m)]$. We know by hypothesis that β is transcendental over $F(\alpha)$, so that by part (a) we have

$$[F(\alpha, \beta) : F(\alpha, \beta^m)] = [F(\alpha)(\beta) : F(\alpha)(\beta^m)] = m$$

Lemma 17.6 then shows that

$$[F(\alpha, \beta) : F(\alpha^n, \beta^m)] = [F(\alpha, \beta) : F(\alpha, \beta^m)] \cdot [F(\alpha, \beta^m) : F(\alpha^n, \beta^m)] = mn$$

[17.13]

- (a) We can write $\alpha \in E$ as

$$\alpha = \frac{f(Y, Z)}{g(Y, Z)}$$

Raising everything to the p th power is a ring homomorphism. So

$$h(Y, Z)^p = \left(\sum_{i,j} a_{ij} Y^i Z^j \right)^p = \sum_{i,j} a_{ij}^p Y^{ip} Z^{jp}$$

Letting $\hat{h}$ be the same polynomial as h but with each coefficient raised to the p th power, we see $h(Y, Z)^p = \hat{h}(Y^p, Z^p)$. Thus

$$\alpha^p = \frac{f(Y, Z)^p}{g(Y, Z)^p} = \frac{\hat{f}(Y^p, Z^p)}{\hat{g}(Y^p, Z^p)} \in L$$

- (b) By the previous exercise, $[E : L] = p^2$. But for any $\alpha \in E$, from the above we see that it's a root of $x^p - \alpha^p \in L[x]$, so that

$$[L[\alpha] : L] \leq p < p^2$$

So $L[\alpha] \neq E$.

[17.14] We prove this by induction on n , the base case $n = 1$ being obvious. Now let E be a splitting field over F of $f(x)$, a polynomial of degree n , and assume the problem's conclusion for all degrees less than n . Pick $\alpha \in E$ that's a root of $f(x)$, and over $F[\alpha]$ write

$$f(x) = (x - \alpha)^r g(x)$$

Since $r \geq 1$, we have $\deg(g) = n - r < n$, and the induction hypothesis applies (replacing F by $F[\alpha]$). This relies on E being a splitting field of $g(x)$ over $F[\alpha]$: but E certainly contains all the roots of $g(x)$, and is generated by the roots of $g(x)$ together with $\alpha \in F[\alpha]$. Thus we have

$$[E : F] = [E : F[\alpha]] \cdot [F[\alpha] : F] \leq (n - r)! \cdot n \leq n!$$

[17.15] Let $\alpha \in L$, and write $f(x) \in F[x]$ as its minimal polynomial. Let $R := \{\alpha, \beta_1, \dots, \beta_m\} \subset L$ be the roots of $f(x)$ contained in L . Then $\theta(R) = \{\theta(\alpha), \theta(\beta_1), \dots, \theta(\beta_m)\}$ are roots of $\theta(f) = f(x)$ contained in $\theta(L) \subset L$. So $\theta(R) \subset R$, but θ is injective (as a homomorphism on a field). Since R is finite, this implies $\theta(R) = R$ and thus $\alpha \in \theta(R) \subset \theta(L)$. Since α was arbitrary, we see that $\theta(L) = L$.

Chapter 18

[18.1] First suppose E is normal over F . Then for $\alpha \in E$, we know that α is algebraic over F , so there is a minimal polynomial $m_\alpha(x) \in F[x]$. Because E is normal and contains the root α of $m_\alpha(x)$, this polynomial splits over E . Let $F \leq K_\alpha$ be the smallest subfield of E containing the roots of $m_\alpha(x)$; then K_α is a splitting field for $m_\alpha(x)$. Since α was arbitrary, and $\alpha \in K_\alpha$, we see that $E = \cup K_\alpha$ is the union of (a subset of) intermediate splitting fields.

Conversely, suppose E is such a union, and let $f(x) \in F[x]$ be an irreducible polynomial with a root $\alpha \in E$. E/F is automatically algebraic since every K/F is algebraic, and E is the union of these K . We want to show $f(x)$ splits over E . Since E is a union of splitting fields, $\alpha \in K$ for some intermediate splitting field K . But K/F is normal by Theorem 18.4, and since $f(x)$ has a root $\alpha \in K$, it splits over K . This means it also splits over E , as desired.

[18.2] If E is normal, then by Theorem 18.4 every F -isomorphism of E into L maps onto E . Now suppose the converse, that every F -isomorphism $\sigma : E \rightarrow L$ is such that $\sigma(E) \leq E$. Let $\alpha \in E$ and $m(x) \in F[x]$ its minimal polynomial. Because L/F is normal, we know $m(x)$ splits over L ; we want to show it splits over E as well, which is to say every root $\beta \in L$ of $m(x)$ is contained in E .

Since $[E : F]$ is finite, we can write $E = F(\alpha_1, \dots, \alpha_n)$. Write $m_i(x) \in F[x]$ for the minimal polynomial of α_i over F , and let $g(x) = m(x) \cdot m_1(x) \cdots m_n(x)$. Now $g(x)$ splits over L , and hence there is a smallest splitting field $F \leq K \leq L$. By Corollary 17.16, there is an

F -isomorphism $\sigma : F[\alpha] \rightarrow F[\beta]$. By Theorem 17.22, there is an extension $\sigma : K \rightarrow K \leq L$ such that $\sigma(\alpha) = \beta$. Restricting this to $E \leq K$, we get an F -isomorphism $\sigma : E \rightarrow L$, which by hypothesis implies $\sigma(E) \leq E$. But then $\beta = \sigma(\alpha) \in E$, as desired.

[18.3] Let M be an algebraic closure for E . Note that M is normal over E (and hence F by Corollary 17.7), and contains E . Define $L \leq M$ to be the intersection of all subfields of M which are normal over F , and contain E . Obviously L contains E , and if $f(x) \in F[x]$ has a root in L , then it has a root in every normal extension of F containing E , and hence $f(x)$ splits over each of these, implying all these subfields contain the splitting subfield of $f(x)$ in M , and so then does L . In other words, $f(x)$ also splits over L , so that L/F is normal. By construction, L is the smallest subfield of M containing E that is normal over F .

Now suppose $E \leq L_1 \leq M_1$ and $E \leq L_2 \leq M_2$, where L_i is a normal closure for E over F , and M_i is an algebraic closure of E . The identity map on E lifts to an E -isomorphism $\sigma : M_1 \rightarrow M_2$. Since σ maps splitting fields to splitting fields, [18.1] implies it maps normal fields over $F \leq E$ to normal fields over $\sigma(F) = F$. In particular, $\sigma(L_1)$ is normal over F , and contains $\sigma(E) = E$. By the minimality of L_2 , we see that $L_2 \leq \sigma(L_1)$. But the same reasoning shows $L_1 \leq \sigma^{-1}(L_2)$, so that $\sigma(L_1) = L_2$, as desired.

[18.4] L/F is normal because L is a splitting field for $g(x) \in F[x]$. Now suppose $E \leq K \leq L$ is such that K is normal over F . If $g(x) = g_1(x) \cdots g_n(x)$ and each of the g_i is irreducible, then because each $g_i(x)$ has a root in $E \leq K$, it must be that they all split over K , and thus $g(x)$ splits over K . But this implies $K = L$ then (both are generated by the roots of $g(x)$ over E). Thus L is a normal closure for E over F .

[18.5] Write $g(x) = g_1(x) \cdots g_n(x)$ as above, with each $g_i(x) \in F[x]$ irreducible. Because there exists $\alpha_i \in E$ with $g_i(\alpha_i) = 0$, we see that $g_i(x)$ is the minimal polynomial for α_i over F . Since E is separable, $g_i(x)$ has distinct roots. Thus $g(x)$ is separable, and by Theorem 18.13, L/F is Galois.

Since E is separable, there is a primitive element: $E = F[\alpha]$, with minimal polynomial $m(x) \in F[x]$. Since, by [18.3], L is unique up to E -isomorphism, we can assume that L is the splitting field of $m(x)$, because that won't change $[L : E]$. If $\deg(m) = n$, then $m(x)$ has n distinct roots by separability, and then $\text{Gal}(L/F)$ embeds in S_n by Lemma 18.3. Meanwhile we also have $[E : F] = n$, and we're done because $[L : F] = |\text{Gal}(L/F)|$ divides $|S_n| = n!$.

[18.6] Write $G_i \leq G$ for the point stabilizer of i in $G \leq S_n$. Then $[G : G_i] = n$ so that the fixed field of G_i has degree n over F . By the primitive element theorem, we can write $F[\alpha]/F$ for this extension, such that the minimal polynomial $m(x) \in F[x]$ has degree n . By transitivity, there exists $\sigma_i \in G$ such that $G_i = \sigma_i^{-1}G_1\sigma_i$. By the fundamental theorem of Galois theory, $F[\sigma_i(\alpha)]/F$ is the extension corresponding to $G_i \leq G$, and of course $\sigma_i(\alpha)$ has minimal polynomial $\sigma_i(m)(x) = m(x)$. In particular, the $\{\sigma_i(\alpha)\}$ (with $\sigma_1 = 1$) are the n distinct roots of $m(x)$. Again by the fundamental theorem of Galois theory, $E/F[\sigma_1(\alpha), \dots, \sigma_n(\alpha)]$ has

Galois group contained in $\cap G_i = \{1\}$, so that these fields are equal. Thus, E is the splitting field of $m(x)$, as desired.

[18.7] If $f(x)$ is separable, then E/F is Galois, and is in particular separable. Thus if $\{\alpha_1, \dots, \alpha_n\}$ are the roots of $g(x)$, each of them has a separable minimal polynomial, which thus has distinct roots (all of which are roots of $g(x)$ as well). Since E is a splitting field for $g(x)$, these minimal polynomials contain all roots of $g(x)$, so that we can write $g(x) = m_1(x) \cdots m_k(x)$. Each of these irreducible factors has distinct roots as mentioned, so $g(x)$ is separable as well. Swapping the roles of $f(x)$ and $g(x)$ proves the reverse direction.

[18.8] E is a splitting field of a polynomial over F , hence of a polynomial over K and L . Thus both E/K and E/L are Galois (since they are assumed to be separable extensions). Let $G, H \leq \text{Gal}(E/F)$ be the Galois groups of E/K and E/L . Now $\text{Gal}(E/F)$ is finite, so the subgroup $N := \langle G, H \rangle$ is finite. Let M be the fixed field of N , so that E/M is Galois. Of course, since $G, H \leq N$, we know that $M \leq K \cap L$. Meanwhile, $K \cap L$ is fixed by all elements of both G and H , hence by the subgroup N they generate. So $M = K \cap L$, and E/M is Galois, hence separable.

[18.9] We know that the Galois group $\text{Gal}(E/\mathbb{Q})$ is D_8 , of order 8. Let $K = \mathbb{Q}[i + \sqrt[4]{2}]$. Suppose $K < E$; then there is a subgroup $1 < H \leq D_8$ that fixes K . Since $|H| \geq 2$, it must be that $[K : \mathbb{Q}] \leq 4$, so that $\alpha := i + \sqrt[4]{2}$ has at most 4 conjugates (all being roots of the minimal polynomial of α over $\mathbb{Q}$). By showing there are at least 5, we have reached a contradiction, and thus $K = E$.

As described in the text, $\text{Gal}(E/\mathbb{Q})$ is generated by τ and σ , with $\tau(i) = -i$ and $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$. The orbit of α under this group thus contains

$$\{i + \sqrt[4]{2}, -i + \sqrt[4]{2}, i + i\sqrt[4]{2}, -i - i\sqrt[4]{2}, i - \sqrt[4]{2}, -i - \sqrt[4]{2}\}$$

And we're done, since this is $6 > 4$ elements in the orbit of α under $\text{Gal}(E/\mathbb{Q})$.

[18.10] The cyclic subgroup of order 4 in $\text{Gal}(E/\mathbb{Q})$ is generated by σ as in the text (and the previous exercise), which sends $\sqrt[4]{2}$ to $i\sqrt[4]{2}$ and fixes i . Note that in particular, $K = \mathbb{Q}[i]$ is fixed by the action of σ . Since $\langle \sigma \rangle$ has index 2 in $\text{Gal}(E/\mathbb{Q})$, and $[\mathbb{Q}[i] : \mathbb{Q}] = 2$, this must be the fixed field.

[18.11] If K is fixed by $H \leq G$ and L by H^σ , then the fundamental theorem of Galois theory shows $L = \sigma(K)$, so they are F -isomorphic. Conversely, suppose $\sigma : K \rightarrow L$ is an F -isomorphism. Since E/F is Galois, there is a polynomial $f(x) \in F[x]$ for which E is a splitting field. Since F is contained in K and L , E is also a splitting field for $f(x)$ over K and L . By Theorem 17.22, and the fact $\sigma(f)(x) = f(x)$, we can extend σ to an isomorphism of E , which fixes F . This extension then lies in $\text{Gal}(E/F)$. If K is fixed by $H \leq G$, then again the fundamental theorem of Galois theory shows L is fixed by H^σ .

[18.12]

(a) Note that E is the splitting field for $\prod (x^2 - p_i)$. Since this polynomial has distinct roots, it is separable, so $E/\mathbb{Q}$ is Galois.

- (b) We prove this by induction. Rational irrationalities shows $G := \text{Gal}(E/\mathbb{Q})$ has order 2^n or 2^{n-1} (in the case $\sqrt{p_n} \in \mathbb{Q}[\sqrt{p_1}, \dots, \sqrt{p_{n-1}}]$). So G is a finite 2-group, and we know by [8.17] that to show G is elementary Abelian, it is enough to show $\Phi(G) = 1$. We will show both that $|G| = 2^n$ and $\Phi(G) = 1$ by showing that G has $2^n - 1$ maximal subgroups, implying $[G : \Phi(G)] = 2^n$. To see this, note that $G/\Phi(G)$ has the same number of maximal subgroups as G , and (as an elementary Abelian group) it has $2^k - 1$, where $|G/\Phi(G)| = 2^k$.

By the fundamental theorem of Galois theory, maximal subgroups of G (those of index 2) come from quadratic extensions $\mathbb{Q} < \mathbb{Q}[\sqrt{k}] \leq E$. So we will exhibit $2^n - 1$ distinct quadratic extensions. Let k be some nonempty product of the $\{p_i\}$, and r a different such nonempty product. In particular, there is a p_i that divides k but not r . We will show $\mathbb{Q}[\sqrt{k}] \neq \mathbb{Q}[\sqrt{r}]$; since both are contained in E and since there are $2^n - 1$ such nonempty products, we will be done.

Suppose instead that the two fields are equal, so that $\sqrt{k} = a + b\sqrt{r}$ with $a, b \in \mathbb{Q}$. Squaring both sides, we have

$$2ab\sqrt{r} = k - a^2 - b^2r \in \mathbb{Q}$$

By [16.4], the left-hand side must be 0, so that $a = 0$ or $b = 0$. We cannot have $b = 0$ by the same problem [16.4], so $a = 0$ and $\sqrt{k} = b\sqrt{r}$. This implies $k = b^2r$, so that p_i divides b , hence p_i^2 divides k , which is a contradiction. Thus $\mathbb{Q}[\sqrt{k}] \neq \mathbb{Q}[\sqrt{r}]$, as desired.

- [18.13] For any $\sigma \in G := \text{Gal}(E/\mathbb{Q})$, we must have $\sigma(\sqrt{p_i}) = \pm\sqrt{p_i}$. If $\tau \in G$ does the same things as σ to these square roots, then $\sigma\tau^{-1}(\sqrt{p_i}) = \sqrt{p_i}$ for all i , and thus $\sigma\tau^{-1}$ fixes every element of E , so that $\sigma = \tau$. There are thus at most 2^n elements of G , given by the 2 choices of sign for each $\sigma(\sqrt{p_i})$. Since the previous problem showed $|G| = 2^n$, every such choice must be reachable from a (unique) element of G ; in particular, there exists $\sigma_i \in G$ with

$$\sigma_i(\sqrt{p_j}) = \begin{cases} -\sqrt{p_j} & j = i \\ \sqrt{p_j} & j \neq i \end{cases}$$

Now suppose $\sum a_i\sqrt{p_i} = 0$ for $\{a_i\} \subset \mathbb{Q}$. Applying σ_n to this equation, we see

$$\begin{aligned} a_1\sqrt{p_1} + \cdots + a_n\sqrt{p_n} &= 0 \\ a_1\sqrt{p_1} + \cdots - a_n\sqrt{p_n} &= 0 \\ 2a_n\sqrt{p_n} &= 0 \end{aligned}$$

Here the third equation comes from subtracting the first two. This last equation clearly implies $a_n = 0$. We can do this for all $1 \leq i \leq n$, so that all $a_i = 0$ and the $\{\sqrt{p_i}\}$ are linearly independent over $\mathbb{Q}$.

- [18.14] We exhibit 2^n distinct Galois conjugates of $\alpha := \sum \sqrt{p_i}$. Now if $K := \mathbb{Q}[\alpha]$ has degree $[K : \mathbb{Q}] = k$, then the minimal polynomial of this sum has degree k , and there are thus at

most k distinct Galois conjugates of α . So we will have shown $[K : \mathbb{Q}] \geq [E : \mathbb{Q}] = 2^n$, so that $K = E$.

By the previous problem, if $I \subset \{1, \dots, n\}$, there is a Galois automorphism σ_I such that

$$\sigma_I(\sqrt{p_j}) = \begin{cases} -\sqrt{p_j} & j \in I \\ \sqrt{p_j} & j \notin I \end{cases}$$

Letting I range over all 2^n subsets, we get 2^n conjugates of α . We now need to show they are all distinct. Suppose that $\sigma_I(\alpha) = \sigma_J(\alpha)$. Removing equal terms on both sides of this equation, we're left with

$$2 \sum_{i \in I \setminus J} \sqrt{p_i} = 2 \sum_{j \in J \setminus I} \sqrt{p_j}$$

But if $I \setminus J$ or $J \setminus I$ is nonempty, then this contradicts the linear independence of the previous problem. Thus we actually have $I = J$ in this case, so that the 2^n Galois conjugates are distinct, as desired.

[18.15] Let $\sigma \in \text{Gal}(E/F)$. Then we can restrict $\sigma_K : K \rightarrow E$. Because K/F is normal and σ is an F -isomorphism, we know that $\sigma_K(K) = K$, so that $\sigma_K \in \text{Gal}(K/F)$. This is clearly a homomorphism, since $(\tau\sigma)_K(\alpha) = \tau\sigma(\alpha) = \tau_K\sigma_K(\alpha)$ for $\alpha \in K$. We only then need to show that every such element of $\text{Gal}(K/F)$ can be realized this way.

For that, let $\phi \in \text{Gal}(K/F)$. Note that E is also an algebraic closure for K by Lemma 17.24, since any element algebraic over F is also algebraic over K . By Theorem 17.30 then, we can extend ϕ to $\phi^E : E \rightarrow E$. Since ϕ is an F -isomorphism, so is ϕ^E , and thus $\phi^E \in \text{Gal}(E/F)$. Finally, we obviously have $(\phi^E)_K \equiv \phi$.

[18.16] Let $\alpha \in E \setminus F$, $m(x) \in F[x]$ its minimal polynomial, and $F \leq K \leq E$ the splitting field for $m(x)$. Then K/F is Galois (since E/F is separable). By Lemma 18.3, $\text{Gal}(K/F)$ acts transitively on the roots of $m(x)$. Because $\alpha \notin F$, we have $\deg(m) > 1$, and so by separability there is a root $\beta \neq \alpha$ in K and an element $\sigma \in \text{Gal}(K/F)$ with $\sigma(\alpha) = \beta$. By the previous exercise, there is a $\hat{\sigma} \in \text{Gal}(E/F)$ which induces σ when restricted to K , and in particular $\hat{\sigma}(\alpha) = \beta \neq \alpha$. Thus α is not in the fixed field of $\text{Gal}(E/F)$. This shows the fixed field is precisely F .

[18.17] Choose $1 \neq \sigma \in G$ and an element $\alpha \in E$ with $\sigma(\alpha) \neq \alpha$. If $m(x) \in F[x]$ is the minimal polynomial of α , then $\Omega = \{\beta \in E \mid m(\beta) = 0\}$ is a finite nonempty subset. By Lemma 18.3, there is a homomorphism from $\text{Gal}(E/F)$ to S_Ω , a finite group, and the image of σ is nontrivial. If K_σ is the kernel of this homomorphism, then K_σ is a finite index normal subgroup not containing σ . Since σ was arbitrary, we can construct these K_g for all nontrivial $g \in G := \text{Gal}(E/F)$. If $\mathcal{N}$ is the set of all finite-index normal subgroups for G , then

$$\bigcap_{N \in \mathcal{N}} N \subseteq \bigcap_{\sigma \in G^*} K_\sigma = \{1\}$$

and so G is residually finite.

[18.18] Let $\sigma \in \text{Aut}(\mathbb{R})$. Because $\sigma(1) = 1$, we know $\sigma(n) = n$ for all $n \in \mathbb{Z}$. Because $n \cdot \frac{m}{n} = m$, this also implies σ fixes $\frac{m}{n}$; in other words, $\sigma \in \text{Gal}(\mathbb{R}/\mathbb{Q})$. Now if $r > 0$, it must be that $r = s^2$ for some $s \in \mathbb{R}$. Then $\sigma(r) = \sigma(s)^2 > 0$ as well. This implies σ preserves the order on $\mathbb{R}$:

$$x > y \iff x - y > 0 \implies \sigma(x) - \sigma(y) = \sigma(x - y) > 0 \iff \sigma(x) > \sigma(y)$$

But then σ is actually *continuous*, and since it fixes the dense subset $\mathbb{Q}$ pointwise, it must be the identity.

[18.19] Note that $F[\alpha] \subset K$, and hence $E \cap F[\alpha] = F$. Also the compositum of E and $F[\alpha]$ in L is just $E[\alpha]$. By Corollary 18.23, we have

$$[E[\alpha] : E] = [F[\alpha] : F] = \deg(f)$$

Thus the minimal polynomial for α over E , which divides $f(x)$, has the same degree, and so is in fact $f(x)$. In particular, $f(x)$ is irreducible over E .

[18.20] Let $F = \mathbb{Q}$, and α the real root of $x^3 - 2$. Also let β be an imaginary root of the same polynomial. If L is the splitting field of this polynomial, let $E = \mathbb{Q}[\alpha]$ and $K = \mathbb{Q}[\beta]$. The minimal polynomial for $\beta \in K$ is just $x^3 - 2$. But the minimal polynomial for β over E is in fact $x^2 + \alpha x + \alpha^2$.

[18.21] We shows in [17.10] that $f(x)$ had degree 4, and the splitting field E was in fact just $\mathbb{Q}[\alpha]$. This shows $\text{Gal}(E/\mathbb{Q})$ has order 4. Let $\beta = \sqrt{2 - \sqrt{2}}$, which (as we showed) is also a root of $f(x)$; thus there is an element σ of the Galois group with $\sigma(\alpha) = \beta$. Since $(\alpha\beta)^2 = 2$, we see that $\sigma(\alpha)^2\sigma(\beta)^2 = 2$, so $\sigma(\beta) = \pm\alpha$. But we also have

$$\left(\frac{\alpha}{\beta} - 1\right)^2 = \frac{(\alpha^2 - \alpha\beta)^2}{(\alpha\beta)^2} = 2$$

If we suppose $\sigma(\beta) = \alpha$, then applying it to the left-hand side gives

$$\left(\frac{\beta}{\alpha} - 1\right)^2 = \frac{(\beta^2 - \alpha\beta)^2}{(\alpha\beta)^2} = (1 - \sqrt{2})^2 \neq 2$$

This shows that in fact $\sigma(\beta) = -\alpha$, and hence $\sigma^2(\alpha) \neq \alpha$. Since σ has order dividing 4, it must have order 4, and thus $\text{Gal}(E/\mathbb{Q})$ is cyclic, generated by σ .

[18.22] Let $F = \mathbb{Q}$, $K = \mathbb{Q}[\sqrt{2}]$, and $E = \mathbb{Q}[\sqrt[4]{2}]$. Then since K/F and E/K are both degree 2, they are Galois. But E/F is not Galois, since the minimal polynomial of $\sqrt[4]{2}$ is $x^4 - 2$, and this doesn't split over E (the splitting field is not real, but $E \subset \mathbb{R}$).

[18.23] Clearly G is a subgroup. By [16.13], the map $G \rightarrow S_\Omega$ is surjective. But if some element $\sigma \in G$ is in the kernel, then it preserves each indeterminate X_i . Since E is generated over F by these indeterminates, $\sigma \equiv 1$. So we have our isomorphism $G \rightarrow S_\Omega$.

[18.24] Embed G in some S_n (for example, take $n = |G|$ and use Cayley's theorem). Let

$E = F(X_1, \dots, X_n)$. By the previous problem, $\text{Gal}(E/F)$ has a subgroup isomorphic to S_n , and hence it has a subgroup isomorphic to G . Let L be the fixed field of G , so that E/L is Galois and $\text{Gal}(E/L) \cong G$.

[18.25] First we show that K is fixed by G . For that, note that any permutation of the X_i fixes $f(X)$, and hence fixes its coefficients, so K is fixed. Now the full fixed field L of G is such that $[E : L] = n!$. But $f(X) \in K[X]$, and since E is a splitting field for $f(X)$ over K , [17.14] shows $[E : K] \leq n!$. Since $[E : K] = [E : L][L : K]$, we see that $[L : K] = 1$, and K is the fixed field of G .

Chapter 19

[19.1] Define $\Delta(a/b)$ via the usual quotient rule of derivatives:

$$\Delta(a/b) = \frac{b\delta(a) - a\delta(b)}{b^2}$$

Clearly $\Delta(r) = \Delta(r/1) = \delta(r)$, so we just need to show this is well-defined, and a derivation. If $a/b = c/d$, we have

$$\begin{aligned} \Delta(a/b) - \Delta(c/d) &= \frac{b\delta(a) - a\delta(b)}{b^2} - \frac{d\delta(c) - c\delta(d)}{d^2} \\ &= \frac{bd^2\delta(a) + b^2c\delta(d) - ad^2\delta(b) - b^2d\delta(c)}{b^2d^2} \\ &= \frac{bd(d\delta(a) + a\delta(d)) - bd(c\delta(b) + b\delta(c))}{b^2d^2} \\ &= \frac{bd(\delta(ad) - \delta(bc))}{b^2d^2} \\ &= 0 \end{aligned}$$

where we have repeatedly used $ad = bc$. To show it is a derivation:

$$\begin{aligned} \Delta(ac/bd) &= \frac{bd\delta(ac) - ac\delta(bd)}{b^2d^2} \\ &= \frac{bda\delta(c) - acb\delta(d)}{b^2d^2} + \frac{bdc\delta(a) - acd\delta(b)}{b^2d^2} \\ &= (a/b)\Delta(c/d) + (c/d)\Delta(a/b) \end{aligned}$$

[19.2] Let δ be the F -derivation on $F[x]$ from Lemma 19.3. From the previous problem, there is a derivation Δ on $E := F(x)$ which agrees with δ on $F[x]$, and in particular is an F -derivation. Since $\Delta(x) = \delta(x) = 1$, this is a nonzero derivation.

[19.3]

(a) Write $f(x) = a_n x^n + \cdots + a_0$. Then we have

$$\delta(f(\alpha)) = a_n \delta(\alpha^n) + \cdots + \delta(a_0) = n a_n \alpha^{n-1} \delta(\alpha) + \cdots + 0 = f'(\alpha) \delta(\alpha)$$

where we've used Lemma 19.1 to simplify the expressions.

(b) We know that $\delta(a) = 0$ for all $a \in F$, so $F \subset K$. If $\alpha, \beta \in K$, then of course $\delta(\alpha + \beta) = 0 + 0$, and

$$\delta(\alpha\beta) = \alpha\delta(\beta) + \beta\delta(\alpha) = 0 + 0$$

Finally, $0 = \delta(1) = \delta(\alpha\alpha^{-1})$ implies $\alpha^{-1} \in K$ as well; thus $K \subset E$ is a subfield.

To see that δ is K -linear, we have for $\omega \in E$

$$\delta(\alpha\omega) = \alpha\delta(\omega) + \omega\delta(\alpha) = \alpha\delta(\omega)$$

(c) For $\omega \in E$, let $f(x)$ be its minimal polynomial over K . From part (a) [which applies because δ is a K -derivation by part (b)], we see that

$$0 = \delta(0) = \delta(f(\omega)) = f'(\omega)\delta(\omega)$$

If $\omega \notin K$, then this implies $f'(\omega) = 0$. By Theorem 19.4, f is not separable over K , and since ω was arbitrary, E is purely inseparable over K .

[19.4] Let $m = [E : F]$. Define $\delta(\alpha^k) = k\alpha^{k-1}$ for $0 \leq k < m$. The set $\{\alpha^k\}$ spans E over F , so we can define δ on all of E by extending F -linearly. Lemma 19.2 then gives us a method to show δ is a derivation. In particular, when $j + k < m$, we have

$$\delta(\alpha^{j+k}) = (j+k)\alpha^{j+k-1} = j\alpha^{j-1}\alpha^k + k\alpha^{k-1}\alpha^j = \alpha^k\delta(\alpha^j) + \alpha^j\delta(\alpha^k)$$

So we only need to worry about $j + k = m + \epsilon$ for $\epsilon \geq 0$. By Corollary 19.11 and Theorem 19.10, we know that $m = p^r$ for some $r > 0$, so that $\alpha^m \in F$. Then we have

$$\delta(\alpha^{j+k}) = \alpha^m \delta(\alpha^\epsilon) = \epsilon \alpha^m \alpha^{\epsilon-1} = (j+k-m)\alpha^{j+k-1} = (j+k)\alpha^{j+k-1}$$

where we've used the fact that $m \equiv 0 \pmod{p}$. This case then follows exactly as the one above, and hence we have defined a derivation. Clearly $\delta(\alpha) = 1$ by construction.

[19.5] If E/F is separable, then by [19.3] for any F -derivation we must have

$$K = \{\alpha \in E \mid \delta(\alpha) = 0\} = E$$

so that $\delta \equiv 0$. If E/F is inseparable, then by Theorem 19.14 there is an intermediate subfield $F \leq L \leq E$ such that E/L is purely inseparable, and $E \neq L$. Because it is a finite extension, we can choose $L \leq K \leq E$ such that $E = K[\alpha]$ and E/K is purely inseparable. By Theorem 19.10, we must have $\alpha^{p^n} \in K$, so the previous problem applies to find a non-zero K -derivation δ on E . Since this is also an F -derivation, we're done.

[19.6]

(a) Just compute:

$$\begin{aligned}
 (\sigma\tau - \tau\sigma)(ab) &= \sigma(a\tau(b) + \tau(a)b) - \tau(a\sigma(b) + \sigma(a)b) \\
 &= [\sigma(a)\tau(b) + a\sigma\tau(b) + \tau(a)\sigma(b) + \sigma\tau(a)b] \\
 &\quad - [\tau(a)\sigma(b) + a\tau\sigma(b) + \sigma(a)\tau(b) + \tau\sigma(a)b] \\
 &= a(\sigma\tau - \tau\sigma)(b) + (\sigma\tau - \tau\sigma)(a)b
 \end{aligned}$$

(b) Just compute:

$$\begin{aligned}
 \delta_a(xy) &= xya - axy \\
 &= xya - xay + xay - axy \\
 &= x(ya - ay) + (xa - ax)y \\
 &= x\delta_a(y) + \delta_a(x)y
 \end{aligned}$$

(c) Just compute:

$$\begin{aligned}
 (\sigma\delta_a - \delta_a\sigma)(x) &= \sigma(xa - ax) - \sigma(x)a + a\sigma(x) \\
 &= \sigma(x)a + x\sigma(a) - \sigma(a)x - a\sigma(x) - \sigma(x)a + a\sigma(x) \\
 &= x\sigma(a) - \sigma(a)x \\
 &= \delta_{\sigma(a)}(x)
 \end{aligned}$$

Similarly, $\delta_a\tau - \tau\delta_a \equiv \delta_{-\tau(a)}$.

[19.7] Of course $[a, a] = a^2 - a^2 = 0$. Similarly, from the distributivity of the multiplication in R , we get distributivity for the bracket as well. Finally, we compute to prove the Jacobi identity:

$$\begin{aligned}
 [a, b, c] + [b, c, a] + [c, a, b] &= (abc - bac - cab + cba) \\
 &\quad + (bca - cba - abc + acb) \\
 &\quad + (cab - acb - bca + bac) \\
 &= 0
 \end{aligned}$$

[19.8] Write $\delta_a(x) := [x, a]$. A key fact is that $[a, b] = -[b, a]$, which follows from

$$0 = [a + b, b + a] = [a, b] + [a, a] + [b, b] + [b, a] = [a, b] + [b, a]$$

Then we have

$$\begin{aligned}
 \delta_a([x, y]) - [\delta_a(x), y] - [x, \delta_a(y)] &= \delta_a([x, y]) + [-\delta_a(x), y] + [\delta_a(y), x] \\
 &= [x, y, a] + [a, x, y] + [y, a, x] \\
 &= 0
 \end{aligned}$$

with the last equality following from the Jacobi identity. So δ_a is a derivation.

[19.9]

- (a) Let $\alpha \in S$ and let $f(x) \in F[x]$ be the minimal polynomial. Since E/F is normal, $f(x)$ splits over E . Since α is separable over F , $f(x)$ has distinct roots, and thus every root of $f(x)$ in E also belongs to S . Thus $f(x)$ splits over S , and this implies S/F is normal. Since it is separable by construction, S/F is Galois.

Let $\sigma \in \text{Gal}(E/F)$. Then $\sigma(\alpha)$ is also a root of $f(x)$, and hence separable. This shows $\sigma(S) \subset S$, and of course since $\sigma^{-1}(S) \subset S$ we must have $\sigma(S) = S$. We thus know that $\sigma|_S \in \text{Gal}(S/F)$. Let $\rho : \text{Gal}(E/F) \rightarrow \text{Gal}(S/F)$ be the restriction homomorphism. If $\tau \in \text{Gal}(S/F)$, then by Theorems 18.4 and 17.22, we can extend it to $\hat{\tau} : E \rightarrow E$, such that $\rho(\hat{\tau}) = \tau$, so that ρ is surjective. To see ρ is injective, let $\sigma \in \text{Gal}(E/F)$ be such that $\sigma|_S$ is the identity. For $\beta \in E \setminus S$, we know from Theorem 19.10 that it has minimal polynomial of the form $x^{p^n} - b = (x - \beta)^{p^n}$. Since $\sigma(\beta)$ is a root of this polynomial, we see $\sigma(\beta) = \beta$. Thus σ is the identity on E , and thus ρ is injective.

- (b) We have $[E : F]_{\text{sep}} = [S : F] = |\text{Gal}(S/F)| = |\text{Gal}(E/F)|$, where the equalities follow by definition; from the fact S/F is Galois; and from part (a).

[19.10] The number of F -embeddings of L into E are just the distinct images of L under $G := \text{Gal}(E/F)$. Now $\sigma, \tau \in G$ have the same image of L precisely when $\sigma\tau^{-1}|_L$ is the identity, which is equivalent to σ and τ being in the same coset of $H := \text{Gal}(E/L)$ in G . Since by Corollary 19.21 $[E : F]_{\text{sep}} = [E : L]_{\text{sep}}[L : F]_{\text{sep}}$, we then have from the previous problem

$$[L : F]_{\text{sep}} = \frac{[E : F]_{\text{sep}}}{[E : L]_{\text{sep}}} = \frac{|G|}{|H|} = [G : H]$$

as desired.

[19.11] Let L be a splitting field for $f(x)$ over F , with roots $\{\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m\}$. From Lemma 17.15, for every i there is an F -isomorphism $\sigma_i : F[\alpha] \rightarrow F[\alpha_i]$. By Theorem 17.22, this extends to an element $\sigma_i \in \text{Gal}(L/F)$. Meanwhile, if $\sigma \in \text{Gal}(L/F)$, then $\sigma(E) = F[\sigma(\alpha)]$, and we must have $\sigma(\alpha) = \sigma_i(\alpha)$ for some $1 \leq i \leq m$. So there are m distinct F -embeddings of E into L , so by the previous problem $[E : F]_{\text{sep}} = m$.

[19.12] Let $f(x) \in F[x]$ have distinct roots. We will show that, from the roots of $f(x^{p^a})$, both p^a and the original roots of $f(x)$ can be recovered. This implies that if $f(x^{p^a}) = g(x^{p^b})$ and both original polynomials have distinct roots, then $p^a = p^b$ and $f(x)$ and $g(x)$ have the same (distinct!) roots, and hence are equal (up to leading coefficient), but $f(x^{p^a}) = g(x^{p^b})$ implies they have the same leading coefficient, hence $f(x) = g(x)$.

Let $\{\alpha_1, \dots, \alpha_m\}$ be the distinct roots of $f(x)$ in an algebraic closure $K \geq F$. Let β_i be a root of $x^{p^a} - \alpha_i$. Then over K , we have the splitting

$$f(x^{p^a}) = c \prod_{i=1}^m (x - \beta_i)^{p^a}$$

This shows that the cardinality of each repeated root of $f(x^{p^a})$ determines p^a . If $\{\gamma_i\}$ are the different roots of $f(x^{p^a})$, then $\{\gamma_i^{p^a}\}$ are the original roots of $f(x)$. Thus the roots of $f(x^{p^a})$ determine both p^a and the roots of $f(x)$, as desired.

[19.13] We work by induction on n , the case $n = 1$ being obvious. Note that all the field extensions we consider here are purely inseparable by Corollaries 19.12 and 19.13. Suppose $n > 1$ and $\alpha \notin F$. Note that α is a root of $x^p - \alpha^p$, so that $[F[\alpha] : F[\alpha^p]] \leq p$. But by Theorem 19.10, α has a minimal polynomial of the form $x^{p^r} - a$ for some $r > 0$ and $a \in F$; This shows $[F[\alpha] : F] = p^r$ and $[F[\alpha^p] : F] \leq p^{r-1}$, and hence $[F[\alpha] : F[\alpha^p]] = p$. By induction, if $[F[\alpha^p] : F] = k$, then $\alpha^{p^k} \in F$. Since $pk = [F[\alpha] : F]$ divides $n = [E : F]$, we have that $\alpha^n \in F$.

[19.14]

- (a) We know that α is a root of $h(x) = x^{p^n} - a = (x - \alpha)^{p^n}$ over S , and thus an irreducible factor of $m(x)$ must look like $(x - \alpha)^k$. Thus the minimal polynomial $m(x)$ is such that $h(x) = m(x)^r$ for some $r \geq 1$. This implies $m(x) = (x - \alpha)^{p^s}$ and thus $\alpha^{p^s} \in F$. By the minimality of n , we must have $h(x) = m(x)$, so it's irreducible.
- (b) $h(x)$ is irreducible over S , and hence over $F[a] \subset S$. So $[F[\alpha] : F[a]] = \deg(h) = p^n$.
- (c) Let $f(x) \in F[x]$ be the minimal polynomial for α over F . From Corollary 19.9, we can write $f(x) = k(x^{p^s})$ for an irreducible and separable polynomial $k(x) \in F[x]$. This implies $\alpha^{p^s} \in S$, and hence by hypothesis that $p^s \geq p^n$. If $g(x) \in F[x]$ is the minimal polynomial of a over F , then $k(x^{p^s}) = f(x)$ divides $g(x^{p^n})$. From the solution to [19.12], this shows $p^s \leq p^n$, so that they are equal. Then $k(a) = k(\alpha^{p^n}) = f(\alpha) = 0$ shows that $k(x) = g(x)$.
- (d) Let $L := F[\alpha] \cap S$; clearly $F[a] \subset L$. From part (b), $[F[\alpha] : F[a]] = p^n$. Because $F[\alpha]/L$ is purely inseparable, we know that $[F[\alpha] : L] = p^s$ and from the previous problem, that $\alpha^{p^s} \in L$. This shows $p^s \geq p^n$, and hence $L = F[a]$ by considering degrees.

[19.15] From Theorem 19.10, there's a power p^n such that every coefficient of $f(x)^{p^n}$ lies in F , but this might not be irreducible. Let $g(x) \in F[x]$ be a monic irreducible factor of $f(x)^{p^n}$. Then $g(x)$ is a constant $a \in E$ times a power of $f(x)$ by irreducibility in $E[x]$: $g(x) = af(x)^m$ for some $m \geq 1$. Since both f and g are monic, we see that $a = 1$ and hence $f(x)^m = g(x) \in F[x]$ is irreducible, as desired.

Chapter 20

[20.1] First suppose that p does not divide n . We have

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = \frac{\Phi_1(x^p)}{\Phi_1(x)}$$

so it's true when $n = 1$. Assume by induction it's true for all proper divisors of $n > 1$. Then we have

$$\prod_{d|n} \Phi_d(x^p) = (x^p)^n - 1 = \prod_{d|n} \Phi_d(x) \Phi_{pd}(x) = \Phi_n(x) \Phi_{pn}(x) \prod_{d|n, d < n} \Phi_d(x^p)$$

where we've used Lemma 20.4 twice, and the last equality uses the induction hypothesis. Dividing out the extremes by the proper divisor product, we see $\Phi_n(x^p) = \Phi_n(x) \Phi_{pn}(x)$, as desired.

Now suppose $p \mid n$. Then if ϵ is a primitive pn th root of unity, clearly it is a root of $f(x) := \Phi_n(x^p)$. But $\phi(pn) = p\phi(n) = \deg(f)$. This shows $f(x)$ is irreducible (by Corollary 20.9), and thus we must have $f(x) \equiv \Phi_{pn}(x)$.

[20.2] $\phi(2n) = \phi(2)\phi(n) = \phi(n) = \deg(\Phi_n)$. But if ϵ is a primitive n th root of unity, then $-\epsilon$ is a primitive $2n$ th root of unity (because n is odd). Since $-\epsilon$ is a root of $\Phi_n(-x)$, and since it has the right degree by the above, we must have $\Phi_{2n}(x) = \Phi_n(-x)$.

[20.3] Note that $\Phi_1(0) = -1$, but $\Phi_2(0) = 1$. Assume it's true for all values $2 < d < n$. Then we have by Lemma 20.4

$$0^n - 1 = \prod_{d|n} \Phi_d(0)$$

By induction we have $-1 = \Phi_1(0)\Phi_n(0)$, so that $\Phi_n(0) = 1$ as well.

[20.4] This is obvious when $n = 1$, so let $n > 1$. Let $f(x) := x^{\phi(n)} \Phi_n(\frac{1}{x})$, which is a polynomial of degree $\phi(n)$. Note that the coefficient of x^i in $f(x)$ is $a_{\phi(n)-i}$. If ϵ is a primitive n th root of unity, then so is ϵ^{-1} . This shows ϵ is a root of $f(x)$. Again, by degree considerations (and the fact $f(x)$ is monic by the previous problem), we must have $f(x) \equiv \Phi_n(x)$. Comparing coefficients, we have $a_i = a_{\phi(n)-i}$.

[20.5]

(a) We have

$$\Phi_q(x^m) = x^{m(q-1)} + x^{m(q-2)} + \cdots + 1 = \sum_{i=1}^q (x^q)^m x^{-im}$$

Now because $m \not\equiv 0 \pmod{p}$, there's a permutation σ of $\{0, 1, \dots, q-1\}$ such that $-im \equiv \sigma(i-1) \pmod{q}$ for all $1 \leq i \leq q$. Choose $c_i > 0$ such that $c_i q - im = \sigma(i-1)$, and set $d_i = m - c_i$. Then we finally have

$$\sum_{i=1}^q (x^q)^m x^{-im} = \sum_{i=1}^q (x^q)^{d_i} x^{\sigma(i-1)} = \sum_{i=0}^{q-1} (x^q)^{d_{i+1}} x^{\sigma(i)} = \sum_{i=0}^{q-1} (x^q)^{e_i} x^i$$

where we set $e_i = d_{\sigma^{-1}(i)+1}$.

(b) From the previous part, we see that

$$\Phi_q(x^m)(x-1) = \sum_{i=0}^{q-1} [(x^q)^{a_i} - (x^q)^{e_i}] x^i \quad a_i = \begin{cases} e_{q-1} + 1 & i = 0 \\ e_{i-1} & 0 < i < q \end{cases}$$

- (c) Note that $\Phi_q(x^m)/\Phi_q(x) = \Phi_q(x^m)(x-1)/(x^q-1)$. From the expression in the previous part, we know what the numerator looks like. And each monomial in the expression of the previous part is divisible by x^q-1 . For example, when $a_i = e_i$, our quotient is 0. If $a_i < e_i$, then we have

$$(x^q)^{a_i} - (x^q)^{e_i} = -x^{qa_i} ((x^q)^{e_i-a_i} - 1)$$

so that

$$\frac{(x^q)^{a_i} - (x^q)^{e_i}}{x^q - 1} = -x^{qa_i} (1 + x^q + \dots + x^{q(e_i-a_i-1)})$$

Similarly, when $e_i < a_i$ we have

$$\frac{(x^q)^{a_i} - (x^q)^{e_i}}{x^q - 1} = x^{qe_i} (1 + x^q + \dots + x^{q(a_i-e_i-1)})$$

Note that all the monomial terms here have exponents divisible by q . When we multiply this expression by x^i , then, we get all the monomials of $\Phi_q(x^m)/\Phi_q(x)$ with exponent equivalent to $i \pmod{p}$. In other words, no powers of x coincide in our expanded expression; since every coefficient is ± 1 above, we see that the non-zero coefficients of $\Phi_q(x^m)/\Phi_q(x)$ are all ± 1 .

- (d) If m is prime, then $m \neq q$ by hypothesis, so [20.1] shows

$$\Phi_{qm}(x) = \Phi_q(x^m)/\Phi_q(x)$$

and by the previous part all the nonzero coefficients of this quotient are ± 1 .

[20.6] We induct on numbers of this form, the case $n = 1$ being trivial. If $a = 1$ in $n = 2^a p^b q^c$, then [20.2] shows $\Phi_n(x) \equiv \Phi_{n/2}(-x)$, so by induction all nonzero coefficients are ± 1 . If $a > 1$, then from [20.1] we have $\Phi_n(x) = \Phi_{n/2}(x^2)$, and again by induction all nonzero coefficients are ± 1 . So we may assume $a = 0$. If $b > 1$ then $\Phi_n(x) = \Phi_{n/p}(x^p)$ (again by [20.1]), so induction finishes the problem again; a similar argument works for $c > 1$. We are thus reduced to the case $n = pq$ (the cases $n = p$ and $n = q$ follow immediately of course). But then by the previous problem, $\Phi_{pq}(x)$ has all nonzero coefficients ± 1 , and we're done.

[20.7] Let P be the set of all primitive roots of unity, and S their sum. Since

$$\Phi_n(x) = \prod_{\zeta \in P} (x - \zeta)$$

we see that the coefficient of $x^{\phi(n)-1}$ (the second highest-degree term in $\Phi_n(x)$) will give us S (up to sign). But because p^2 divides n , [20.1] shows $\Phi_n(x) = \Phi_{n/p}(x^p)$. This shows the coefficient of $x^{\phi(n)-1}$ is 0 because $p > 1$.

[20.8] Let $K = \langle \mathbb{Q}_n, \mathbb{Q}_m \rangle$ be the compositum, and note that $K = \mathbb{Q}_{mn}$ by Theorem 20.12. By

the same theorem, $\mathbb{Q}_n \cap \mathbb{Q}_m = \mathbb{Q}$. Since everything in sight is Galois, we see by natural irrationalities that

$$[K : \mathbb{Q}_m] = [\mathbb{Q}_n : \mathbb{Q}] = \phi(n)$$

$K = \mathbb{Q}_m[\epsilon]$ for a primitive n th root of unity ϵ . This shows the minimal polynomial of ϵ over $\mathbb{Q}_m$ has degree $\phi(n)$, and since $\Phi_n(x)$ has this same degree, as well as ϵ as a root, it must be that $\Phi_n(x)$ is the desired minimal polynomial, and hence irreducible over $\mathbb{Q}_m$.

[20.9] In a cyclic group $C = \langle \tau \rangle$ of order n , there is an automorphism sending τ to τ^m . If $D = \langle \epsilon \rangle \subset \mathbb{Q}_n$ is the cyclic group generated by a primitive n th root of unity, then by Corollary 20.10 there is a Galois automorphism corresponding to the above automorphism of C , thus sending ϵ to ϵ^m .

[20.10] Let $\mathbb{Q}_7 = \mathbb{Q}[\epsilon]$ for a primitive root of unity ϵ . We know that $\text{Gal}(\mathbb{Q}_7/\mathbb{Q})$ is cyclic of order 6, and is in fact generated by the map $\gamma : \epsilon \mapsto \epsilon^3$ (as can be check by iterating this until it's the identity map). There is a unique subgroup of index 3 in this Galois group, namely the one of order 2 generated by the inversion map $\iota : \epsilon \mapsto \epsilon^{-1}$. In particular, $\tau := \epsilon + \epsilon^6$ is fixed by ι and thus lives in the fixed field $K \leq \mathbb{Q}_7$ of $\langle \iota \rangle$, with $[K : \mathbb{Q}] = 3$. We will show that $\tau \notin \mathbb{Q}$, so that $K = \mathbb{Q}[\tau]$ (since 3 is prime), and then we will compute the minimal polynomial of τ explicitly.

To show $\tau \notin \mathbb{Q}$, we simply note that $\gamma(\tau) \neq \tau$. If it did, that would imply we have $\epsilon + \epsilon^6 = \epsilon^3 + \epsilon^4$, and thus ϵ would be a root of $x^6 - x^4 - x^3 + x = 0$, but that polynomial factors as $x(x^5 - x^3 - x^2 + 1)$, so ϵ would have degree at most 5 over $\mathbb{Q}$. Since in fact $[\mathbb{Q}[\epsilon] : \mathbb{Q}] = \phi(7) = 6$, this contradiction shows $\gamma(\tau) \neq \tau$, as claimed. The minimal polynomial of τ will have roots transitively permuted by the Galois group $\langle \gamma \rangle / \langle \iota \rangle$, and in particular those roots are $\{\tau, \gamma(\tau), \gamma^2(\tau)\}$. We compute

$$\begin{aligned} \tau + \gamma(\tau) + \gamma^2(\tau) &= \epsilon + \epsilon^6 + \epsilon^3 + \epsilon^4 + \epsilon^2 + \epsilon^5 \\ &= -1 + \sum_{i=0}^6 \epsilon^i \\ &= -1 \\ \tau\gamma(\tau) + \tau\gamma^2(\tau) + \gamma(\tau)\gamma^2(\tau) &= (\epsilon + \epsilon^6)(\epsilon^3 + \epsilon^4) + (\epsilon + \epsilon^6)(\epsilon^2 + \epsilon^5) + (\epsilon^3 + \epsilon^4)(\epsilon^2 + \epsilon^5) \\ &= 2 \sum_{i=1}^6 \epsilon^i \\ &= -2 \\ \tau\gamma(\tau)\gamma^2(\tau) &= (\epsilon + \epsilon^6)(\epsilon^3 + \epsilon^4)(\epsilon^2 + \epsilon^5) \\ &= 2 + \sum_{i=1}^6 \epsilon^i \\ &= 1 \end{aligned}$$

So our minimal polynomial is $x^3 + x^2 - 2x - 1$.

[20.11] We will write our sum as $\sum a_i \epsilon^i$ for ϵ a primitive p th root of unity. Here the a_i are non-negative integers. Suppose this is equal to the rational number $\frac{r}{s}$. Clearing denominators, we have the expression

$$sa_{p-1}\epsilon^{p-1} + \cdots + sa_1\epsilon^1 - r = 0$$

This means ϵ is a root of the polynomial $f(x) = sa_{p-1}x^{p-1} + \cdots + sa_1x - r$, of degree at most $p-1 = \phi(p)$. Since $\Phi_p(x)$ has degree $p-1$ and is irreducible, it must be that $f(x)$ is a rational multiple of $\Phi_p(x)$, and in particular we must have

$$sa_{p-1}x^{p-1} + \cdots + sa_1x - r = sa_{p-1}(x^{p-1} + \cdots + x + 1)$$

This implies the values sa_i are all the same, so that the a_i are all the same. We have thus shown that for such a non-empty sum to be rational, every primitive root must occur (and in fact, must occur the same number of times).

[20.12] Let $\text{Gal}(\mathbb{Q}_p/\mathbb{Q})$ be generated by the map γ with $\gamma(\epsilon) = \epsilon^m$ for some $0 < m < p$. Then γ^2 generates the unique subgroup of index 2 in $\text{Gal}(\mathbb{Q}_p/\mathbb{Q})$, and note that

$$\gamma^2(\alpha) = \sum_{i=0}^{p-1} \epsilon^{m^2 i^2} = \sum_{i=0}^{p-1} \epsilon^{(im)^2}$$

Since multiplication by m is a permutation (modulo p) of $\mathbb{Z}/p\mathbb{Z} = \{0, \dots, p-1\}$, we see that $\gamma^2(\alpha) = \alpha$. But $\alpha \notin \mathbb{Q}$ by the previous problem, since the map $c \mapsto c^2$ is not injective on $\mathbb{Z}/p\mathbb{Z}$ (both 1 and -1 map to 1), so the expression for α does not contain all primitive p th roots of unity. In particular, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 2$, and since the Galois group $\text{Gal}(\mathbb{Q}_p/\mathbb{Q})$ is cyclic, this is the unique degree 2 extension.

[20.13] First note that $i^2 - j^2 = (i-j)(i+j)$. If we write $u = i-j$ and $v = i+j$, then we can recover $i = (u+v)/2$ and $j = (v-u)/2$. So there is a bijection then from the set $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ to itself, sending (i, j) to $(i-j, i+j)$. All this implies, as in the problem's hint, that

$$\sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \epsilon^{i^2-j^2} = \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \epsilon^{uv}$$

Now $\alpha\bar{\alpha}$ is clearly equal to the sum on the left. Meanwhile, for the sum on the right, we have

$$\sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \epsilon^{uv} = \sum_{u=1}^{p-1} \sum_{v=0}^{p-1} \epsilon^{uv} + \sum_{v=0}^{p-1} \epsilon^0 = \sum_{u=1}^{p-1} \sum_{v=0}^{p-1} \epsilon^v + p = \sum_{u=1}^{p-1} 0 + p = p$$

The key here is that when $u \neq 0$, then $v \mapsto uv$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$, and the sum of all p th roots of unity is 0.

[20.14]

- (a) When $p \equiv 1 \pmod{4}$, then $\text{Gal}(\mathbb{Q}_p/\mathbb{Q})$ has order divisible by 4. That means the Galois group for $\mathbb{Q}[\alpha]/\mathbb{Q}$ has even order, and in particular contains the unique element of order 2 in $\text{Gal}(\mathbb{Q}_p/\mathbb{Q})$: the inversion map. Since α is fixed by this map, we see that $\alpha = \bar{\alpha}$; by the previous problem, then, $\alpha = \pm\sqrt{p}$.

- (b) For any integer k , k^2 is either 0 or 1 modulo 4. In particular, $i^2 + j^2 \not\equiv 0 \pmod{p}$ when $p \equiv 3 \pmod{4}$, unless $i = j = 0$. This implies that if $S = \{i^2 \mid i \in \mathbb{Z}/p\mathbb{Z}\}$, then $S \cap -S = \{0\}$. Note that $|S^*| = \frac{p-1}{2}$; this is because the squaring map on $(\mathbb{Z}/p\mathbb{Z})^*$ has kernel of order 2. So $S^* \cap -S^* = \emptyset$, and $\mathbb{Z}/p\mathbb{Z} = \{0\} \sqcup S^* \sqcup -S^*$, with every element of S^* having two preimages under the squaring map. All of this together gives us

$$\alpha + \bar{\alpha} = \left(1 + 2 \sum_{j \in S^*} \epsilon^j\right) + \left(1 + 2 \sum_{j \in -S^*} \epsilon^j\right) = 2 + 2 \sum_{j \neq 0}^{p-1} \epsilon^j = 2 \sum_{j=0}^{p-1} \epsilon^j = 0$$

From this and the previous problem, $\alpha = \pm i\sqrt{p}$.

- [20.15] Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial for β . Since $\text{Gal}(\mathbb{Q}_n/\mathbb{Q})$ is Abelian, all subgroups are normal, and hence all intermediate fields of $\mathbb{Q}_n/\mathbb{Q}$ are Galois. In particular, $K := \mathbb{Q}_n \cap \mathbb{R}$ is Galois. By assumption, $\beta \in K$, so that $f(x)$ actually has a root in K , so (by normality) splits over K . Let $\gamma \in K$ be any root of $f(x)$, and let $\sigma \in \text{Gal}(K/\mathbb{Q})$ be such that $\sigma(\beta) = \gamma$. Then

$$\gamma^{2m} = \sigma(\beta^{2m}) = \sigma(\beta^m)^2 = (\beta^m)^2 = \beta^{2m}$$

where we've used that $\beta^m \in \mathbb{Q}$ is fixed by σ . Since $\beta, \gamma \in \mathbb{R}$, we have that both β^2 and γ^2 are non-negative; together with $\gamma^{2m} = \beta^{2m}$ this means $\gamma^2 = \beta^2$. Of course, this is to say that $\gamma = \pm\beta$. Thus $f(x)$ has at most 2 distinct roots over K , and since it splits over K , must have degree at most 2. In fact, if $\beta \notin \mathbb{Q}$, then $f(x)$ has degree exactly 2, and since we know the 2 roots, we see $f(x) = x^2 - \beta^2$, so that $f(x) \in \mathbb{Q}[x]$ implies $\beta^2 \in \mathbb{Q}$. The case $\beta \in \mathbb{Q}$ trivially implies $\beta^2 \in \mathbb{Q}$.

- [20.16] Note that $i\beta \in \mathbb{R}$, so if $\beta^m \in \mathbb{Q}$, then $(i\beta)^{2m} \in \mathbb{Q}$. If $i \in \mathbb{Q}_n$, then by the previous problem, we have $(i\beta)^2 = -\beta^2 \in \mathbb{Q}$, so that $\beta^2 \in \mathbb{Q}$ as well. We can ensure $i \in \mathbb{Q}_n$ by replacing $\mathbb{Q}_n$ with the compositum $\langle \mathbb{Q}_n, \mathbb{Q}[i] \rangle$; this is $\mathbb{Q}_m$ for $m \geq n$ by Theorem 20.12.

[20.17]

- (a) If C is the group of n th roots of unity in E , then we have by assumption that $|C| = m$, and since $\text{Gal}(E/F)$ will act via automorphisms on C , we have a homomorphism $\text{Gal}(E/F) \rightarrow \text{Aut}(C) \cong U_m$. This map is injective since any element $\sigma \in \text{Gal}(E/F)$ that fixes all n th roots of unity must fix all of E , as the splitting field of $x^n - 1$. So

$$\phi(m) = |U_m| \geq |\text{Gal}(E/F)|$$

Meanwhile, $|\text{Gal}(E/F)| = [E : F]$, and $\bar{\Phi}_n$ is irreducible over F , of degree $\phi(n)$. Since this is an irreducible factor of $x^n - 1$, we see that $[E : F] \geq \phi(n)$. But U_m is a quotient of U_n (proved next), so all the inequalities above are equalities, and $\phi(m) = \phi(n)$. This means $U_m \cong U_n$ and $\text{Gal}(E/F) \cong U_m$.

To see U_m is a quotient of U_n , note that m divides n , since every element of the cyclic group C (of order m) has order dividing n . In particular, $\mathbb{Z}/n\mathbb{Z}$ maps onto $\mathbb{Z}/m\mathbb{Z}$. These rings are finite, hence Artinian. Then U_n maps onto U_m by [14.11].

(b) Since m divides n , if $m = \prod p_i^{\alpha_i}$ then $n = \prod p_i^{\beta_i}$ with $\beta_i \geq \alpha_i$. We have

$$\phi(p_i m) = \begin{cases} p_i \phi(m) & \alpha_i > 0 \\ (p_i - 1)m & \alpha_i = 0 \end{cases}$$

So if any $\beta_j > \alpha_j > 0$, we would have $\phi(n) \geq \phi(p_j m) > \phi(m)$. Similarly, if $p_j > 2$, then $\beta_j > \alpha_j$ means $\phi(n) > \phi(m)$. Since $\phi(n) = \phi(m)$, either $\alpha_j = \beta_j$ for all j (so that $n = m$), or $n = 2m$, and m is odd.

Suppose we're in the case $n \neq m$, so $n = 2m$. Now if $p \neq 2$, then F has a primitive second root of unity (namely, -1), and thus the splitting field E/F has an order 2 root of unity. Since 2 divides n , this implies that C has even order, contradicting that $|C| = m$ is odd. So we must have $p = 2$.

(c) There are no p th roots of unity in E . So if p divides n , then $C \subset E$ has order m strictly less than n . From the previous part, this means $p = 2$ and $n = 2m$ with m odd, so that 4 does not divide n .

(d) If $n \neq m$, then from the previous parts we know $p = 2$ so of course $\gcd(n, p-1) \leq 2$. So for now we assume $n = m$. Note that E is finite, so that E^* is cyclic. It thus has a unique subgroup of order $p-1$, which must be F^* . So $C \cap F$ is precisely those elements of C with order dividing $p-1$, and there are $\gcd(n, p-1)$ of those. So we're done if we show $|C \cap F| \leq 2$.

Every element of $C \cap F$ is fixed by every element of $\text{Gal}(E/F)$. Since $\text{Gal}(E/F)$ is isomorphic to the full automorphism group of C , there is an element $\sigma \in \text{Gal}(E/F)$ which acts by inversion on C . The only possible fixed points of the inversion map is the subgroup $\{c \in C \mid c^2 = 1\} \leq C$. Since $C \cap F$ is contained in this subgroup, and this subgroup has order at most 2, we see that $|C \cap F| \leq 2$ as desired.

[20.18] We suppose $n > 1$, the case $n = 1$ being trivial. Then if $\tau = \sqrt[n]{p}$, and ϵ is a primitive n th root of unity in $\mathbb{C}$, we see that both τ and $\epsilon\tau$ are roots of $x^n - p$, and thus their quotient $\epsilon \in E$. This means $F = \mathbb{Q}[\epsilon] \leq E$. Note $E = F[\tau]$; let $p(x) \in F[x]$ be the minimal polynomial for τ , with $m = \deg(p)$.

$p(x)$ is an irreducible factor in $F[x]$ of $x^n - p$. But so is $p_i(x) := p(\epsilon^i x)$ for all i . Since the roots of $x^n - p$ are all of the form $\epsilon^i \tau$, this shows that the $\{p_i(x)\}$ will all divide $x^n - p$, and will eventually cover all its roots. This just means that for some finite set I (we can assume $0 \in I$), we have

$$x^n - p = \prod_{i \in I} p_i(x)$$

This means that $n = m \cdot |I|$, so that m divides n . Let $\{\tau, \epsilon^{\alpha_1} \tau, \dots, \epsilon^{\alpha_k} \tau\}$ be the roots of $p(x)$. Looking at its constant term, we see that $\tau^m \epsilon^\alpha \in F$, where $\alpha = \sum \alpha_j$ and $\epsilon^\alpha \in F$. Thus $\tau^m \in F$. Since $(\tau^m)^n = p^m \in \mathbb{Q}$, we know from [20.15] that we must have $\tau^{2m} \in \mathbb{Q}$. But if $p^{2m/n} \in \mathbb{Q}$, by [16.4] n divides $2m$. So $m = n$ or $m = \frac{n}{2}$. And of course we have

$$[E : \mathbb{Q}] = [E : F][F : \mathbb{Q}] = m\phi(n)$$

The case $m = \frac{n}{2}$ does happen. Since $E = F[\tau]$, and $[F : \mathbb{Q}]$ is Galois, natural irrationalities says that $[E : F] = \frac{n}{2}$ precisely when $F \cap \mathbb{Q}[\tau]$ is a quadratic extension of $\mathbb{Q}$, for example when $\sqrt{p} \in F$. This happens though: $\mathbb{Q}_8 = \mathbb{Q}[i, \sqrt{2}]$, and thus $\mathbb{Q}_8 \cap \mathbb{Q}[\sqrt[8]{2}] = \mathbb{Q}[\sqrt{2}]$. So the splitting field of $x^8 - 2$ has degree 16, not 32.

[20.19] Of course, by Lemma 20.25, if $\alpha \in K$, then $\sqrt{\alpha} \in K$ as well, so K is closed under taking square roots. The smallest such subfield is just the intersection of all subfields of $\mathbb{C}$ closed under taking square roots. Now suppose there is a field $L \subset K$ that is closed under square roots. If $\alpha \in K$, Theorem 20.18 shows there is a Galois extension $E/\mathbb{Q}$ with degree 2^n and $\alpha \in E \subset K$. The theorem gives us a chain of quadratic extensions $\mathbb{Q} = E_0 \subset E_1 \subset \cdots \subset E_n = E$. We show that each $E_i \subset L$, and this implies $\alpha \in L$. Since α was arbitrary, this shows $K \subset L$ and we're done.

We induct on i to show $E_i \subset L$, the case $i = 0$ (and $E_0 = \mathbb{Q}$) being obvious. Now if $E_i \subset L$, then $[E_{i+1} : E_i] = 2$, and thus there's an element $\beta \in E_i$ with $E_{i+1} = E_i[\sqrt{\beta}]$. Since $\beta \in L$ and L is closed under square roots, $\sqrt{\beta} \in L$, and thus $E_{i+1} \subset L$ as desired.

[20.20] Let a, b, c be the sides of a triangle, constructible by hypothesis. Heron's formula gives the area as

$$A = \sqrt{s(s-a)(s-b)(s-c)} \quad s = \frac{a+b+c}{2}$$

This is the square root of a constructible number, hence constructible. But then $\sqrt{A}$ is constructible as well, and we can make a square with side length $\sqrt{A}$, hence of area A .

Chapter 21

[21.1] Let E be the splitting field over $F := GF(2)$ of $f(x) = x^3 + x + 1$, with $\alpha \in E$ a root of $f(x)$. $f(x)$ is irreducible (it has no root in F), so $[F[\alpha] : F] = 3$. By Corollary 21.5, $F[\alpha] \cong GF(8)$. Since $|F[\alpha]^*| = 7$ is prime, every non-identity element is a generator of the cyclic multiplicative group, so in particular $F[\alpha]^* = \langle \alpha \rangle$, with $\alpha^3 + \alpha + 1 = f(\alpha) = 0$. Using the identity $\alpha^3 = \alpha + 1$ and the fact the characteristic is 2, we can write the addition table of $F[\alpha]$ (seen on next page).

[21.2] Let E be the splitting field of $f(x) = x^2 - 3$ over $GF(5)$. Note $f(x)$ is irreducible because it has no root in $GF(5)$. So $[E : F] = 2$ and by Corollary 21.5, $E \cong GF(25)$. There is a root $\epsilon \in E$ of $f(x)$, so $\epsilon^2 = 3$. Because $\epsilon \notin GF(5)$, it must be that $\{1, \epsilon\}$ is F -linearly independent, and from $[E : F] = 2$ we see they form an F -basis for E . Now E^* has order 24, so for an element $a \in E$ to *not* be a generator, it would have to have order less than 24, but still dividing $24 = 2^3 \cdot 3$. So if both $a^{12} \neq 1$ and $a^8 \neq 1$, then a is in fact a generator for E^* . We have

$$(1 + \epsilon)^{12} = (1 + \epsilon)^{10}(1 + \epsilon)^2 = (1 + \epsilon^5)^2(1 + \epsilon)^2 = (1 - \epsilon)^2(1 + \epsilon)^2 = 3^2 = -1$$

Table 1: Addition table of $GF(8)$

+	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	1	α	α^2	α^3	α^4	α^5	α^6
1	1	0	α^3	α^6	α	α^5	α^4	α^2
α	α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^6	α^2	α^5	1	α^4	α^3	α	0

Similarly, $(1 + \epsilon)^8 = 2 + \epsilon \neq 1$, so $1 + \epsilon$ has order 24 and generates E^* .

[21.3] Let $E = GF(q^n)$ with $F = GF(q)$ a subfield of E . Since E^* is cyclic, let α be a generator. Then if $\phi(x) = \alpha x$ as a map from $E \rightarrow E$, this map is linear (by the distributive property) and F -linear (by commutativity). It thus represents an element of $GL(n, q)$ since $[E : F] = n$. But if $\phi^m \equiv 1$, then $1 = \phi^m(1) = \alpha^m$; since α has order $q^n - 1$, we see that so does ϕ as an element of $GL(n, q)$.

[21.4] Let E be the splitting field of Φ_n over $F = GF(p)$. By Lemma 21.10, $Gal(E/F)$ is cyclic; by part (a) of [20.17], this means that U_n is cyclic. If $n = 2^a p_1^{a_1} \cdots p_r^{a_r}$, then by Lemma 20.11 we have

$$U_n \cong U_{2^a} \times U_{p_1^{a_1}} \times \cdots \times U_{p_r^{a_r}}$$

Since U_{p^a} is isomorphic to the automorphism group of the cyclic group C_{p^a} , whenever $p^a > 2$, it must contain an element of order 2: inversion. So if more than one odd prime divides n , or $r > 0$ and $a > 1$, the above equation shows U_n has more than one element of order 2, which is impossible in a cyclic group. So either $n = 2p_1^{a_1}$ or $n = 2^a$. But U_8 is not cyclic: each element $\{1, 3, 5, 7\}$ squares to 1. Since $\mathbb{Z}/\langle 2^a \rangle$ has $\mathbb{Z}/\langle 8 \rangle$ as a quotient for $a \geq 3$, [14.11] shows U_{2^a} has U_8 as a quotient, and thus it also cannot be cyclic. So when $n = 2^a$ then $a < 3$, and thus n divides 4.

[21.5] Since $x^4 + 1 = \Phi_8(x)$, the previous problem shows $\Phi_8(x)$ is not irreducible modulo any prime p . Since any finite field $GF(q)$ will contain its prime subfield $GF(p)$, and $x^4 + 1$ isn't irreducible over $GF(p)$, it cannot be irreducible over any finite field.

[21.6] Any irreducible polynomial over $GF(2)$ must have an odd number of monomial terms, since otherwise 1 is a root. So the possibilities are:

$$x^4 + x^3 + 1 \quad x^4 + x^2 + 1 \quad x^4 + x + 1 \quad x^4 + x^3 + x^2 + x + 1$$

These don't have a root over $GF(2)$, but there is a single irreducible quadratic over $GF(2)$: $x^2 + x + 1$. Its square will be a reducible quartic, and its square is $x^4 + x^2 + 1$. Removing that from the above list, we see there are 3 irreducible quartics over $GF(2)$, agreeing with Theorem 21.11.

[21.7] Fix i and for every $j \neq i$, let $a_j + b_j = 1$ in R , with $a_j \in I_i$ and $b_j \in I_j$. Then we have

$$1 = \prod_{j \neq i} (a_j + b_j) = (\prod_{j \neq i} a_j + \cdots) + \prod_{j \neq i} b_j$$

where the expression in parentheses on the right-hand side belongs to I_i , since each term has at least one a_j factor. Meanwhile, $\prod_{j \neq i} b_j$ is a member of every I_j with $j \neq i$. Write c_i for this product of the b_j . Then $1 - c_i \in I_i$, and so in the map of the problem with $R \rightarrow (R/I_1) \oplus \cdots \oplus (R/I_m)$, c_i maps to the element e_i , which has 0 in every coordinate except a 1 in the i th position. Doing this for every $1 \leq i \leq m$, we see that

$$\sum r_i c_i \mapsto (r_1, \dots, r_m)$$

and so our map is surjective. The kernel D is elements of R in every I_i ; that is, $D = \cap I_i$. So we have the desired isomorphism.

[21.8] Suppose $[F[\alpha] : F] = n$. Then $F[\alpha]$ has order q^n , and hence $\alpha^{q^n} = \alpha$. If $\alpha^{q^m} = \alpha$, then let $L \leq E$ be the subset $L = \{a \in E \mid a^{q^m} = a\}$. This contains both F and α , and since it's a field (by Lemma 21.4), we see $F[\alpha] \leq L$. Let $|L| = q^r$, so that $[L : F] = r$. Then by Theorem 21.7, n divides r . If $\beta \in L^*$ is a multiplicative generator (of order $q^r - 1$), then from $\beta^{q^m} = \beta$, we see that $q^r - 1$ divides $q^m - 1$; again by Theorem 21.7, this implies r divides m . Altogether then, n divides m , as desired.

[21.9] let E be a splitting field of $f(x) = x^q - x - 1$ over $F = GF(q)$. Note that $f(x)$ has no roots in F , since $a^q = a$ for all $a \in F$. If $\alpha \in E$ is a root of $f(x)$, then $\alpha^q = \alpha + 1$, and repeatedly raising both sides to the q th power shows $\alpha^{q^p} = \alpha$ (since $p \cdot 1 = 0$). Since $\alpha \notin F$, the previous problem shows $[F[\alpha] : F] = p$. Thus the minimal polynomial of α over F has degree p ; since as α moves through all the roots of $f(x)$, this will cover all irreducible factors of $f(x)$, we are done.

[21.10] Since R is a finite ring, it is Artinian. Because R has no nonzero nilpotent elements, it has no nonzero nilpotent ideals, and is thus a Wedderburn ring. By Theorem 14.15, R is isomorphic to a direct sum of matrix rings over division rings. Every such division ring will be finite (since R is), so by Wedderburn's theorem is actually a field. Since $M_n(F)$ has nilpotent elements when $n > 1$ (for example, e_{12}), we see that R is actually a direct sum of fields, hence commutative.

[21.11] Let $R = \langle S \rangle \leq \text{End}(A)$ be the subring generated by S . The hypotheses of the problem imply that A is a simple R -module, and hence $\text{End}_R(A) = C_{\text{End}(A)}(R)$ is a division ring by Schur's lemma. Because A (and hence $\text{End}(A)$) is finite, Wedderburn's theorem implies $C_{\text{End}(A)}(R)$ is a finite field. The nonzero elements of $C_{\text{End}(A)}(R)$ thus form a cyclic group, say generated by θ , and $C_{\text{End}(A)}(S) = C_{\text{End}(A)}(R)$, so every nonzero element is a power of θ .

Chapter 22

[22.1] Of course if E is a repeated square-root extension of F , it is contained in one, so (i) implies (ii). Similarly, a square-root extension F_1 over F_0 has degree dividing 2, so inductively a repeated square-root extension F_r over F has degree a power of 2. If $E \leq F_r$, then $[E : F]$ divides $[F_r : F]$, so $[E : F]$ is also a power of 2. All this says that (ii) implies (iii).

Now assume $[E : F] = 2^n$, and we want to show that E is a repeated square-root extension. We do this by induction on n , the case $n = 0$ being trivial. Recalling that E/F is Galois by hypothesis, we see the Galois group G_F^E is a finite 2-group of order 2^n . It thus has a normal subgroup of order 2 (contained in its non-trivial center), call it $L \triangleleft G$. The corresponding field $K \leq E$ is such that $[K : F] = 2^{n-1}$. By induction, K is a repeated square-root extension. Since $[E : K] = 2$, there is some element $\alpha \in E$ with $f(\alpha) = 0$ for a quadratic polynomial $f(x) \in K[x]$, and of course $E = K[\alpha]$. By "completing the square" (this is where we need the characteristic of F is not 2), we can find an element $\beta \in E$ with $\beta^2 \in K$ and $E = K[\beta]$. Thus E is a repeated square-root extension of F .

[22.2] Let the Galois group $G_F^E \cong C_{n_1} \times \cdots \times C_{n_r}$ be a decomposition into a product of finite cyclic groups. Let $H_i \leq G_F^E$ be the (normal) subgroup

$$H_i = \prod_{j \neq i} C_{n_j}$$

So $C_{n_i} \times H_i = G_F^E$. Finally let K_i be the fixed field of H_i . Then by the fundamental theorem of Galois theory, we have $G_F^{K_i} \cong C_{n_i}$ is cyclic, of order n_i dividing n . By Kummer's theorem then, there exists $\alpha_i \in K_i$ with $\alpha_i^{n_i} \in F$ and $K_i = F[\alpha_i]$.

If $K = \langle K_1, \dots, K_r \rangle$, then the fundamental theorem shows

$$G_F^K = \bigcap_{1 \leq i \leq r} H_i = \{1\}$$

so that $K = E$, and thus $E = F[\alpha_1, \dots, \alpha_r]$. Thus E is generated over F by some roots of the polynomial $f(x) \in F[x]$ with

$$f(x) = \prod_{1 \leq i \leq r} (x^{n_i} - \alpha_i^{n_i})$$

Since F contains n th roots of unity, all roots of $f(x)$ are contained in E , and hence E is a splitting field for $f(x)$.

[22.3]

- (a) Let $f(x) = (x^{2n} + 2)(x - 2) \cdots (x - 2m)$. Note that this polynomial has exactly m real roots, namely $\{2, \dots, 2m\}$. Now let $g_k(x) = f(x) - \frac{2}{k}$ for an odd positive integer k . $g_k(x)$ is irreducible since $kg_k(x)$ satisfies Eisenstein's criterion at the prime 2; Gauss's lemma ensures a factorization of $g_k(x)$ over $\mathbb{Q}[x]$ would yield a factorization of $kg_k(x)$ over $\mathbb{Z}[x]$.

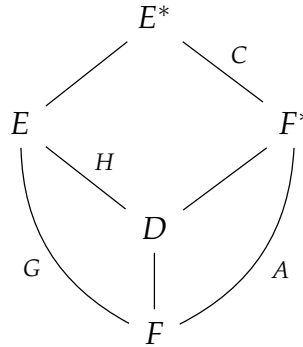
Since $g_k(x)$ shifts the graph of $f(x)$ in $\mathbb{R}^2$ down by $\frac{2}{k}$, it will continue to have at least m real roots (this relies on $f(x)$ having no repeated real roots). It won't pick up any additional real roots as long as the graph doesn't cross the x -axis anew after the shift. In particular, if $\frac{2}{k} < f(c)$ at all points where $f'(c) = 0$ and $f(c) > 0$, then all local minimums of $f(x)$ above the x -axis will remain above the x -axis after the shift. So $g_k(x)$ has exactly m real roots for these values of k .

- (b) In the previous part let $m = p - 2$ and $n = 1$. Then $g_k(x)$ has degree p and exactly $p - 2$ real roots when k is large enough. By Lemma 22.5, the splitting field of $g_k(x)$ over $\mathbb{Q}$ has Galois group S_p .

[22.4] We can obviously reduce to the case F has positive characteristic p . Let $n = p^k m$ with m not divisible by p . By Corollary 18.12 $F[\alpha^m]$ is separable over F . Since $(\alpha^m)^{p^k} \in F$, however, Corollary 19.11 shows $F[\alpha^m]$ is purely inseparable over F . This can only happen if $F[\alpha^m] = F$, so that $\alpha^m \in F$ as desired.

[22.5]

- (a) We assume n is coprime to the characteristic of F , which is possible by the last problem. Let $F^* = F[\epsilon]$, where ϵ is a primitive n th root of unity, following Lemma 20.3. We then have the following diagram of fields:



Here we've labeled edges by Galois groups, with $G = \text{Gal}(E/F)$. We have $D = E \cap F^*$ and $E^* = \langle E, F^* \rangle = F^*[\alpha]$. By Kummer's theorem E^*/F^* is Galois with group C , cyclic of order dividing n . By natural irrationalities (which applies since E/D is Galois), we see that $H \cong C$ is also cyclic. By Lemma 20.7 F^*/F is Galois and the Galois group A is Abelian. The fundamental theorem of Galois theory then ensures D/F is Galois, and its Galois group must also be Abelian (let's call it B). Again by the fundamental theorem, we see that $G/H \cong B$ is Abelian, so $G' \leq H$. Since H is cyclic, this implies G' is cyclic as well.

- (b) If n is prime, then in the above diagram, $|H| = 1$ or p . If H is trivial, then $E = D$ and $E \leq F^*$. Since the Galois group A of F^*/F is cyclic because n is prime, this implies $\text{Gal}(E/F)$ is also cyclic, as a quotient of A .

If $|H| = p$, then $D = F$ (since $[E : F] \leq n$), and $G = H$ is cyclic.

[22.6]

- (a) Let $F = \mathbb{Q}[i]$ and $L = \mathbb{Q}[\sqrt[8]{2}]$. Since L is real and $[F : \mathbb{Q}] = 2$, we see $F \cap L = \mathbb{Q}$. And of course, $E = \langle F, L \rangle$. We know that $\sqrt[8]{2}$ satisfies $x^8 - 2$, which is irreducible by Eisenstein's criterion, so $[L : \mathbb{Q}] = 8$. Since $F/\mathbb{Q}$ is Galois, natural irrationalities tells us $[E : \mathbb{Q}] = [F : \mathbb{Q}][L : \mathbb{Q}] = 16$.
- (b) We write $\alpha = \sqrt[8]{2}$, and let ϵ be a primitive 8th root of unity, which is contained in E ; to see this, note

$$\epsilon = \frac{1+i}{\sqrt{2}}$$

Now E is a splitting field of $f(x) = x^8 - 2$ over F , and $E = F[\alpha]$. Since $[E : F] = 8$ we know that $f(x)$ is irreducible over F . Thus the identity map on F extends to a map $\sigma : F[\alpha] \rightarrow F[\alpha\epsilon]$ by Lemma 17.15, and then extends to a map $\sigma : E \rightarrow E$ by Theorem 17.22; this means $\sigma \in \text{Gal}(E/F)$. Of course $\sigma(i) = i$ since $i \in F$, and also

$$\sigma(\sqrt{2}) = \sigma(\alpha^4) = \sigma(\alpha)^4 = -\sqrt{2}$$

This implies $\sigma(\epsilon) = -\epsilon$. Note we have

$$\begin{aligned}\sigma^2(\alpha) &= \sigma(\alpha)\sigma(\epsilon) \\ &= -\alpha i \\ \sigma^4(\alpha) &= -\sigma^2(\alpha)i \\ &= -\alpha\end{aligned}$$

Since $\text{Gal}(E/F)$ has order $[E : F] = 8$, this implies $\text{Gal}(E/F) = \langle \sigma \rangle$ is cyclic.

- (c) Let $K = \mathbb{Q}[i\sqrt{2}]$, so that $[E : K] = 8$ and $E = K[\alpha]$. If τ is complex conjugation, then both σ and τ are in $\text{Gal}(E/\mathbb{Q})$, but not in $\text{Gal}(E/K)$. Since $\text{Gal}(E/K)$ is a normal index 2 subgroup of $\text{Gal}(E/\mathbb{Q})$, it must be that both σ^2 and $\sigma\tau$ are in $\text{Gal}(E/K)$. But

$$\begin{aligned}\sigma^3\tau(\alpha) &= \sigma(-\alpha i) \\ &= -i\alpha\epsilon \\ \sigma\tau\sigma^2(\alpha) &= \sigma\tau(-\alpha i) \\ &= \sigma(\alpha i) \\ &= i\alpha\epsilon\end{aligned}$$

So that $(\sigma^2)(\sigma\tau) \neq (\sigma\tau)(\sigma^2)$ and $\text{Gal}(E/K)$ is non-Abelian.

[22.7]

- (a) if $f(x) = x^4 - 6x^2 + 7$, then

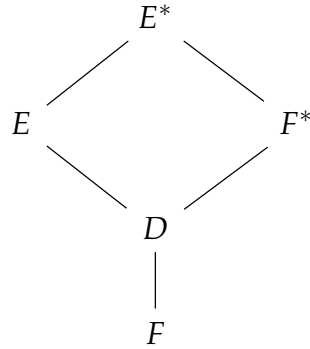
$$f(x+1) = x^4 + 4x^3 - 8x + 2$$

and this is irreducible by Eisenstein's criterion, hence so is $f(x)$.

- (b) The quadratic formula shows the roots of $f(x)$ are $\pm\sqrt{3 \pm \sqrt{2}}$. Let $\alpha = \sqrt{3 + \sqrt{2}}$ and $\beta = \sqrt{3 - \sqrt{2}}$. All these roots are real, and hence by Theorem 22.15 $[E : \mathbb{Q}]$ is a power of 2, so that $\text{Gal}(E/\mathbb{Q})$ is a 2-group. If $\text{Gal}(E/\mathbb{Q})$ was Abelian, then $E = \mathbb{Q}[\alpha]$ (since then $\mathbb{Q}[\alpha]$ is Galois over $\mathbb{Q}$ by the fundamental theorem). This would mean $[E : \mathbb{Q}] = 4$, so to show $\text{Gal}(E/\mathbb{Q})$ is non-Abelian, it's enough to show $[E : \mathbb{Q}] > 4$, or equivalently that $E \neq \mathbb{Q}[\alpha]$.

If $E = \mathbb{Q}[\alpha]$, then also $E = \mathbb{Q}[\beta]$. Thus $\mathbb{Q}[\alpha] = \mathbb{Q}[\beta]$ would both be the same quadratic extension over $\mathbb{Q}[\sqrt{2}]$. Now $x^2 - \alpha^2$ is an irreducible polynomial over $\mathbb{Q}[\sqrt{2}]$, so the non-trivial Galois automorphism sends α to $-\alpha$, and must do the same thing to β . This implies $\alpha\beta = \sqrt{7}$ would be fixed by the Galois group, so that $\sqrt{7} \in \mathbb{Q}[\sqrt{2}]$. Since this is false by [18.12], we see $\mathbb{Q}[\alpha] \neq \mathbb{Q}[\beta]$ and thus $[E : \mathbb{Q}] > 4$ and $\text{Gal}(E/\mathbb{Q})$ is non-Abelian.

- [22.8] Since n is coprime to the characteristic of F , we can adjoin a primitive n th root of unity: $F^* = F[\epsilon]$, and similarly $E^* = E[\epsilon] = F^*[\alpha]$. We can then form the diagram



Now F^*/F is Galois, so natural irrationalities applies, and $[E : D] = [E^* : F^*]$. By Kummer's theorem, the latter index divides n , and of course $[E : D]$ divides $[E : F]$, so by hypothesis $[E : D] = 1$, and $E = D$. Then E is Galois over F with Abelian Galois group, by the fundamental theorem and the fact $\text{Gal}(F^*/F)$ is Abelian.

Chapter 23

[23.1]

- (a) Let $\theta : V \rightarrow F^n$ be given by mapping a matrix to its first row. This is F -linear, and if $\theta(A) = \theta(B)$, then $\theta(A - B) = 0$. This means the first row of $A - B \in V$ is all zeroes, so cannot be invertible. By hypothesis, $A - B = 0$ so $A = B$. In other words, θ is injective, so $\dim(V) \leq \dim(F^n) = n$.
- (b) Assume $\dim(V) > 1$, and let $A, B \in V$ be linearly independent matrices. If $f(x)$ is the characteristic polynomial $\det(xI - AB^{-1})$, then $f(x) \in F[x]$ has degree n . Now if $\lambda \in F$ was such that $f(\lambda) = 0$, that would mean $\lambda I - AB^{-1}$ was non-invertible,

and multiplying with B on the right shows that $\lambda B - A \in V$ is non-invertible. Again, by hypothesis this means $A = \lambda B$, and linear independence means a contradiction. So $f(x)$ has no linear irreducible factors; if $g(x)$ is an irreducible factor of $f(x)$, an extension E/F with a root of $g(x)$ would be such that $1 < [E : F] \leq n$.

- (c) Define $\rho : E \rightarrow M_n(F)$ by letting $\rho(\alpha)$ be the matrix corresponding to multiplication by α in the n -dimensional vector space E over F . This is injective (since $\alpha \cdot 1 = 0$ implies $\alpha = 0$), and since it's F -linear the image $\rho(E) \leq M_n(F)$ is an n -dimensional F -vector subspace.

[23.2] Let L/E be an extension so that L/F is Galois. Then if $G = \text{Gal}(L/F)$, there are subgroups $H \leq J \leq G$ such that $\text{Gal}(L/E) = H$ and $\text{Gal}(L/K) = J$. Let U be a set of coset representatives for H in J , and V a set of coset representatives for J in G , so that UV is a set of coset representatives for H in G .

- (a) By Corollary 23.10,

$$N_{E/F}(\alpha) = \prod_{uv \in UV} \alpha^{uv} = \prod_{v \in V} \left(\prod_{u \in U} \alpha^u \right)^v = \prod_{v \in V} N_{E/K}(\alpha)^v = N_{K/F}(N_{E/K}(\alpha))$$

- (b) By Corollary 23.10,

$$T_{E/F}(\alpha) = \sum_{uv \in UV} \alpha^{uv} = \sum_{v \in V} \left(\sum_{u \in U} \alpha^u \right)^v = \sum_{v \in V} T_{E/K}(\alpha)^v = T_{K/F}(T_{E/K}(\alpha))$$

[23.3] By [19.13], for $\alpha \in E$ we have $\alpha^n \in F$. Then

$$N_{E/F}(\alpha)^n = N_{E/F}(\alpha^n) = \alpha^{n^2}$$

Since n is a power of the characteristic of F by Corollary 19.12, the above can be rewritten as

$$0 = N_{E/F}(\alpha)^n - \alpha^{n^2} = (N_{E/F}(\alpha) - \alpha^n)^n$$

And thus $N_{E/F}(\alpha) = \alpha^n$.

[23.4] First we handle the case where F has characteristic 0. Then since $\alpha^n = N_{E/F}(\alpha)$ is in F for all $\alpha \in E$, Theorem 22.19 shows $E = F$, so it is (trivially) a purely inseparable extension.

Next consider the case F has characteristic p . Let S with $F \leq S \leq E$ be the field of separable elements of E over F . We also write $r = [E : S]$ and $s = [S : F]$, noting that r is a power of p by Corollary 19.12. By the primitive element theorem we may write $S = F[\alpha]$ for some element $\alpha \in S$. Of course $(\alpha^r)^s = \alpha^n \in F$ by hypothesis. But also

$$(\alpha^r + 1)^s = [(\alpha + 1)^r]^s = (\alpha + 1)^n \in F$$

Now $F[\alpha^r] \leq S$, but α is a root of $f(x) = x^r - \alpha^r = (x - \alpha)^r$, so the minimal polynomial of α over $F[\alpha^r]$ divides $f(x)$. Since α is separable over F (and hence $F[\alpha^r]$), its minimal polynomial must be degree 1, so that $\alpha \in F[\alpha^r]$ and $S = F[\alpha^r]$. But then write $N_{E/F}(\alpha) = \beta$ and $N_{E/F}(\alpha + 1) = \gamma$. From above we have that α^r is a root of the polynomial

$$x^s - \beta - (x + 1)^s + \gamma$$

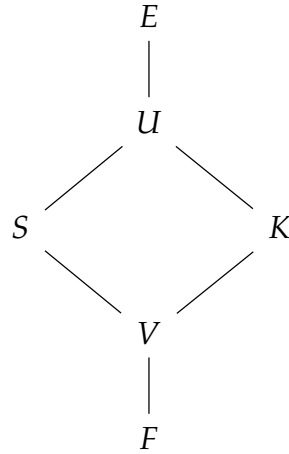
and if $s > 1$ this is a non-zero polynomial of degree $< s$. This contradicts that $[F[\alpha^r] : F] = s$, so it must be $s = 1$ and E/F is purely inseparable.

[23.5] If E/F is separable, there's nothing to show. So assume E/F is inseparable, with $F \leq S \leq E$ and S the separable subfield. Since E/S is purely inseparable and $[E : S] = r$, problem [19.13] shows $\alpha^r \in S$. By Corollary 23.8, $N_{E/F}(\alpha^r) = N_{S/F}(\alpha^r)^r$. We then have (recalling that r is a power of the characteristic of F)

$$0 = N_{E/F}(\alpha^r) - N_{S/F}(\alpha^r)^r = N_{E/F}(\alpha)^r - N_{S/F}(\alpha)^r = (N_{E/F}(\alpha) - N_{S/F}(\alpha))^r$$

And so $N_{E/F}(\alpha) = N_{S/F}(\alpha)$.

[23.6] If E/F is inseparable, then one of K/F or E/K is inseparable, so the traces on both side of [23.2] (b) are zero. So we focus on the norms. We assume that E/F is inseparable and write $F \leq S \leq E$ with S the separable subfield. We also let U be the separable subfield of E/K (so that $\langle K, S \rangle \leq U$), and $V = K \cap S$, to give the diagram



Any element of K that is separable over F is in $S \cap K = V$, so K/V is purely inseparable. And of course U/S is purely inseparable. We then have from the previous problem

$$N_{K/F}(N_{E/K}(\alpha)) = N_{K/F}(N_{U/K}(\alpha^{[E:U]})) = N_{V/F}(N_{U/K}(\alpha^{[E:U]})^{[K:V]})$$

If $\beta \in S$, then Lemma 19.20 shows the minimal polynomial of β over V (which will be separable) is still irreducible over K , so β has the same minimal polynomial over V and K . Since the norm is determined by this minimal polynomial, we see that $N_{S/V}(\beta) = N_{U/K}(\beta)$. Using the previous problem and [23.3] gives

$$N_{E/F}(\alpha) = N_{S/F}(\alpha^{[E:S]}) = N_{V/F}(N_{S/V}(\alpha^{[E:S]})) = N_{V/F}(N_{U/K}(\alpha^{[E:S]}))$$

Since norms are multiplicative, the first equation above shows

$$N_{K/F}(N_{E/K}(\alpha)) = N_{V/F}\left(N_{U/K}\left(\alpha^{[E:U][K:V]}\right)\right)$$

Meanwhile $[K : V] = [U : S]$ by Theorem 19.19, so the second equation above gives

$$N_{E/F}(\alpha) = N_{V/F}\left(N_{U/K}\left(\alpha^{[E:U][U:S]}\right)\right) = N_{V/F}\left(N_{U/K}\left(\alpha^{[E:U][K:V]}\right)\right)$$

These are the same, and we are done.

[23.7] By Theorem 21.10, $\text{Gal}(E/F) = \langle \sigma \rangle$ where $\sigma(\alpha) = \alpha^q$. Then

$$N_{E/F}(\alpha) = \prod_{i=0}^{n-1} \sigma^i(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i} = \alpha^{\sum q^i} = \alpha^{(q^n-1)/(q-1)}$$

[23.8] Let $\sigma \in \text{Gal}(E/F)$ be as in the previous problem. Consider the map θ given by $\theta(\alpha) = \alpha^\sigma / \alpha$. If $\theta(\alpha) = 1$, then $\alpha^\sigma = \alpha$, and thus α is fixed by all elements of $\text{Gal}(E/F)$; that is, $\alpha \in F$. So we see $\ker(\theta)$ has order $q - 1$. This means the image has size $(q^n - 1)/(q - 1)$. By Hilbert's Theorem 90, this image set is exactly the kernel of $N_{E/F}$.

[23.9] First, if $\alpha = \beta^\sigma - \beta$, then

$$T_{E/F}(\alpha) = T_{E/F}(\beta^\sigma) - T_{E/F}(\beta) = 0$$

where the last equality holds from Corollary 23.12. Now suppose that $T_{E/F}(\alpha) = 0$. Corollary 23.11 shows that

$$T_{E/F}(\alpha) = \sum_{i=0}^{n-1} \sigma^i(\alpha)$$

If $\psi(k) = \alpha + \sigma(\alpha) + \cdots + \sigma^{k-1}(\alpha)$, then $\psi(1) = \alpha$ and $\psi(n) = 0$. We also have

$$\psi(k+m) = \psi(k)\sigma^k(\psi(m))$$

This shows that $\psi(k+n) = \psi(k)$ and if we define $\hat{\psi}(\sigma^k) = \psi(k)$, we get a well-defined crossed homomorphism. By Corollary 23.16, this must be a principal crossed homomorphism, so that $\alpha = \hat{\psi}(\sigma) = \beta^\sigma - \beta$ for some $\beta \in E$.

[23.10] Because $G = KA$ and $K \cap A = \{1\}$, every element of G has a unique expression as ka , with $k \in K$ and $a \in A$. So if $x \in H$, we can write $x = ka$, and then $xa^{-1} \in K$. If there was a $b \in A$ with $xb \in K$, then $(xa^{-1})^{-1}(xb) = ab \in K \cap A$ implies $a = b^{-1}$, so we have uniqueness.

If $xa, yb \in K$ for $x, y \in H$ and $a, b \in A$, then $xy(a^y b) \in K$. So if we define $\theta : H \rightarrow A$ so that $\theta(x)$ is this unique element of A with $x\theta(x) \in K$, we see

$$\theta(xy) = \theta(x)^y \theta(y)$$

and θ is a crossed homomorphism.

Conversely, let $\theta : H \rightarrow A$ be a crossed homomorphism, and define the set $K = \{x\theta(x) \mid x \in H\}$. Since $\theta(1) = \theta(1 \cdot 1)$, being a crossed homomorphism implies $\theta(1) = 1$. Similarly, because $\theta(1) = \theta(x^{-1}x)$, being a crossed homomorphism shows $\theta(x)^{-1} = \theta(x^{-1})^x$. This means that

$$[x\theta(x)]^{-1} = \theta(x^{-1})^x x^{-1} = x^{-1}\theta(x^{-1}) \in K$$

and K is closed under inverse. For products we see

$$x\theta(x)y\theta(y) = xy\theta(x)^y\theta(y) = xy\theta(xy) \in K$$

So K is a subgroup of G . If $a \in A \cap K$, then $a = x\theta(x)$ and $x \in H \cap A$, so $x = a = 1$. Also, as H is contained in KA , we must have $G = HA \leq KA$, and K is a complement of A .

[23.11] We use the setup of the previous problem. if $\theta : H \rightarrow A$ is a principal crossed homomorphism, then there is an $a \in A$ with $\theta(x) = a^x a^{-1}$. But then $x\theta(x) = axa^{-1}$ and so $K = aHa^{-1}$. Conversely, if $H = K^g$, then since $g = ka$, we can say $H = K^a$. Then for $x \in H$, the unique element $\theta(x) \in A$ such that $x\theta(x) \in K$ is $\theta(x) = [x, a^{-1}]$, and θ is a principal crossed homomorphism.

[23.12]

- (a) Note that every element in the coset of $g \in G$ looks like bx_g with $b \in A$, and from the fact A is Abelian we have $a^g = a^{bx_g} = a^{x_g}$. So this map is well-defined, and we just need to show it's an action. Since $x_1 \in A$, clearly $a^1 = a$, and for $g, h \in G$ we have

$$a^{gh} = a^{x_{gh}} = a^{x_g x_h z} = (a^{x_g})^{x_h}$$

Here $z \in A$. So we do in fact have a well-defined action.

- (b) Let $g, h, r \in G$. Let $c = \phi(h, r)$ so that $x_h x_r = x_{hr} c$. Also let $b = \phi(g, hr)$, meaning $x_g x_{hr} = x_{ghr} b$. Together this implies

$$x_g x_h x_r = x_g x_{hr} c = x_{ghr} b c$$

Now also let $a = \phi(gh, r)$ so that $x_{gh} x_r = x_{ghr} a$. And finally let $d = \phi(g, h)$ so that $x_g x_h = x_{gh} d$. Together these two imply

$$x_g x_h x_r = x_{gh} d x_r = x_{gh} x_r d^{x_r} = x_{ghr} a d^{x_r}$$

Equating these two expressions and using the action defined in part (a), we have

$$\phi(g, hr)\phi(h, r) = \phi(gh, r)\phi(g, h)^r$$

and ϕ is a factor set.

- (c) If a complement H exists, then for every $x_g \in X$ there's a unique element $h_g \in H$ with $h_g = x_g a_g$. Define the function $\theta : G \rightarrow A$ by $\theta(g) = a_g$. Note that

$$x_g a_g x_r a_r = x_g x_r a_g^r a_r = x_{gr} \phi(g, r) a_g^r a_r$$

Since the element on the left is in H , this implies $\theta(gr) = \phi(g, r) \theta(g)^r \theta(r)$, which is another way to say

$$\phi(g, r) = \theta(g)^{-r} \theta(r)^{-1} \theta(gr)$$

Taking $\nu(g) = \theta(g)^{-1}$, we see $\delta^1(\nu) = \phi$, so ϕ is a coboundary.

Conversely, suppose $\delta^1(\nu) = \phi$. Define the subset $H = \{x_g \nu(g)^{-1} \mid x \in G\}$. We will show H is a subgroup, and a complement to A . For $g, r \in G$ we have

$$\begin{aligned} \nu(g) x_g^{-1} &= \left(\nu(1) \phi(g^{-1}, g) \nu(g^{-1})^{-g} \right) x_g^{-1} \\ &= \nu(1) x_1^{-1} x_{g^{-1}} x_g \nu(g^{-1})^{-g} x_g^{-1} \\ &= (\nu(1) x_1^{-1}) x_{g^{-1}} \nu(g^{-1})^{-1} \\ &= x_{g^{-1}} \nu(g^{-1})^{-1} \\ x_g \nu(g)^{-1} x_r \nu(r)^{-1} &= x_g x_r \nu(g)^{-r} \nu(r)^{-1} \\ &= x_g x_r \phi(g, r)^{-1} \nu(gr)^{-1} \\ &= x_g x_r (x_r^{-1} x_g^{-1} x_{gr}) \nu(gr)^{-1} \\ &= x_{gr} \nu(gr)^{-1} \end{aligned}$$

Here we've used that since $\phi(1, 1) = \nu(1)^1 \nu(1) \nu(1)^{-1} = \nu(1)$, and the fact $x_1 x_1 = x_1 x_1$, we must have $\nu(1) = x_1$. So we see that H is a subgroup. Suppose $x_g = a \nu(g)$ for $a \in A$. Then $x_g \in A$ so that $x_g = x_1$, and $x_1 \nu(1)^{-1} = 1$ as just described. Thus $H \cap A = \{1\}$. Finally note that $x_g = (x_g \nu(g)^{-1}) \nu(g) \in HA$, so that $\Gamma = HA$, and H is a complement.

- [23.13] Let α be a root of $x^n - a$, so that all the roots look like $\alpha \epsilon^i$ for $0 \leq i < n$, with ϵ a primitive n th root of unity in $\mathbb{C}$. Then we have

$$\begin{aligned} \Delta(f) &= \prod_{0 \leq i < j < n} (\alpha \epsilon^i - \alpha \epsilon^j)^2 \\ &= (-1)^{n(n-1)/2} \prod_{i \neq j} (\alpha \epsilon^i - \alpha \epsilon^j) \\ &= (-\alpha^2)^{n(n-1)/2} \prod_{i \neq j} (\epsilon^i - \epsilon^j) \\ &= (-\alpha^2)^{n(n-1)/2} \prod_{i=0}^{n-1} \left(\epsilon^i \prod_{k=1}^{n-1} (1 - \epsilon^k) \right) & (\epsilon^n = 1) \\ &= (-\alpha^2)^{n(n-1)/2} \prod_{i=0}^{n-1} \epsilon^i n & (*) \\ &= (-\epsilon)^{n(n-1)/2} a^{n-1} n^n \end{aligned}$$

In (*) we've used the value of $\prod(1 - \epsilon^k)$ as in the problem's hint. To finish the problem, we have

$$(-\epsilon)^{n(n-1)/2} = \begin{cases} -1 & n \equiv 0 \pmod{4} \\ 1 & n \equiv 1 \pmod{4} \\ 1 & n \equiv 2 \pmod{4} \\ -1 & n \equiv 3 \pmod{4} \end{cases}$$

[23.14]

- (a) Let $\{a_0, a_2, \dots, a_{n-1}\}$ be the roots (with multiplicity) of $f(x)$. Then the roots of $g(x)$ are $\{a_0, \dots, a_{n-1}, a_n\}$ with $a_n = a$. In that ordering, we have

$$\Delta(g) = \prod_{0 \leq i < j \leq n} (a_j - a_i)^2 = \prod_{k=0}^{n-1} (a - a_k)^2 \prod_{0 \leq i < j < n} (a_j - a_i)^2 = f(a)^2 \Delta(f)$$

- (b) If we let $g(x) = (x - 1)f(x)$, then $g(x) = x^n - 1$. Since $f(1) = n$, from the previous part and the previous problem we have

$$\Delta(f) = \frac{\Delta(g)}{f(1)^2} = \frac{\pm n^n}{n^2} = \pm n^{n-2}$$

where the sign choice is exactly the same as in the previous problem.

[23.15]

Since $[E : \mathbb{Q}] = p$, if $\alpha \in E$ is irrational, it must be that $E = \mathbb{Q}[\alpha]$. Let $\beta = \sqrt[p]{2}$, and let $B = \{1, \beta, \beta^2, \dots, \beta^{p-1}\}$ be a basis for E over $\mathbb{Q}$. By Theorem 23.22, $\Delta_{E/F}(B) = \Delta(g)$, where $g(x) = x^p - 2$ is the minimal polynomial of β . From [23.13], we see that $\Delta(g) = (-\epsilon)^{p(p-1)/2} p^p 2^{p-1}$.

Now if $f(x) \in \mathbb{Q}[x]$ is the minimal polynomial for $\alpha \in E$, then since $E = \mathbb{Q}[\alpha]$, Theorem 23.22 and Theorem 23.17(b) show that $\Delta(f) = r^2 \Delta(g)$ with $r \in \mathbb{Q}$. In particular,

$$(-1)^{(p-1)/2} p \Delta(f) = (-1)^{(p^2-1)/2} \epsilon^{p(p-1)/2} r^2 p^{p+1} 2^{p-1} = \left(r p^{(p+1)/2} 2^{(p-1)/2} \right)^2$$

And so the expression in the problem is a perfect square.

[23.16]

Since E/F is finite-degree and separable, there are only finitely many intermediate fields between F and E , and by the primitive element theorem, there is a finite set $\{\alpha_1, \dots, \alpha_m\} \subset E$ such that every subfield of E containing F is $F[\alpha_i]$ for some $1 \leq i \leq m$. Let $s_i = \Delta(f_i)$, where $f_i(x) \in F[x]$ is a minimal polynomial for α_i . Now if $\alpha \in E$ is arbitrary, it must be that $F[\alpha] = F[\alpha_i]$ for some i . Let $f(x) \in F[x]$ be the minimal polynomial of α . Then Theorem 23.22 and Theorem 23.17(b) show that $\Delta(f) = \beta^2 \Delta(f_i)$ for some $\beta \in F$. This means that $s_i \Delta(f)$ is a square in F , so the finite set $S = \{s_1, \dots, s_m\}$ works.

[23.17]

- (a) Suppose $\sum r_i \alpha_i = 0$, with each $r_i \in F$ and not all of them zero. Then $\sum r_i \sigma_j(\alpha_i) = 0$ for all j , and this shows the vector $[r_1, \dots, r_n]$ is in the kernel of B , so $\det(B) = 0$.
- (b) Note that the (i, j) entry of $B^T B$ is given by

$$(B^T B)_{i,j} = \sum_{k=1}^n \sigma_k(\alpha_i) \sigma_k(\alpha_j) = \sum_{k=1}^n \sigma_k(\alpha_i \alpha_j) = T_{E/F}(\alpha_i \alpha_j)$$

Thus by definition $\Delta_{E/F}(B) = \det(B^T B) = \det(B)^2$.

Chapter 24

[24.1]

- (a) Note that the list $(\frac{\alpha}{\beta}, \frac{\beta}{\gamma}, \frac{\gamma}{\alpha})$ satisfies the polynomial $xyz - 1$, and thus the list is algebraically dependent over F .
- (b) By symmetry, it is enough to show that $(\frac{\alpha}{\beta}, \frac{\beta}{\gamma})$ is algebraically independent. If they weren't, there would be a nonzero polynomial $f(x, y) \in F[x, y]$ with the pair as zeroes; let the degree of $f(x, y)$ in x be m , and the degree in y be n . Then

$$y^m z^n f\left(\frac{x}{y}, \frac{y}{z}\right) \in F[x, y, z]$$

and it has (α, β, γ) as roots, contradicting that list's algebraic independence. Thus $(\frac{\alpha}{\beta}, \frac{\beta}{\gamma})$ is algebraically independent.

[24.2]

We have that α is a root of the polynomial $(\beta\gamma)x^2 - (\alpha\beta)(\gamma\alpha)$, and similarly for the other two; this means all three are algebraic over $K := F(\alpha\beta, \beta\gamma, \gamma\alpha)$. In particular, this implies the transcendence degree of $F(\alpha, \beta, \gamma)$ over K is 0. Since the transcendence degree of $F(\alpha, \beta, \gamma)$ over F is 3, Theorem 24.8 implies that K has transcendence degree 3 over F , meaning $(\alpha\beta, \beta\gamma, \gamma\alpha)$ are algebraically independent by Lemma 24.4.

[24.3]

$\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\gamma}$ are algebraic over $F(\alpha, \beta, \gamma)$, meaning that if $L = F(\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\gamma})$, then L has transcendence degree 3 over F . Let $K = F(\alpha\sqrt{\beta}, \beta\sqrt{\gamma}, \gamma\sqrt{\alpha})$. Note that $\sqrt{\alpha}$ is a root of the polynomial

$$t^9 - \frac{\gamma\sqrt{\alpha}(\alpha\sqrt{\beta})^4}{(\beta\sqrt{\gamma})^2} \in K[t]$$

Similar polynomials work for the other two roots, so that L is algebraic over K . Just as in the previous problem, Theorem 24.8 then implies K has transcendence degree 3 over F , and Lemma 24.4 implies $(\alpha\sqrt{\beta}, \beta\sqrt{\gamma}, \gamma\sqrt{\alpha})$ is a transcendence basis, hence algebraically independent over F .

[24.4]

Suppose $K \leq S \leq E$, where S/K is separable, and E/S is purely inseparable. We know that $T_{E/K} \equiv 0$ if $S \neq E$, and from [23.5] that $N_{E/K}(\alpha) = N_{S/K}(\alpha^{[E:S]})$. It is thus enough

to prove the case where $E = S$ is a separable extension of K . In that case, Corollary 23.10 shows that $T_{E/K}(\alpha)$ is a sum of Galois conjugates of α , and $N_{E/K}(\alpha)$ is a product of Galois conjugates. Since $F \leq K$, all these Galois conjugates are algebraic over F , hence so are their sums and products.

[24.5] If E is not totally transcendental over F , then there is an element $\beta \in E \setminus F$ algebraic over F . Of course, $\beta \notin K$ as K is purely (hence totally) transcendental. Since $[E : K] = p$ is prime, this implies $E = K[\beta]$. Let $B = \{1, \beta, \dots, \beta^{p-1}\}$. If $f(x) \in K[x]$ is the minimal polynomial of β over K , and $g(x) \in F[x]$ is the minimal polynomial of β over F , then $f(x)$ divides $g(x)$, so all roots of $f(x)$ are algebraic over F . Then the coefficients of $f(x)$, as symmetric polynomials of the roots of $f(x)$, are algebraic over F , and hence $f(x) = g(x) \in F[x]$. This implies that if $\Delta_{E/K}(B) = a$, then $a \in F$ since Theorem 23.22 shows

$$\Delta_{E/K}(B) = \Delta(f) = \Delta(g) \in F$$

If $C = \{1, \alpha, \dots, \alpha^{p-1}\}$, then Theorems 23.17 and 23.22 imply

$$\Delta = \Delta_{E/K}(C) = ab^2$$

where $b \in K$. This is exactly the contrapositive of the problem statement.

[24.6] Let $\mathcal{Y}$ be the set of subsets of $\mathcal{X}$ which are algebraically independent over F , partially ordered by inclusion; note that $\mathcal{Y}$ is non-empty, since it contains $\emptyset \subset \mathcal{X}$. If $\{U_i\}_I$ is a linearly ordered collection in $\mathcal{Y}$, then $U = \cup U_i$ is also in $\mathcal{Y}$. To see this, note that if U is algebraically dependent over F , then there is a finite subset $U_0 \subset U$ that is algebraically dependent. But then $U_0 \subset U_i$ for some $i \in I$, contradicting that U_i is algebraically independent over F . Thus U is algebraically independent, so $\mathcal{Y}$ satisfies the conditions of Zorn's lemma: picking a maximal $\mathcal{X}_0 \in \mathcal{Y}$ is enough.

[24.7] We know α is algebraic over $F(\mathcal{X})$, and so it is the zero of some polynomial

$$f(t) = \sum_{i=0}^n \alpha_i t^i$$

with each $\alpha_i \in F(\mathcal{X})$. But each α_i is a quotient of polynomials in a finite subset $\mathcal{X}_i \subset \mathcal{X}$. Thus $f(t)$ is defined over $F(\mathcal{Y})$, where $\mathcal{Y} = \cup \mathcal{X}_i$ is finite; α is then algebraic over $F(\mathcal{Y})$, as a root of $f(t)$.

[24.8] What is needed is to show that $\mathcal{X}$ is algebraically independent over F . Let $\mathcal{Y} \subset \mathcal{X}$ be a maximal subset that is algebraically independent over F (this exists because $\mathcal{X}$ is finite). If $\alpha \in \mathcal{X} \setminus \mathcal{Y}$, then Lemma 24.2 shows α is algebraic over $F(\mathcal{Y})$. This means $F(\mathcal{X})$ is algebraic over $F(\mathcal{Y})$. Since E is algebraic over $F(\mathcal{X})$, this implies E is algebraic over $F(\mathcal{Y})$; minimality then implies $\mathcal{X} = \mathcal{Y}$, so $\mathcal{X}$ is algebraically independent over F , as desired.

[24.9] Let $\sigma \in \text{Gal}(E/K)$ be an arbitrary automorphism. If $\alpha \in A$, then α satisfies some polynomial $f(t) \in F[x]$. Since $F \leq K$, σ fixes $f(t)$, and thus α^σ is also a root of $f(t)$, hence

$\alpha^\sigma \in A$ as well. This shows that σ fixes A , and we have a homomorphism from $\text{Gal}(E/K)$ to $\text{Aut}(A)$; let G denote this finite group of automorphisms of A . If $\alpha \in A$ is fixed by all of G , then α is fixed by $\text{Gal}(E/K)$, so $\alpha \in K$. But K is totally transcendental over F , and α is algebraic over F , so $\alpha \in F$. Of course F is fixed by G since $F \leq K$, and so we see that F is the fixed subfield of G acting on A . By Theorem 18.20, A is Galois over F with Galois group G .

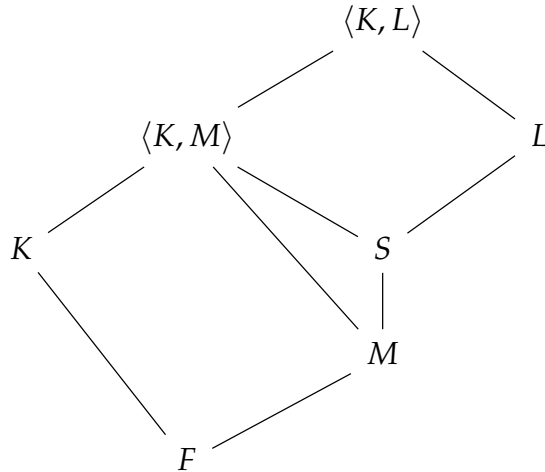
[24.10] Suppose $F(\alpha) \cap F(\beta) = K > F$. By Lüroth's theorem, we can write $K = F(\gamma) \subset F(\alpha)$, or $K = F(\delta) \subset F(\beta)$. By Corollary 17.8, we know that both $[F(\alpha) : K]$ and $[F(\beta) : K]$ are finite. This means α and β are algebraic over K , so that $F(\alpha, \beta)/K$ is an algebraic extension. But then (with $L = F(\alpha, \beta)$)

$$td_{L/F} = td_{L/K} + td_{K/F} = 0 + 1$$

This contradicts (α, β) being algebraically independent over F , so that $td_{L/K} = 2$. Thus it must be that $K = F$.

[24.11] Let $E = \mathbb{Q}(T)$, $K = \mathbb{Q}(T^2)$, and $L = \mathbb{Q}(T - T^2)$. Then E is a quadratic extension of both K and L , and is thus Galois over them. Let $\sigma \in \text{Gal}(E/K)$ be the non-trivial element, so $\sigma(T) = -T$. Let $\tau \in \text{Gal}(E/L)$ be the non-trivial element, so $\tau(T) = 1 - T$. If $K \cap L = M > \mathbb{Q}$, then as in the previous problem, by Lüroth's theorem and Corollary 17.8 $[K : M]$ and $[L : M]$ are finite, so $[E : M]$ is finite. This implies that $\text{Gal}(E/M)$ is finite, by Lemma 18.16. However both σ and τ fix M , so that $\tau\sigma \in \text{Gal}(E/M)$, and $\tau\sigma(T) = 1 + T$ has infinite order. This contradiction shows we must have $M = \mathbb{Q}$.

[24.12] Let M be a field with $F \leq M \leq L$. We show that $[M : F] \leq [\langle K, M \rangle : K]$, so that by Lemma 24.14, K and L are linearly disjoint. We have the following diagram of fields:



Now L/S is Galois, so $[L : S] = [\langle K, L \rangle : \langle K, M \rangle]$; since L/F is also Galois, we also have that $[L : F] = [\langle K, L \rangle : K]$ (all of this is by natural irrationalities). Thus we have

$$[M : F] = \frac{[L : F]}{[L : S][S : M]} = \frac{[\langle K, L \rangle : K]}{[\langle K, L \rangle : \langle K, M \rangle][S : M]} = \frac{[\langle K, M \rangle : K]}{[S : M]} \leq [\langle K, M \rangle : K]$$

[24.13] First note $K \cap L = F$ since K is totally transcendental and L is algebraic over F . Let A be a subfield $F \leq A \leq L$, with $[A : F]$ finite. Then there is a Galois extension $A \leq S$; by the previous problem S and K are linearly disjoint (hence so are A and K). Since this holds for any such $A \leq L$ with $[A : F]$ finite, Lemma 24.14 shows L and K are linearly disjoint.

[24.14] Since T is a zero of the polynomial $p(x) - \frac{p}{q}q(x)$, it is enough to show this polynomial is irreducible of degree d when $d > 0$. But this is just Corollary 24.19.

[24.15]

(a) Let $\sigma(T) = p(T)/q(T)$. Since σ is surjective, by the previous problem both $p(T)$ and $q(T)$ have degree at most 1, which shows

$$\sigma(T) = f(T) = \frac{aT + b}{cT + d}$$

If $ad = bc$, then either $c = 0$ (so $\sigma(T) = \frac{b}{d}$), or $c \neq 0$ (so $\sigma(T) = \frac{a}{c}$); in both cases σ is not surjective since its image lands in F .

(b) If $ad \neq bc$, then $f(T)$ shown above is not a constant, since in this case $a(aT + b) + \beta(cT + d) = 0$ has no non-zero solutions when $ad - bc \neq 0$. Both T and $f(T)$ are transcendental over F , so both $F(T)$ and $F(f(T))$ are F -isomorphic to $F(x)$, and are thus F -isomorphic to each other. The isomorphism $\sigma : F(T) \rightarrow F(f(T))$ is surjective by the previous problem. Thus $\sigma \in \text{Gal}(E/F)$. It is unique because any element $\tau \in \text{Gal}(E/F)$ fixes F , and is hence completely determined by $\tau(T)$.

[24.16] For given matrices $A, B \in GL(2, F)$, write σ_A for the corresponding automorphism of E , which is an automorphism by the previous problem and the fact $\det(A) = ad - bc \neq 0$. If we let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \quad AB = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$

we can compute that

$$((T)\sigma_A)\sigma_B = \frac{a\sigma_B(T) + b}{c\sigma_B(T) + d} = \frac{a(eT + f) + b(gT + h)}{c(eT + f) + d(gT + h)} = \frac{(ae + bg)T + (af + bh)}{(ce + dg)T + (cf + dh)} = (T)\sigma_{AB}$$

So we have a homomorphism. By the previous problem this is surjective. The kernel is those A such that $\sigma_A(T) = T$. We can solve to get

$$\begin{aligned} aT + b &= T(cT + d) \\ cT^2 + (d - a)T - b &= 0 \end{aligned}$$

Since this should be the zero polynomial, we see $c = b = 0$ and $a = d$. Then the kernel is the set of scalar matrices, so $PGL(2, F) \cong \text{Gal}(E/F)$.

[24.17] Let $E = \mathbb{Q}(T)$, and let $F \leq E$ be the fixed subfield of $G \leq PGL(2, \mathbb{Q})$. By the previous problem, $PGL(2, \mathbb{Q}) \cong \text{Gal}(E/\mathbb{Q}) \cong \text{Aut}(E)$, so that by Theorem 18.20 E/F is Galois with Galois group G . By Lüroth's theorem F is purely transcendental of degree 1 over $\mathbb{Q}$, and so Theorem 24.23 shows G is a Galois group of some extension $\mathbb{Q} \leq L$.

Chapter 25

[25.1] Let L/F be an algebraic closure of F . If F has positive characteristic and is not perfect, then by Lemma 25.3 F has irreducible polynomials of unbounded degree. So by Corollary 19.8 we know that L/F is separable. Let n be the maximum degree of an irreducible polynomial in $F[x]$. If $\alpha \in L$ is a root of this polynomial, then $[F[\alpha] : F] = n$. If $F[\alpha] \neq L$, then there is a $\beta \in L \setminus F[\alpha]$, and then $F[\alpha, \beta] > F[\alpha]$. By the primitive element theorem, we can write $F[\alpha, \beta] = F[\gamma]$, and then if $g(x) \in F[x]$ is the minimal polynomial of γ , we have

$$\deg(g(x)) = [F[\gamma] : F] > [F[\alpha] : F] = n$$

This contradicts the maximality of n , so that $F[\alpha] = L$ is a finite-degree extension, as desired.

[25.2] Let $E_0 = F$ and let $\alpha_0 \in E_0$ be an element that is not a p th power. Then $x^p - \alpha_0$ has no root in E_0 , so we can let β_0 be a root and write $E_1 = E_0[\beta_0]$. Since $\beta_0^p \in E_0$, Kummer's theorem shows that E_1/E_0 is a Galois extension of degree p . Thus we have realized an extension of degree p^1 over F .

We now work inductively, assuming we've constructed E_n/F of degree p^n , such that E_n/E_{n-1} is Galois of degree p . By Theorem 25.6, there is an element $\alpha_n \in E_n$ such that $x^p - \alpha_n$ is irreducible over E_n . If β_n is a root of this polynomial, then we can define $E_{n+1} = E_n[\beta_n]$; by Kummer's theorem again, E_{n+1}/E_n is Galois of degree p , and so we see that $[E_{n+1} : F] = p^{n+1}$. Inductively then we've constructed extensions of degree p^e for all integers $e \geq 1$.

[25.3]

(a) If $a^2 + b^2 = u$, then

$$\left(\frac{a}{u}\right)^2 + \left(\frac{b}{u}\right)^2 = \frac{a^2 + b^2}{u^2} = \frac{u}{u^2} = \frac{1}{u}$$

(b) Suppose $\alpha_1^2 + \cdots + \alpha_k^2 = -1$, with $k > 2$ odd. If we assume k is the minimal such integer where an equation like this is possible, then it must be that $\alpha_1^2 + \alpha_2^2 \neq 0$. We can then write

$$\begin{aligned} \alpha_1^2 + \cdots + \alpha_k^2 + 1^2 &= 0 \\ 1 + \frac{\alpha_3^2 + \alpha_4^2}{\alpha_1^2 + \alpha_2^2} + \cdots + \frac{\alpha_k^2 + 1^2}{\alpha_1^2 + \alpha_2^2} &= 0 \end{aligned}$$

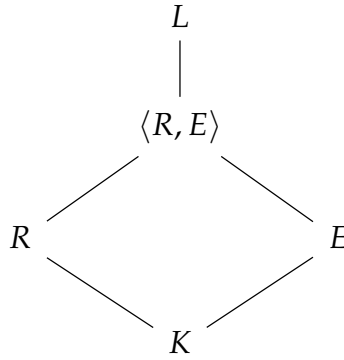
Each of these fractional terms is in $S_2(F)$ by part (a) and the problem text. Writing the i th fraction as $\beta_i^2 + \gamma_i^2$, we see then that we have (with $k = 2n + 1$)

$$1 + \beta_1^2 + \gamma_1^2 + \cdots + \beta_n^2 + \gamma_n^2 = 0$$

And thus -1 is expressed as a sum of $2n < k$ squares, contradicting the minimality of k . So either $k \leq 2$ or k is even.

[25.4] Let F be formally real, and L an algebraic closure of F ; also let $\mathcal{Z}$ be the poset of all formally real subfields $F \leq K \leq L$, ordered by containment. $F \in \mathcal{Z}$, so it is non-empty. Also if $\{K_i\}_I$ is a linearly ordered chain in $\mathcal{Z}$, then let $K = \cup K_i$; this is a field, and it is formally real. To see this, note that if $-1 = \alpha_1^2 + \cdots + \alpha_m^2$ in K , then all of the α_j would belong to some K_i , and then K_i would not be formally real. So K is an upper bound of the chain in $\mathcal{Z}$, so the hypotheses of Zorn's lemma are satisfied, and $\mathcal{Z}$ contains a maximal element.

[25.5] Let L be an algebraic closure of E , so that L is also an algebraic closure of $K \leq E$. As in the proof of Corollary 25.10, let R be a maximal formally real subfield of L containing K , so that R is realclosed. We then have the following diagram



We know that $K \subset R \cap E$, and because K is maximal among formally real subfields of E containing F , this must be an equality. Now $[L : R] \leq 2$ by Theorem 25.11 and the Artin-Schreier theorem, but E/K is Galois so we have by natural irrationalities

$$[E : K] = [\langle R, E \rangle : R] \leq [L : R] \leq 2$$

[25.6] As computed in Chapter 18, $\text{Gal}(E/\mathbb{Q}) \cong D_8$. In fact, we can write $\text{Gal}(E/\mathbb{Q}) = \langle \sigma, \tau \rangle$, where τ is complex conjugation and $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ has order 4. Noting that both τ and σ^2 fix $F = \mathbb{Q}[\sqrt{2}]$, and the fact $[E : F] = 4 = |\langle \sigma^2, \tau \rangle|$, it must be that $\text{Gal}(E/F)$ is in fact $H := \langle \sigma^2, \tau \rangle$. Since H is elementary Abelian, there are exactly 3 proper nontrivial subgroups, and hence 3 proper intermediate fields between F and E : $\mathbb{Q}[\sqrt[4]{2}]$, $\mathbb{Q}[i, \sqrt{2}]$, and $\mathbb{Q}[i\sqrt[4]{2}]$. Of course $\mathbb{Q}[\sqrt[4]{2}] \subset \mathbb{R}$ is formally real, and hence a maximally formally real field. But so is $\mathbb{Q}[i\sqrt[4]{2}]$, since it is isomorphic to $\mathbb{Q}[\sqrt[4]{2}]$ by Lemma 17.15, as both generators are roots of the irreducible $x^4 - 2$. Thus $\mathbb{Q}[i\sqrt[4]{2}]$ is also a maximal formally real subfield between F and E . However, H fixes the field $\mathbb{Q}[\sqrt[4]{2}]$ setwise, and so $H = \text{Gal}(E/F)$ is not transitive on the maximal formally real intermediate fields of E/F .

[25.7] Let $F_0 = \mathbb{Q}$, and assuming F_i is already constructed, let $F_{i+1} \subset \mathbb{R}$ be $F_i[U_i]$, where U_i is the set of square roots of all positive elements of F_i ; that is,

$$U_i = \{\sqrt{\alpha} \mid \alpha \in F_i \cap \mathbb{R}^+\}$$

Since $F_0 \subset F_1 \subset \dots$, the infinite union $F = \cup F_i$ is a field. Let $S \subset F$ be the set of nonzero squares in F . If $\alpha^2, \beta^2 \in S$, then there is some $i \geq 0$ with $\alpha^2, \beta^2 \in F_i$. But then $\sqrt{\alpha^2 + \beta^2} \in F_{i+1}$, so $\alpha^2 + \beta^2 \in S$, and S is closed under addition.

We now show $\beta := \sqrt[3]{2} \notin F$, since this implies $x^3 - 2$ is irreducible over F , because otherwise some root would belong to F , but this polynomial has only one real root. This is enough to conclude F is not real-closed, since $[F[\beta] : F] = 3$, and by Theorem 25.17 $F[\beta]$ is formally real. Suppose for contradiction that $\beta \in F$, so that $\beta \in F_i$ for some $i \geq 0$. Then we can write

$$\beta = p(\alpha_1, \dots, \alpha_m)$$

where $p(x_1, \dots, x_m) \in F_{i-1}[x_1, \dots, x_m]$ and $\{\alpha_1, \dots, \alpha_m\} \subset U_{i-1}$. But $[F_{i-1}(\alpha_1, \dots, \alpha_m) : F_{i-1}]$ is a power of 2, since we're adjoining square roots, while $[F_{i-1}(\beta) : F_{i-1}]$ divides 3. Because we're assuming $F_{i-1}(\beta) \subset F_{i-1}(\alpha_1, \dots, \alpha_m)$, this implies $[F_{i-1}(\beta) : F_{i-1}] = 1$ and $\beta \in F_{i-1}$. Continuing this way, we eventually get $\beta \in F_0 = \mathbb{Q}$, which is absurd. So $\beta \notin F$ and F is not real-closed.

[25.8] Suppose $F(x)$ is not formally real, so that we can find $p_i(x), q_i(x) \in F[x]$ such that

$$-1 = \left(\frac{p_1(x)}{q_1(x)} \right)^2 + \dots + \left(\frac{p_m(x)}{q_m(x)} \right)^2$$

Clearing denominators, this is equivalent to $\sum f_i(x)^2 + q(x)^2 = 0$, where $q(x) = \prod q_i(x)$ and $f_i(x) = p_i(x)q(x)/q_i(x)$. If α_i is the constant term of $f_i(x)$, and β is the constant term of $q(x)$, then this means

$$\sum_{i=1}^m \alpha_i^2 + \beta^2 = 0$$

Since this sum is happening in F , and F is formally real, we see that all the α_i and β are 0. Thus we can divide $\sum f_i(x)^2 + q(x)^2 = 0$ by x and then again compare constant coefficients; continuing this way, we see that all the $f_i(x)$ and $q(x)$ are identically zero polynomials, contradicting the original expression for -1 (since the $q_i(x)$ need to be non-zero). This contradiction then shows $F(x)$ is in fact formally real.

[25.9]

- (a) Let $F_n = \mathbb{Q}(x, \alpha_1, \dots, \alpha_n)$, and let $r \in \mathbb{R}$ be a transcendental number larger than n . Because r is transcendental over $\mathbb{Q}$, there is an isomorphism $\theta : \mathbb{Q}(x) \rightarrow \mathbb{Q}(r)$. If we let $\beta_i = \sqrt{r - i}$, then F_n is a splitting field for

$$p_x(t) = \prod_{i=1}^n (t^2 - x - i)$$

and similarly $K_n := \mathbb{Q}(r, \beta_1, \dots, \beta_n)$ is the splitting field for $p_r(t)$ (using the obvious notation). By Theorem 17.22, θ extends to an isomorphism from F_n to K_n . Since $K_n \subset \mathbb{R}$, we see F_n is formally real.

- (b) If $K = \cup F_n$ was not formally real, then we could find $\gamma_i \in K$ for $1 \leq i \leq m$ with $\sum \gamma_i^2 = -1$. Since there must be some n with all the $\gamma_i \in F_n$, this would imply F_n is not formally real, which contradicts part (a). So K must be formally real as well.
- (c) Suppose K had an Archimedean order, so that there existed an $m \in \mathbb{Z}$ with $x \leq m$. But $\alpha_m \in K$ with $\alpha_m^2 = x - m$; by Lemma 25.20(g), we see $x - m > 0$, so that $x > m$. This contradiction shows no such $m \in \mathbb{Z}$ exists, and thus K must be non-Archimedean.

[25.10]

- (a) Suppose K is real-closed, and let $P \subset K$ be a positive set for an order. By Lemma 25.20(g), its non-zero squares $S \subset P$, and of course then $-S \cap P = \emptyset$ by Lemma 25.20(c). Since

$$P \sqcup \{0\} \sqcup -P = K = S \sqcup \{0\} \sqcup -S$$

it must be that $P = S$. So the positive set for K is uniquely determined. Since a field isomorphism $\theta : K \rightarrow L$ will preserve non-zero squares, we see that L is real-closed with (unique) positive set $\theta(S)$. Thus $\alpha < \beta$ in K if and only if $\theta(\alpha) < \theta(\beta)$ in L .

- (b) Let $F = \mathbb{Q}(x)$, which is formally real by [25.8]. If $r \in \mathbb{R}$ is a transcendental number, then $F \cong \mathbb{Q}(r)$. Choose $0 < r < 1$ and choose another transcendental $s \in \mathbb{R}$ with $1 < s < 2$. Then F inherits orders from both $\mathbb{Q}(r)$ and $\mathbb{Q}(s)$ (as subfields of $\mathbb{R}$). Let F_r and F_s be F with these orders. Then the identity map $\iota : F_r \rightarrow F_s$ is an isomorphism, but in F_r we have $x < 1$ while in F_s it happens that $x > 1$. Thus ι is not order-preserving.

[25.11]

- (a) Suppose $\theta : \mathbb{R} \rightarrow \mathbb{R}$ is an injective homomorphism, and $\theta(\alpha) = \beta \neq \alpha$. Assume without loss of generality that $\alpha < \beta$ (replace α with $-\alpha$ otherwise). If $r \in \mathbb{Q}$ is a rational number with $\alpha < r < \beta$, then $\theta(r) = r$. But then $\alpha < r$ while $\theta(\alpha) > \theta(r)$, contradicting part (a) of the previous problem. Thus θ must be the identity map.
- (b) If $K \geq \mathbb{R}$ has an Archimedean order, then by Theorem 25.26 there is an isomorphism θ from K into $\mathbb{R}$. By the previous part $\theta|_{\mathbb{R}}$ is the identity map, so that θ can only be injective if $K = \mathbb{R}$. Thus for $K > \mathbb{R}$, K must not have an Archimedean order.
- (c) Let E be an algebraic closure of $\mathbb{R}(x)$. Note that $\mathbb{R}(x)$ is formally real by [25.8], so there is a maximal formally real subfield $\mathbb{R}(x) \leq K < E$, which is real-closed by Corollary 25.10. Then $[E : K] = 2$ by the Artin-Schreier theorem and Theorem 25.11. Since E/K is Galois (being separable and normal), there is a non-trivial involution $\sigma \in \text{Gal}(E/K)$, which fixes K (and hence $\mathbb{R}(x) \subset K$). Since $K > \mathbb{R}$, the previous part shows K has no Archimedean order.

[25.12]

Let $R = \{\alpha \in F \mid -n < \alpha < n \text{ for some } n \in \mathbb{Z}\}$. We show R is a subring of F by showing it's closed under addition and multiplication. If $\alpha, \beta \in R$, then let $-m < \alpha < m$ and $-n < \beta < n$. We see that

$$-m - n < \alpha + \beta < m + n$$

so $\alpha + \beta \in R$. Of course $-\alpha \in R$ as well. Now if $\beta > 0$, we have

$$-mn < -m\beta < \alpha\beta < m\beta < mn$$

meaning $\alpha\beta \in R$. If $\beta < 0$, the above shows $-\alpha\beta \in R$, so $\alpha\beta \in R$ in this case too.

Finally we show V is an ideal. We already know it is an additive subgroup by Lemma 25.24. If $v \in V$ then for any $k \in \mathbb{Z}^+$, we have $v < \frac{1}{km}$. This means $\alpha v < mv < \frac{1}{k}$. Since k was arbitrary, we see $\alpha v \in V$.

[25.13] Let $K \subset E$ be a maximal formally real subfield of E . Since $K \neq E$, [25.5] shows $[E : K] = 2$. By the fundamental theorem of Galois theory, there is a subgroup $H \leq \text{Gal}(E/\mathbb{Q})$ of order 2 such that K is the fixed field of H . Let $H = \langle \sigma \rangle$, where σ is an involution. If $g \in \text{Gal}(E/\mathbb{Q})$, then σ^g is an involution and K^g is the fixed field of σ^g . Note that K^g is formally real and $[E : K^g] = 2$, so K^g is also a maximal formally real subfield of E . Meanwhile, if $L \leq E$ is any other maximal formally real subfield of E , Corollary 25.28 shows there's a $g \in \text{Gal}(E/\mathbb{Q})$ with $L = K^g$. All of this shows the maximal formally real subfields of E are exactly those fixed fields of σ^g as g ranges over $\text{Gal}(E/\mathbb{Q})$.

Now if $F \leq E$ is formally real, it is contained in some maximal formally real subfield K^g , and hence $F \subset \text{Fix}(\sigma^g) = K^g$. Conversely, if $F \subset \text{Fix}(\sigma^g)$, then $F \subset K^g$ and so F is formally real.

Chapter 26

[26.1] Let $e \in R$ be a non-trivial idempotent. Then $1 - e$ is also a non-trivial idempotent, since

$$(1 - e)^2 = 1 - e - e + e = 1 - e$$

Now if $P \leq R$ is a prime ideal, then from $e(1 - e) = 0 \in P$ we see that either $e \in P$ or $1 - e \in P$, so P does contain a non-trivial idempotent.

[26.2] Let $n = \prod p_i^{\alpha_i}$ and let $m = \prod p_i$, where $\{p_1, \dots, p_r\}$ are the primes dividing n . If $a^k \in (n)$, we see that p_i divides a for each $1 \leq i \leq r$, and thus m divides a so $a \in (m)$. This shows $\sqrt{(n)} \leq (m)$. Meanwhile if $\alpha = \max(\alpha_1, \dots, \alpha_r)$ then $m^\alpha \in (n)$, so $m \in \sqrt{(n)}$ and thus we get the reverse containment $(m) \leq \sqrt{(n)}$, implying equality: $(m) = \sqrt{(n)}$.

[26.3] Suppose $x \in R$ is such that $x \in \sqrt{AB}$, so that $x^m \in AB$ for some $m > 0$. Since $AB \subset A \cap B$, we see $x^m \in A \cap B$ so $x \in \sqrt{A \cap B}$. If $x^m \in A \cap B$, then $x^m \in A$ and $x^m \in B$, so $x \in \sqrt{A} \cap \sqrt{B}$. Finally, if $x \in \sqrt{A} \cap \sqrt{B}$, then $x^m \in A$ and $x^n \in B$ for some $m, n > 0$. Then $x^{m+n} \in AB$ so $x \in \sqrt{AB}$. Since x was arbitrary, this shows

$$\sqrt{AB} = \sqrt{A \cap B} = \sqrt{A} \cap \sqrt{B}$$

[26.4]

- (a) For an ideal $A \leq R$, let $X_A = \{P \in \text{Spec}(R) \mid A \subseteq P\}$. Then $X_A \cup X_B = X_{AB}$. To see this, note that if $AB \subset P$, then by primeness either $A \subset P$ or $B \subset P$. Meanwhile, if $A \subset P$ (or $B \subset P$), then of course $AB \subset A \cap B \subset P$.
- (b) For a collection $\{A_i\}_I$ of ideals, let $B = \langle A_i \rangle_I$. We claim $\cap X_{A_i} = X_B$. To see this, note that if $A_i \subset P$ for all $i \in I$, then of course $B \subset P$. Meanwhile, if $B \subset P$, then $A_i \subset B \subset P$ for all $i \in I$.
- (c) Suppose $\{A_i\}_I$ is such that for every finite subset $F \subset I$, there exists a prime ideal P_F such that

$$P_F \in \bigcap_{i \in F} X_{A_i}$$

From part (b), this shows that over F , $\sum A_i = \langle A_i \rangle \neq R$. In particular, $1 \notin \sum A_i$. This shows that $B = \langle A_i \rangle_I$ is proper, since otherwise 1 would be a finite sum of elements in the $\{A_i\}_I$. Since B is a proper ideal, Lemma 26.2 shows there is a prime ideal $P \supset B$, and thus $\cap X_{A_i}$ is non-empty.

[26.5]

- (a) Define the homomorphism $R \rightarrow \mathbb{R}$ sending $f \in R$ to $f(a)$ for $a \in \mathbb{R}$. This is surjective (because of constant functions), and the kernel is M_a . Because $\mathbb{R}$ is a field, M_a is maximal: there are no ideals between (0) and R/M_a .
- (b) Define $f(x) = (1 - \log(x))^{-1}$. By continuity it must be that $f(0) = 0$; meanwhile, $f(x) \neq 0$ for $x > 0$. We see that

$$\begin{aligned} \lim_{x \rightarrow 0} \frac{f^n(x)}{x} &= \lim_{x \rightarrow 0} \frac{1}{x(1 - \log(x))^n} \\ &= \lim_{x \rightarrow 0} \frac{x^{-1}}{(1 - \log(x))^n} \\ &= \lim_{x \rightarrow 0} \frac{-x^{-2}}{-nx^{-1}(1 - \log(x))^{n-1}} \quad (\text{L'Hospital rule}) \\ &= \frac{1}{n} \lim_{x \rightarrow 0} \frac{x^{-1}}{(1 - \log(x))^{n-1}} \end{aligned}$$

By induction on n we see this limit is ∞ , and thus $\frac{f^n}{x}$ is not a continuous function, so $f^n \notin (x)$. We know from Lemma 26.2 that the principal ideal (x) is contained in a prime ideal P which is disjoint from the multiplicative set $\{1, f, f^2, \dots\}$. If P was maximal, then by the next part we would have $P = M_0$. But $f \in M_0$, and this contradiction shows P is a prime non-maximal ideal of R .

- (c) Suppose $M \leq R$ is a maximal ideal not equal to M_a for any $a \in [0, 1]$. Then for any $a \in [0, 1]$, there is an $f_a \in M$ with $f_a(a) \neq 0$. Since f_a is continuous, there is an open neighborhood U_a for which $0 \notin f_a(U_a)$. Because $[0, 1]$ is compact, there are finitely many $\{a_1, \dots, a_n\}$ where $\cup U_i = [0, 1]$. Then $\sum f_i^2$ is an element of M that is non-zero everywhere, hence invertible. This contradiction shows no such M exists.

[26.6]

- (a) If e_x and e_y (for $x \neq y$) are both not in the ideal P , then since $e_x e_y \equiv 0 \in P$, it must be that P is not prime. So for prime ideals, at most one of the e_x is not in P .
- (b) Suppose first that f vanishes at finitely many points $\{x_1, \dots, x_n\}$. Let P_i be a prime ideal containing all elements that have a zero at x_i ; this is prime since if $g(x_i)h(x_i) = 0$, then either $g(x_i) = 0$ or $h(x_i) = 0$. If $g^m \in (f)$ then $g(x_i) = 0$ for all $1 \leq i \leq n$, and thus $g \in \cap P_i$. Conversely if $g \in \cap P_i$, then $g(x_i) = 0$ and we see that $g \in (f)$ because $g(x) = r(x)f(x)$ with

$$r(x) = \begin{cases} 0 & f(x) = 0 \\ \frac{g(x)}{f(x)} & f(x) \neq 0 \end{cases}$$

We have thus shown in this case that $\sqrt{(f)} = \cap P_i$. Conversely if $\sqrt{(f)} = \cap P_i$ for finitely many prime ideals P_i with $1 \leq i \leq n$, then from part (a) there is a finite set $Y \subset X$ where $e_x \in \cap P_i$ if $x \notin Y$. But then $e_x^m \in (f)$ implies that we cannot have $f(x) = 0$, and thus the zeroes of f are contained in the finite set Y .

[26.7]

Let $P_1, \dots, P_n$ be the minimal primes of R , so that $\cap P_i = \sqrt{(0)}$ is the nilradical. If $r \in R$ is such that there exists a non-nilpotent $s \in R$ with rs nilpotent, then $rs \in \cap P_i$. Since each P_i is prime, either $r \in P_i$ or $s \in P_i$. If $r \notin P_i$ for all $1 \leq i \leq n$, then $s \in \cap P_i$ implies s is nilpotent, a contradiction. Thus there's some i with $r \in P_i$.

Conversely, suppose $r \in P_i$ for some $1 \leq i \leq n$. Let J be the set of integers i where $r \in P_i$. Then J is non-empty. If $J = \{1, \dots, n\}$, then we can take $s = 1$ so that $r = rs$ is nilpotent. Otherwise, choose

$$s \in \bigcap_{i \notin J} P_i \setminus \sqrt{(0)}$$

Note this set difference is non-empty by Corollary 26.9. Then s is non-nilpotent, but $rs \in P_i$ for all $1 \leq i \leq n$, so it is nilpotent.

[26.8]

Suppose $M_1, \dots, M_n$ are the maximal ideals of R . If $x \in R$ is a non-unit, then it belongs to some maximal ideal by Lemma 26.2. Conversely, if $z \in R$ is not in any maximal ideal, then again by Lemma 26.2 the principal ideal (z) must meet the multiplicative subset $\{1\}$ non-trivially, so that z is a unit. Thus $\cup M_i$ is the set of all non-units in R .

Now suppose there are ideals $A_1, \dots, A_n$ of R such that $\cup A_i$ is the set of all non-units in R . By Lemma 26.2 each A_i is contained in some maximal ideal M_i , so that $\cup M_i$ is also the set of non-units in R . Let $M \leq R$ be a maximal ideal; then it contains only non-units, so $M \subset \cup M_i$; by Theorem 26.13, we have $M \subset M_i$ for some i , and then maximality implies $M = M_i$. So R only has the finitely many maximal ideals.

[26.9]

Since $(p) \leq \mathbb{Z}$ is maximal, Corollary 26.15 shows (p^n) is primary for all $n > 0$. Now suppose m is an integer divisible by two distinct primes p and q ; we show (m) is not primary, which finishes the problem. Let $a = \frac{m}{q}$. Then $aq \in (m)$, so if it was primary, we would have $a \in (m)$ or $q^r \in (m)$ for some $r \geq 1$. But m does not divide a since $|a| < |m|$.

And m does not divide q^r since p divides m . This contradiction shows (m) is not primary, as desired.

[26.10]

- (a) Since $R/(x) \cong F[y]$ is a domain, (x) is prime. $(xy) \subset (x)$ so if $I = (x)/(xy)$, then I is an ideal of $\bar{R} = R/(xy)$, and $\bar{R}/I \cong R/(x)$ is still a domain, and I is prime in $\bar{R}$.
- (b) Let S be a ring and $P \leq S$ a prime ideal. Since $P^n \leq P$, we have $\sqrt{P^n} \leq P$. But if $x \in P$, then $x^n \in P^n$, so $x \in \sqrt{P^n}$.
- (c) Since $\bar{x} \cdot \bar{y} = 0$ in $\bar{R}$, the product clearly belongs to I^2 . But $\bar{x} \notin I^2$, since this is equivalent to saying $x \in (x)^2 = (x^2)$ up in R by the correspondence theorem. And this is not true since it would imply $(x) = (x^2)$, but $R/(x)$ is a domain and $R/(x^2)$ has zero divisors. Similarly $\bar{y} \notin \sqrt{I^2} = I$ since it is equivalent to saying $y \in (x)$ up in R , but that is also false, because it implies $(x, y) = (x)$ as ideals, and $R/(x, y) \cong F$ is a field, and $R/(x) \cong F[y]$ is not. Thus $I^2 \leq \bar{R}$ is not primary.

[26.11]

- (a) Since $P \subset P^E$, of course $P^n \leq (P^E)^n$, and then since $P^n \leq R$, we have P^n is contained in $(P^E)^n \cap R = P^{(n)}$.
- (b) Let's show that for ideals $A, B \leq R$ then $(AB)^E = A^E B^E$. This will clearly imply that $(P^n)^E = (P^E)^n$. Since $1 \in S$ we have $S^2 = S$ so that

$$(AB)^E = ABS = ABS^2 = ASBS = A^E B^E$$

- (c) If P is maximal, then P^n is primary, so the previous part and Lemma 26.18(d) show that

$$P^{(n)} = \left[(P^E)^n \right]^C = \left[(P^n)^E \right]^C = P^n$$

[26.12]

If there is a prime ideal with $U \leq P$ but $V \not\leq P$, then in R_P we would have $U^E \leq P^E$ a proper ideal, but $V^E = R_P$. Similar reasoning works with U and V swapped; this means U and V are contained in exactly the same prime ideals. Let this set of primes be $\{P_i\}_I$. Then by Corollaries 26.5 and 26.6 we have

$$U = \sqrt{U} = \bigcap_{i \in I} P_i = \sqrt{V} = V$$

[26.13]

We assume that $I \cap M = \emptyset$, since otherwise this is vacuous. If P is an isolated prime for I and $P \cap M = \emptyset$, then P^E is a prime containing I^E , by Lemma 26.18 parts (a) and (e). If $I^E \leq Q < P^E$ with $Q \leq S$ prime, then $I \leq I^{EC} \leq Q^C < P$ with Q^C prime, again by Lemma 26.18 (parts (a) and (c-f)). Thus Q does not exist, and P^E is an isolated prime for I^E . Let $P_1, \dots, P_n$ be the isolated primes for I that intersect M trivially. As just seen, $P_1^E, \dots, P_n^E$ are isolated primes for I^E .

If $I^E \leq Q$ with $Q \leq S$ prime, then as above we have $I \leq I^{EC} \leq Q^C$ with Q^C prime. By Theorem 26.7 we have $P_i \leq Q^C$ for some i , and then $P_i^E \leq Q^{CE} = Q$. Thus $P_1^E, \dots, P_n^E$ are all the isolated primes over I^E .

[26.14] Let $M = \{b \in \mathbb{Z} \mid b^{-1} \in R\}$. Then from $1 \in R$ and $a^{-1}b^{-1} = (ab)^{-1}$ we see that M is a multiplicative system. Of course $\mathbb{Z} \subset R$ and if $b \in M$, then $b^{-1} \in R$ by definition. Thus the localization $\mathbb{Z}_M \subset R$. An element of R looks like nm^{-1} for $n, m \in \mathbb{Z}$, and we can assume n and m are coprime. There are thus integers $a, b \in \mathbb{Z}$ with

$$am + bn = 1$$

Dividing the above by m , we see that $m^{-1} = a + b(nm^{-1}) \in R$. This means that $m \in M$ so that $nm^{-1} \in \mathbb{Z}_M$, and we have the reverse containment $R \subset \mathbb{Z}_M$.

[26.15]

- (a) If the domain R is a field, then let $b = 0$ for $a = 0$ or $b = a^{-1}$ for $a \in R$ nonzero. Then in all cases $a = a^2b$. Conversely, if R is a von Neumann regular domain, let $a \in R$ be nonzero, and choose $b \in R$ with $a = a^2b$. Then $a(1 - ab) = 0$, and since R is a domain this implies $ab = 1$, so that a has an inverse. $a \in R$ was arbitrary (but nonzero), so R is a field.
- (b) If every ideal in R is radical, let $a \in R$ and let $I = (a^2)$. Since I is radical, we know $\sqrt{I} = I$, and thus $a \in I$. This means there's a $b \in R$ with $a = a^2b$, so R is von Neumann regular. Conversely, if R is von Neumann regular, let $I \leq R$ be an ideal with $a \in \sqrt{I}$, and choose $b \in R$ with $a = a^2b$. If $a^m \in I$ with $m > 1$, then from $a^{m-1} = a^mb$ we see that $a^{m-1} \in I$. Continuing this way shows $a \in I$, so that $I = \sqrt{I}$ is radical.

[26.16] Suppose that $A, B \leq R$ are comaximal ideals, so that there's an $a \in A$ and a $b \in B$ with $a + b = 1$. Of course $AB \subset A \cap B$. But if $x \in A \cap B$, then

$$x = x(a + b) = xa + xb$$

and both xa and xb are in AB . Thus $AB = A \cap B$. For the general case, let $A_1, \dots, A_n$ be pairwise comaximal. Choose $a_i \in A_i$ and $b_i \in A_n$ for $1 \leq i < n$, such that $a_i + b_i = 1$. Then

$$1 = \prod_{i=1}^{n-1} (a_i + b_i) = \prod_{i=1}^{n-1} a_i + (\dots) \in \prod_{i=1}^{n-1} A_i + A_n$$

And thus $\prod_{i=1}^{n-1} A_i$ and A_n are comaximal. The first case done here (and induction) then shows

$$\prod_{i=1}^n A_i = \left(\prod_{i=1}^{n-1} A_i \right) A_n = \left(\prod_{i=1}^{n-1} A_i \right) \cap A_n = \left(\bigcap_{i=1}^{n-1} A_i \right) \cap A_n = \bigcap_{i=1}^n A_i$$

[26.17] Suppose A and B are comaximal, and write $a + b = 1$ with $a \in A$ and $b \in B$. Then under the natural map $R \rightarrow R/A \oplus R/B$, we have that $sa + rb \mapsto (r, s)$, since $a = 1 - b$ maps to $(0, 1)$, and similarly b maps to $(1, 0)$. So our natural map is surjective, with

quotient $A \cap B$, which is equal to AB by the previous problem. We have thus established the isomorphism

$$R/AB \cong R/A \oplus R/B$$

In the general case, we know that $A_1 \cdots A_{n-1}$ is comaximal with A_n from the previous problem, so the first case (and induction) shows

$$\frac{R}{A_1 \cdots A_n} \cong \frac{R}{A_1 \cdots A_{n-1}} \oplus \frac{R}{A_n} \cong \frac{R}{A_1} \oplus \cdots \oplus \frac{R}{A_n}$$

[26.18] If $x, y \in (A : B)$, then $(x + y)B = xB + yB \subset A$, so $(A : B)$ is closed under addition. Also if $r \in R$ then $rxB \subset rA \subset A$, so $(A : B)$ is an ideal (it is non-empty because it contains 0).

Now suppose A is primary and $B \not\subset A$. Let $xy \in (A : B)$, with $x \notin (A : B)$, so that there exists $b \in B$ with $xb \notin A$. Then $(xb)y = (xy)b \in A$, but $xb \notin A$, so since A is primary it must be that $y^m \in A$, and then $y^m \in (A : B)$. This shows $(A : B)$ is primary as well. Of course $A \subset (A : B)$, so $\sqrt{A} \subset \sqrt{(A : B)}$. For the reverse inclusion, let $x^n \in (A : B)$, so that $x^n B \subset A$. If $b \in B \setminus A$, then from $x^n b \in A$ and A being primary, we see that there's an $m > 0$ with $x^{nm} \in A$. This just says that $x \in \sqrt{A}$, and so $\sqrt{(A : B)} \subset \sqrt{A}$.

[26.19] Let $P \in \mathcal{X}$ be a maximal element, and choose $m \in M$ with $mP = 0$. If $A > P$ and $B > P$ are strictly larger ideals, then both are not in $\mathcal{X}$. Since $A \notin \mathcal{X}$, it must be that $mA \neq 0$. If $0 \neq n \in mA$, then from $B \notin \mathcal{X}$ we have $nB \neq 0$. This shows $mAB \neq 0$, and so $AB \not\subset P$. By Lemma 26.1 this shows P is prime.

[26.20]

- (a) Note that every nonzero proper ideal of S is prime. Thus if $T \leq S$ is non-zero, then S/T is a domain. But every ideal of S/T is prime, hence radical, so by [26.15] part (b), S/T is von Neumann regular. By part (a) of that same problem, S/T is a field. This shows the arbitrary nonzero proper ideal T is maximal.
- (b) Let A and B be distinct proper nonzero ideals of S . Then $A \cap B$ is a proper ideal, but it cannot be maximal since $A \cap B < A$. By part (a), it must be that $A \cap B = \{0\}$. If M is any other nonzero proper ideal of S , then M is maximal, hence prime. Since $AB = \{0\} \subset M$, it must be that $A \subset M$ or $B \subset M$. By maximality of all these ideals, either $M = A$ or $M = B$.

[26.21] We give two proofs. First, if $A + B \neq R$, then there's a maximal ideal $M \leq R$ with $A + B \leq M$. Since $\sqrt{M} = M$, this implies $\sqrt{A} \leq M$ and $\sqrt{B} \leq M$, so they cannot be comaximal. This is the contrapositive of what we want to show.

For the second proof, suppose $x \in \sqrt{A}$ and $y \in \sqrt{B}$ are such that $x + y = 1$. Let $x^m \in A$ and $y^n \in B$. Then

$$1 = (x + y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n-i}$$

For each of the terms in that sum, either the exponent of x is $\geq m$, or the exponent of y is $\geq n$. Either way, the term is contained in A or B . This shows $1 \in A + B$, as desired.

[26.22] Let $B = \cap \mathcal{P}'$, and suppose $B \neq \sqrt{A}$. Then it must be that $B \not\subset Q$. Let $P < Q$ be an isolated prime over A , which exists by Theorem 26.7. Since P is prime (hence primary), and $B \not\subset P < Q$, we have by [26.18]

$$P = \sqrt{P} = \sqrt{(P : B)} \supset \sqrt{Q} = Q$$

where we've used that $QB \subset \cap \mathcal{P} = \sqrt{A} \subset P$. The above equation is a contradiction, so it must be that $B = \sqrt{A}$.

Chapter 27

[27.1]

- (a) We know that $\cap_i P_i = \sqrt{I}$ and by Lemma 27.9, there exists an $n > 0$ with $(\sqrt{I})^n \leq I$. We thus have

$$\prod_{i=1}^t P_i^n = \left(\prod_{i=1}^t P_i \right)^n \leq \left(\bigcap_{i=1}^t P_i \right)^n = (\sqrt{I})^n \leq I$$

- (b) Suppose $\prod_i P_i^{e_i} \leq I$ and $e_j = 0$. Then since $I \leq P_j$ we see that

$$\prod_{i \neq j} P_i^{e_i} \leq P_j$$

Since P_j is prime, this means for some $1 \leq k \leq t$ we have $P_k \leq P_j$. Since these are both minimal primes over I , it must be that $P_k = P_j$ and this is a contradiction. Thus $e_j > 0$.

[27.2]

- (a) Note that $\bar{r} \neq 0$ in R/I . Also $P_1, P_2 \leq \text{ann}(\bar{r})$. By Lemma 27.15, $\text{ann}(\bar{r})$ is contained in some associated prime P of R/I . Thus $P_1, P_2 \leq P$. But P is an isolated prime by hypothesis, so minimal over I ; since P_1 and P_2 contain I by hypothesis, we see $P_1 = P = P_2$.
- (b) Call an exponent tuple $(e_1, \dots, e_t)$ *admissible* if $\prod P_i^{e_i} \leq I$. Note that if $(e_1, \dots, e_t)$ is admissible and $(f_1, \dots, f_t)$ is another tuple with $f_i \geq e_i$ for all i , then of course $(f_1, \dots, f_t)$ is admissible as well. We'll say that $(e_1, \dots, e_t)$ is *minimally admissible* if it is admissible and any tuple $(f_1, \dots, f_t)$ with $f_i < e_i$ for some i is not admissible. The problem then asks to show there's a unique minimally admissible tuple.

Before showing existence, we'll show uniqueness. If $(e_1, \dots, e_t)$ and $(g_1, \dots, g_t)$ are minimally admissible tuples, then we can't have $g_i < e_i$ for any i , since then $(g_1, \dots, g_t)$

would not be admissible. Similarly, we can't have $e_i < g_i$ for any i . This shows $g_i = e_i$ for all $1 \leq i \leq t$.

We know from the previous problem that there exists an admissible tuple; pick one $(e_1, \dots, e_t)$ that is minimal in the lexicographic ordering, and note that $e_i > 0$ for all i by part (b) of the previous problem. We will show this is a minimally admissible tuple. Suppose not, that there exists an admissible tuple $(g_1, \dots, g_t)$ with $g_i < e_i$ (and i is the first index where this happens). By the lexicographic minimality of $(e_1, \dots, e_t)$, we know that

$$\prod_{j=1}^{i-1} P_j^{e_j} \cdot P_i^{e_i-1} \cdot \prod_{j=i+1}^t P_j^{e_j} \not\leq I$$

Choose $r \in R$ in the left-hand product, such that $r \notin I$. Of course $rP_i \leq I$, so from part (a) we know that $rP_j \not\leq I$ for all $j \neq i$. This shows that for $j \neq i$,

$$(e_1, \dots, e_j + 1, \dots, e_i - 1, \dots, t)$$

is not admissible. Applying the same reasoning repeatedly to this tuple, we see for any $k \geq 0$ that $(e_1, \dots, e_j + k, \dots, e_i - 1, \dots, t)$ is not admissible. Now if $j \neq i$ and $g_j > e_j$, we do this for $k = g_j - e_j$. If $g_j \leq e_j$, we leave $k = 0$. Doing this for all $j \neq i$ then shows the following tuple is not admissible:

$$(\max(e_1, g_1), \dots, \max(e_{i-1}, g_{i-1}), e_i - 1, \dots, \max(e_t, g_t))$$

But the i th entry of this tuple is at least g_i , and this contradicts $(g_1, \dots, g_t)$ being admissible. Thus no such tuple $(g_1, \dots, g_t)$ exists, and $(e_1, \dots, e_t)$ must be minimally admissible.

[27.3] Let $P < I$ be a finitely generated prime ideal of R , with $I = (a)$; say $P = (ar_1, \dots, ar_t)$ for $r_i \in R$. Since $P \neq I$, we know $a \notin P$, and since P is prime, this implies $r_i \in P$ for all $1 \leq i \leq t$. This means that $P = Pa = PI$. Thus by Lemma 27.11 there exists $x \in I$ with $P(1 - x) = \{0\}$. Since R is a domain and $x \neq 1$, we see that we must have $P = (0)$.

[27.4] For $a \in I$, choose non-zero $x \in M$ with $a \in \text{ann}(x)$. Now $\text{ann}(x)$ is contained in some associated prime P_i for M , and we know there are finitely many such associated primes by Theorem 27.16. Since $a \in I$ was arbitrary, this shows $I \subset \cup P_i$ where the P_i are the associated primes of M . By Theorem 26.13 it must be that $I \leq P_i$ for some i . If $P_i = \text{ann}(y)$ for $y \in M$, this shows $yI = \{0\}$.

[27.5]

- (a) If I is primary, then $I = I$ is a standard Lasker-Noether decomposition of I . By Theorem 27.13, we see that $\text{ass}(R/I) = \{\sqrt{I}\}$. Conversely, assume $\text{ass}(R/I) = \{P\}$. Then again by Theorem 27.13, in a standard Lasker-Noether decomposition we would have $I = Q$ with $\sqrt{Q} = P$. But Q is primary, and hence so is I .
- (b) Part (a) implies I is primary with $\sqrt{I} = P$. By Lemma 27.9 there exists an $n > 0$ with $P^n \leq I$. This means that $(R/I) P^n = \{0\}$.

[27.6]

- (a) Let $I = \text{ann}(x)$ so that $xR \cong R/I$. The associated primes of xR are a subset of those for M , so we see that R/I has associated primes $\{P\}$. By the previous problem, $(R/I)P^n = \{0\}$ for some $n > 0$, and since $RP^n = P^n$ this shows $(xR)P^n = xP^n = \{0\}$.
- (b) Let $M = \langle x_1, \dots, x_t \rangle$. By the previous part, we can find positive integers $n_1, \dots, n_t$ with $x_i P^{n_i} = \{0\}$. If $n = \max(n_i)$ then $x_i P^n = \{0\}$ for all x_i , and hence $MP^n = \{0\}$.

[27.7]

- (a) Saying $I \leq R$ is a primary ideal is saying that for $x, r \in R$ with $xr \in I$ and $x \notin I$, we must have $r^n \in I$ for some $n \geq 0$. Since this is equivalent to insisting that $Rr^n \leq I$, this is the same as saying I is primary as a submodule of R .
- (b) Assume first that P is the only associated prime of M/N . By the previous problem, $(M/N)P^n = \{0\}$ for some integer n . This is equivalent to $MP^n \leq N$. If $x \in M \setminus N$ and $xr \in N$ for some $r \in R$, then $\bar{x} \neq 0$ in M/N so $r \in \text{ann}(\bar{x})$. By Lemma 27.15, $r \in P$. Thus we have

$$Mr^n \leq MP^n \leq N$$

and N is primary. Conversely, let N be primary and P, Q two associated primes of M/N . Choose $x, y \in M \setminus N$ with $P = \text{ann}(\bar{x})$ and $Q = \text{ann}(\bar{y})$. If $r \in P$ then $xr \in N$ but $x \notin N$, so N being primary means there's an integer n with $Mr^n \leq N$. In particular, $yr^n \in N$ so that $r^n \in Q$. Since Q is prime, this means $r \in Q$, and since $r \in P$ was arbitrary, this shows $P \leq Q$. Swapping the roles of P and Q shows also $Q \leq P$ so that $P = Q$.

[27.8]

Let $BA = \cap_i Q_i$ be a standard Lasker-Noether decomposition, with $\sqrt{Q_i} = P_i$. If $B \not\leq Q_i$ for some i , then there exists $b \in B \setminus Q_i$. since $bA \leq Q_i$, it must be that $A \leq \sqrt{Q_i} = P_i$. Lemma 27.9 guarantees the existence of an integer n_i with $P_i^{n_i} \leq Q_i$, and thus $A^{n_i} \leq Q_i$. If we do this for all i where $B \not\leq Q_i$, we get a finite collection $\{n_j, \dots\}$ where $A^{n_j} \leq Q_j$. Letting n be $\max(n_j, \dots)$ we see that

$$B \cap A^n \subset \bigcap_{i=1}^t Q_i = BA$$

[27.9]

- (a) Let $x \in M$ and $B = \{r \in R \mid xr \in N\}$. If $r, s \in B$ and $t \in R$, then of course

$$\begin{aligned} x(r+s) &= xr + xs \\ xrt &= (xr)t \end{aligned}$$

Since N is a submodule, both right-hand expressions are in N , so $B \leq R$ is an ideal. Now suppose $a \in A \leq R$ with $xa \in N$. Then by definition $a \in B$, so $xa \in x(A \cap B)$. Conversely, if $r \in A \cap B$, then $xr \in N$ and $xr \in xA$. So we've shown

$$xA \cap N = x(A \cap B)$$

(b) By the previous problem, choose n such that $B \cap A^n \leq BA$. Then by part (a)

$$xA^n \cap N = x(A^n \cap B) \leq xBA = (xB)A \leq NA$$

(c) This is clearly true if $N = M$, so we assume $N < M$. Note that M is Noetherian, so if the statement is false, there's a maximal $N \leq M$ where it fails; this means there must be an ideal $U \leq R$ such that $MU^n \cap N \not\leq NU$ for any $n \geq 0$. If $x \in M \setminus N$, we have that $xR + N > N$, and hence the statement doesn't fail for $xR + N$. For any ideal $V \leq R$ then, there exists an integer $n \geq 0$ with

$$MV^n \cap (xR + N) \leq (xR + N)V = xV + NV$$

Intersecting both sides with N gives $MV^n \cap N \leq NV + (xV \cap N)$ (this uses $NV \leq N$ and Dedekind's lemma). By part (b) there's an $m \geq 0$ with $xU^m \cap N \leq NU$, and thus if $V = U^m$ the above gives

$$MU^{mn} \cap N \leq NU^m + (xU^m \cap N) \leq NU^m + NU \leq NU$$

This contradicts the choice of $N < M$, and this contradiction shows no such N exists.

[27.10] Suppose R/A and R/B are both Noetherian (or Artinian). Since $AB \leq AB$, we see that A/AB is naturally an R/B module. Since A is finitely generated as an R -module, A/AB is finitely generated as an R/B -module, and hence is Noetherian (or Artinian) as an R/B -module, and hence as an R -module as well. The short exact sequence

$$0 \rightarrow A/AB \rightarrow R/AB \rightarrow R/A \rightarrow 0$$

shows R/AB is Noetherian (or Artinian) as well.

[27.11] Let $\mathcal{X} = \{I \leq R \mid R/I \text{ not Artinian}\}$. Since $(0) \in \mathcal{X}$ by hypothesis, we see that since R is Noetherian there's a maximal element $P \in \mathcal{X}$. Then R/P is non-Artinian, and we just need to show P is prime. If $A > P$ and $B > P$ are such that $AB \leq P$, then R/A is Artinian, as is R/B . By the previous problem, R/AB is Artinian. But R/AB has quotient R/P , which is non-Artinian. This contradiction shows A and B don't exist, so P is prime.

[27.12] Let $\mathcal{X}$ be the set of non-finitely-generated ideals of R . If we assume R is not Noetherian, then $\mathcal{X}$ is non-empty. If $\{I_\alpha\}_A$ is some linearly ordered set of elements of $\mathcal{X}$, then $J = \cup I_\alpha$ is an ideal of R . If it was finitely generated, then the finitely many generators would end up in I_α for some $\alpha \in A$, meaning $J = I_\alpha$ is finitely generated. This contradiction shows $J \in \mathcal{X}$, so the hypotheses of Zorn's lemma are satisfied. Let $P \in \mathcal{X}$ be a maximal element, and note $P \leq R$ cannot be prime by hypothesis.

Choose ideals $A > P$ and $B > P$ with $AB \leq P$. Then R/A and R/B are Noetherian, since every ideal is finitely generated by the correspondence theorem and maximality of $P \in \mathcal{X}$. By [27.10] R/AB is also Noetherian. This implies P/AB is finitely generated. Since A and B are finitely generated (neither is in $\mathcal{X}$), so is AB . Together this implies P is finitely

generated (generated by generators of AB and preimages of generators of P/AB). That's our final contradiction to R not being Noetherian.

[27.13] If $I \leq R$ is radical, then it is the intersection of its isolated primes by Corollary 26.8, of which there are finitely many by Corollary 27.5. So we can write $I = \cap_i P_i$ for $1 \leq i \leq t$. Since each P_i is primary, this is a primary decomposition, and it is standard because it is irredundant by Corollary 26.9. By the uniqueness of these primary decompositions (Theorem 27.13), $\{P_1, \dots, P_t\}$ are all the associated primes of I (this relies on $\sqrt{P_i} = P_i$ because P_i is prime). This shows all associated primes of I are isolated, so it has no embedded primes.

[27.14] R , as a module over itself, is surely finitely generated, and hence there are finitely many associated primes of R by Theorem 27.16; let these associated primes be $\{P_1, \dots, P_t\}$, and choose non-zero $r_i \in R$ with $P_i = \text{ann}(r_i)$. This shows each P_i is contained in Z , the set of zero divisors in R . Conversely, if $z \in Z$, then there's a non-zero $r \in R$ with $z \in \text{ann}(r)$. By Lemma 27.15, we must have $z \in P_i$ for some $1 \leq i \leq t$. So we have shown $Z = \cup_i P_i$, a finite union of prime ideals.

Chapter 28

[28.1] Let $t \in T$ be a zero of the monic polynomial

$$f(x) = x^n + s_{n-1}x^{n-1} + \dots + s_1x + s_0$$

where the $s_i \in S$. We know that $U := R[s_0, \dots, s_{n-1}]$ is a finitely-generated R -module by Lemma 28.8. We also know that $U[t]$ is a finitely-generated U -module by the same lemma. But then $U[t]$ is a finitely-generated R -module. To see this, let $\mathcal{X} \subset U$ be a finite set so that $U = R\mathcal{X}$, and similarly choose $\mathcal{Y} \subset U[t]$ with $U[t] = U\mathcal{Y}$. Then $\mathcal{Z} = \mathcal{X}\mathcal{Y}$ is a finite set, and for any element $v \in U[t]$, we have

$$v = \sum_{y \in \mathcal{Y}} u_y y = \sum_{y \in \mathcal{Y}} \sum_{x \in \mathcal{X}} (r_{xy} x) y = \sum_{xy \in \mathcal{X}\mathcal{Y}} r_{xy} (xy)$$

Since v was arbitrary, this shows $U[t] = R\mathcal{Z}$, as desired. By Lemma 28.7, then, $t \in U[t]$ is integral over R .

[28.2] First, note that $\omega^2 = -1 - \omega$, and thus every element of $\mathbb{Q}[\omega]$ can be written as $a + b\omega$ with $a, b \in \mathbb{Q}$. Since $\{1, \omega\}$ is $\mathbb{Q}$ -linearly independent, and $[\mathbb{Q}[\omega] : \mathbb{Q}] = 2$, we see that $\{1, \omega\}$ is a $\mathbb{Q}$ -basis for $\mathbb{Q}[\omega]$ over $\mathbb{Q}$. Let $R \leq \mathbb{Q}[\omega]$ be the algebraic integers; we want to show that for every $a + b\omega \in R$, we can take both a and b in $\mathbb{Z}$.

Let $\sigma \in \text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ be the non-trivial automorphism (complex conjugation), where $\sigma(\omega) = \omega^2$. Then if $a + b\omega \in R$, we see that so is

$$\sigma(a + b\omega) = a + b\omega^2 = a + b(-1 - \omega) = (a - b) - b\omega$$

Since $(a + b\omega) + \sigma(a + b\omega) \in \mathbb{Q} \cap R = \mathbb{Z}$, we see that $2a - b \in \mathbb{Z}$. Knowing that $\omega \in R$, the same reasoning applied to $(a + b\omega)\omega = -b + (a - b)\omega$ shows that $a - 3b \in \mathbb{Z}$. From these two expressions it's not hard to see that both

$$\begin{aligned} 3(2a - b) - (a - 3b) &= 5a \\ (2a - b) - 2(a - 3b) &= 5b \end{aligned}$$

are in $\mathbb{Z}$. So we can write $a = \frac{u}{r}$ and $b = \frac{v}{s}$ where $u, v \in \mathbb{Z}$ and $r, s \in \{1, 5\}$. Of course if $r = 1$, then from $a - 2b \in \mathbb{Z}$ we see $s = 1$ as well; similarly if we assume $s = 1$. Thus we are done unless we have $r = s = 5$.

Assuming this case, we can now look at

$$(a + b\omega)\sigma(a + b\omega) = \left(\frac{u + v\omega}{5}\right) \left(\frac{u + v\omega^2}{5}\right) = \frac{u^2 - uv + v^2}{25}$$

As before, this product is in $\mathbb{Q} \cap R = \mathbb{Z}$, so that 25 divides $u^2 - uv + v^2$. From $a - 2b \in \mathbb{Z}$ we see that 5 divides $u - 2v$, and hence 25 divides $(u - 2v)^2 = u^2 - 4uv + 4v^2$. Adding these two quadratics shows

$$0 \equiv (u^2 - uv + v^2) + (u^2 - 4uv + 4v^2) \equiv 2u^2 \pmod{5}$$

This implies 5 divides u , and hence $a \in \mathbb{Z}$. Of course then so is $b \in \mathbb{Z}$. Altogether, we've shown $R \subset \mathbb{Z}[\omega]$, and since $\omega \in R$, we actually have equality.

[28.3] Let $h(x) = a_n x^n + \cdots + a_0$ be a polynomial in $\mathbb{Z}[x]$. Define $\tau h \in \mathbb{Z}[x]$ as

$$\tau h(x) = x^{\deg(h)} h\left(\frac{1}{x}\right) = a_0 x^n + \cdots + a_n$$

We will assume α is non-zero, and note that $f(x) \in \mathbb{Z}[x]$ by Lemma 28.10. First, assume $f(0) = \pm 1$. Then α^{-1} is a root of $\pm \tau f(x)$, which is a monic polynomial in $\mathbb{Z}[x]$. Thus α^{-1} is an algebraic integer. Conversely, suppose α^{-1} is an algebraic integer, with minimal polynomial $g(x)$, which lives in $\mathbb{Z}[x]$ by Lemma 28.10. Then α^{-1} is still a root of $\tau f(x)$, and so $g(x)$ divides $\tau f(x)$. Similarly $f(x)$ divides $\tau g(x)$. It follows from these divisibilities that

$$\deg(g) \leq \deg(\tau f) \leq \deg(f) \leq \deg(\tau g) \leq \deg(g)$$

So $\deg(g) = \deg(f)$, and it must be that $\tau f(x) = f(0)g(x)$. This implies that $f(0)$ divides every coefficient of $\tau f(x)$ (which are the same coefficients of $f(x)$), and hence that $f(0)$ divides 1 (the constant term of $\tau f(x)$ and leading term of $f(x)$). Since $f(0) \in \mathbb{Z}$ we have $f(0) = \pm 1$.

[28.4] Let α be a nonzero algebraic integer, and let $f(x) \in \mathbb{Z}[x]$ be its minimal polynomial. For any nonzero integer $n \in \mathbb{Z}$, we see that $\frac{\alpha}{n}$ is a root of $f(nx) \in \mathbb{Z}[x]$. Now if $f(nx) = g(x)h(x)$, we would also have

$$f(x) = g\left(\frac{x}{n}\right) h\left(\frac{x}{n}\right)$$

Since $f(x)$ is irreducible in $\mathbb{Q}[x]$, we must have g or h is constant. In other words, if $\deg(f) = k$, then $n^{-k}f(nx)$ is an irreducible monic polynomial in $\mathbb{Q}[x]$, for which $\frac{\alpha}{n}$ is a root, so $n^{-k}f(nx)$ is the minimal polynomial for $\frac{\alpha}{n}$. By Lemma 28.10, if $\frac{\alpha}{n}$ is an algebraic integer, then $n^{-k}f(nx) \in \mathbb{Z}[x]$. In particular, we see that n^k must divide $f(0)$. This shows $|n|$ is bounded by $|f(0)|$, and so there are only finitely many integers where $\frac{\alpha}{n}$ is an algebraic integer. Call this finite set $\mathcal{D}$.

By picking a maximal element $n \in \mathcal{D}$ we get the first part of the problem. Now suppose $\frac{\alpha}{m}$ is an algebraic integer. Pick integers $a, b \in \mathbb{Z}$ with $am + bn = d$, the GCD of m and n . Then the following is an algebraic integer:

$$a \left(\frac{\alpha}{n} \right) + b \left(\frac{\alpha}{m} \right) = \frac{am\alpha}{mn} + \frac{bn\alpha}{mn} = \frac{\alpha}{mn/d}$$

$mn/d \in \mathbb{Z}$ and thus $mn/d \in \mathcal{D}$. By maximality then, $mn \leq dn$; but $d \leq m$ and hence $d = m$, so m divides n .

[28.5] Since $I \subset R$ is an S -ideal, it is of course an R -ideal as well, and hence finitely generated, say $I = \langle x_1, \dots, x_n \rangle$. Since $R \neq S$, choose $s \in S \setminus R$; note that s is non-integral over R since R is integrally closed. Saying that $Is \subset I$ means there are $r_{ij} \in R$ such that

$$x_j s = \sum_{i=1}^n x_i r_{ij}$$

Letting $X = (x_1, \dots, x_n)$, we can then form the matrix $A = (r_{ij})$ such that $Xs = XA$. In particular, $X(Is - A) = 0$. Letting B be the adjugate of $(Is - A)$, we see then that $X(Is - A)B = X \det(Is - A) = 0$. Let $d = \det(Is - A) \in S$.

Since $Xd = 0$, we see that $Id = 0$. If $d = 0$, then s would be a zero of the monic polynomial $\det(It - A) \in R[t]$, and this contradicts s being non-integral over R . Thus $d \neq 0$.

[28.6] Suppose $\mathbb{Z} \subset T \subset \mathbb{C}$ and there exists nonzero $n \in \mathbb{Z}$ with nT algebraic integers. For the sake of contradiction, assume there exists $s \in T$ that is not integral over $\mathbb{Z}$ (of course s is algebraic though). Let $R \leq \mathbb{Q}[s]$ be the ring of integers, so that R is Noetherian and integrally closed (and is in fact a Dedekind domain). Since $s \notin R$, we can form the proper overring $S = R[s]$. Finally define the S -ideal $I = \{r \in R \mid rS \subset R\}$.

By the previous problem, there exists $d \neq 0$ in S such that $Id = \{0\}$. Since $\mathbb{Q}[s]$ is a domain, this means that $I = \{0\}$. However, for any integer m we have $s^m \in T$ so that $ns^m \in R$; this implies $n \in I$. We now have a contradiction, showing s does not exist.

[28.7]

- (a) Let $f(x)$ be as in the problem. Note that $f(x) \in F[c_0, \dots, c_{n-1}]$. Since $f(\alpha_i) = 0$, we see that α_i satisfies a monic polynomial over $F[c_0, \dots, c_{n-1}]$, and hence is integral over it. This is true for all i , and by Lemmas 28.8 and 28.7 we see $F[\alpha_1, \dots, \alpha_n]$ is integral over $F[c_0, \dots, c_{n-1}]$.

- (b) Assume that $\{\alpha_1, \dots, \alpha_n\}$ is algebraically independent over F , so that $F(\alpha_1, \dots, \alpha_n)$ has transcendence degree n over F . By part (a), $F(\alpha_1, \dots, \alpha_n)$ is algebraic over $F(c_0, \dots, c_{n-1})$, so by Theorem 24.8 $F(c_0, \dots, c_{n-1})$ has transcendence degree n over F . By Lemma 24.4, this implies $\{c_0, \dots, c_{n-1}\}$ is algebraically independent over F .

Thus $F(c_0, \dots, c_{n-1})$ is a rational function field, the field of fractions of $F[c_0, \dots, c_{n-1}]$. But this latter ring is a UFD, hence integrally closed. By part (a) then,

$$F[\alpha_1, \dots, \alpha_n] \cap F(c_0, \dots, c_{n-1}) \subset F[c_0, \dots, c_{n-1}]$$

Since the other containment direction is obvious, we have an equality.

[28.8] With $n = [E : \mathbb{Q}]$, write

$$\prod_{\sigma \in \text{Gal}(E/\mathbb{Q})} (x - \alpha^\sigma) = x^n + c_{n-1}x^{n-1} + \dots + c_0$$

Note that $c_i \in \mathbb{Q}$ while also being algebraic integers; hence $c_i \in \mathbb{Z}$. c_i is a sum of $\binom{n}{i}$ terms, each a product of i conjugates of α . The problem hypothesis then implies

$$|c_i| \leq \binom{n}{i} a^i$$

In particular, there are only finitely many integers c_i could be. There are thus only finitely many monic polynomials of degree n whose coefficients all satisfy these bounds. The roots of all such polynomials then form a finite set; call it $\mathcal{T}$. Since $\mathcal{S} \subset \mathcal{T}$, we see that $\mathcal{S}$ is also finite.

[28.9] The assumption of being Abelian can be weakened; we will only assume that all elements of $\text{Gal}(E/\mathbb{Q})$ commute with the complex conjugation map τ . By (iii) of Theorem 18.4, $\tau(E) = E$, and hence $\tau \in \text{Gal}(E/\mathbb{Q})$ (note that it might be the trivial automorphism). From the $|\alpha| = 1$ hypothesis, we see then

$$|\alpha^\sigma|^2 = (\alpha^\sigma)(\alpha^\sigma)^\tau = (\alpha)^\sigma(\alpha^\tau)^\sigma = (\alpha\alpha^\tau)^\sigma = (|\alpha|^2)^\sigma = 1^\sigma = 1$$

So $|\alpha^\sigma| = 1$. Since $\sigma \in \text{Gal}(E/\mathbb{Q})$ was arbitrary, the previous problem implies $\alpha \in \mathcal{S}$, a finite set. But for any integer $m > 0$, $|\alpha^m| = |\alpha|^m = 1$, and hence $\alpha^m \in \mathcal{S}$. As a finite set, we must have some $n > m$ with $\alpha^m = \alpha^n$, implying $\alpha^{n-m} = 1$, so that α is a root of unity.

[28.10] Let F be the field of fractions of R , so that $R \leq S \leq F$. Suppose $ar^{-1} \in F$ is such that it is integral over S . Using that every element of S looks like bm^{-1} for $m \in M$, we know there's a monic polynomial over S with ar^{-1} as a root:

$$(ar^{-1})^n + b_{n-1}m_{n-1}^{-1}(ar^{-1})^{n-1} + \dots + b_0m_0^{-1} = 0$$

Set $m := m_0m_1 \cdots m_{n-1}$. Multiplying the above expression by m^n gives

$$(amr^{-1})^n + \frac{b_{n-1}m}{m_{n-1}}(amr^{-1})^{n-1} + \dots + \frac{b_0m^n}{m_0} = 0$$

Each of these coefficients is in R , hence amr^{-1} is integral over R , and hence belongs to R . Since $m \in M$, this means $ar^{-1} = (amr^{-1})m^{-1} \in S$. We have thus shown S is integrally closed.

[28.11] From the text, we know that an integral basis for $\mathbb{Q}[\sqrt{d}]$ looks like $\{1, \sqrt{d}\}$ when $d \not\equiv 1 \pmod{4}$. Using that the non-trivial element of the Galois group sends $\sqrt{d}$ to $-\sqrt{d}$, we can then compute the discriminant

$$\det \begin{pmatrix} 1+1 & \sqrt{d}-\sqrt{d} \\ \sqrt{d}-\sqrt{d} & d+d \end{pmatrix} = 4d$$

When $d \equiv 1 \pmod{4}$, the text shows an integral basis can be taken as $\{1, \frac{1+\sqrt{d}}{2}\}$. Again we compute the discriminant:

$$\det \begin{pmatrix} 1+1 & \frac{1+\sqrt{d}}{2} + \frac{1-\sqrt{d}}{2} \\ \frac{1+\sqrt{d}}{2} + \frac{1-\sqrt{d}}{2} & \frac{1+2\sqrt{d}+d}{4} + \frac{1-2\sqrt{d}+d}{4} \end{pmatrix} = (1+d) - 1 = d$$

[28.12] Let $\mathcal{C}$ be representatives for the conjugacy classes of G , and for $x \in \mathcal{C}$, let K_x be the size of the conjugacy class. Then we have

$$\begin{aligned} \langle \chi, \chi \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi}(g) \\ &= \frac{1}{|G|} \sum_{x \in \mathcal{C}} K_x \chi(x) \overline{\chi}(x) \\ &= \frac{\chi(1)}{|G|} \sum_{x \in \mathcal{C}} \chi(x) \frac{K_x \overline{\chi}(x)}{\chi(1)} \\ &= \frac{\chi(1)}{|G|} \sum_{x \in \mathcal{C}} \chi(x) \overline{\omega}_\chi(x) \end{aligned}$$

Since χ is irreducible, $\langle \chi, \chi \rangle = 1$, and we thus have the problem's sum is $\frac{|G|}{\chi(1)}$. Since the sum is an algebraic integer, and clearly a rational number, it is a rational integer; in particular, $\chi(1)$ divides $|G|$.

[28.13] Suppose G is simple and $|\mathcal{S}| \leq 2$. If G is non-Abelian, then $\mathcal{S}$ is non-empty (there must be non-linear irreducible characters), so pick $p \in \mathcal{S}$. By the previous problem, p divides $|G|$, so let $P \leq G$ be a Sylow p -subgroup. If $g \in Z(P)$ is a non-trivial element, then $[G : C_G(g)]$ is not divisible by p . Let $\mathcal{A}$ be the irreducible characters of degree divisible by p , and $\mathcal{B}$ the non-trivial irreducible characters whose degree is not divisible by p . Note that G is non-Abelian simple, so it has no non-trivial linear characters. If ρ is the regular representation, then

$$0 = \rho(g) = 1 + \sum_{\chi \in \mathcal{A}} \chi(1)\chi(g) + \sum_{\chi \in \mathcal{B}} \chi(1)\chi(g)$$

By Lemma 28.28 and Theorem 28.27, the sum over $\mathcal{A}$ is zero. If $|\mathcal{S}| = 1$, then $\mathcal{B}$ is empty, and we have the contradiction $0 = 1$. If $q \neq p$ is in $\mathcal{S}$, then q divides $\chi(1)$ for each $\chi \in \mathcal{B}$,

and the above gives $0 = 1 + q\alpha$, where α is an algebraic integer. This implies $-q^{-1}$ is an algebraic integer, and that's our final contradiction. So G is Abelian, and by simplicity must be of prime order.

[28.14] By [28.12], the only possible degrees for the characters are $\{1, p, p^2, p^3\}$. Since, over the irreducible characters, $\sum \chi(1)^2 = |G| = p^3$, we see the actual possibilities are $\{1, p\}$. Of course $p^3 > [G : G'] > 1$, and hence there are either p or p^2 linear characters of G . Let $\mathcal{A}$ be the linear characters, and $\mathcal{B}$ the irreducible non-linear characters. Then from

$$p^3 = \sum_{\chi \in \mathcal{A}} \chi(1)^2 + \sum_{\chi \in \mathcal{B}} \chi(1)^2 = |\mathcal{A}| + p^2 |\mathcal{B}|$$

We see that if $|\mathcal{A}| = p$, we would have p^2 dividing $p^3 - p$, which doesn't happen. Thus $|\mathcal{A}| = p^2$, and $\mathcal{B}$ has $(p^3 - p^2)/p^2 = p - 1$ characters. Since $|\mathcal{A}| + |\mathcal{B}|$ is the number of conjugacy classes in G , we see that number is $p^2 + p - 1$.

[28.15] Since $\chi(g)$ is a sum of roots of unity, there is a cyclotomic field $\mathbb{Q}(\zeta_n)$ containing $\chi(g)$. Since $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is Abelian, and $\chi(g)$ is an algebraic integer, [28.9] applies, and $\chi(g)$ is a root of unity.

Chapter 29

[29.1] Let $R = F[x, y]$ and $A = (x, y) \leq R$, and suppose $p/q \in A^{-1} \subset F(x, y)$. Then we must have both px/q and py/q in R ; since p and q can be chosen to be relatively prime, this means q divides x and divides y . By considering degrees, this can only happen when $q \in F$. Thus $A^{-1} \subset R$; clearly $R \subset A^{-1}$ so $A^{-1} = R$. Then $(A^{-1})^{-1} = R \neq A$.

[29.2] A PID is always a UFD, so assume that R is a Dedekind domain that is an UFD, and we will show it's a PID. Let $M \leq R$ be a maximal ideal; we can assume $M \neq (0)$ since otherwise R is a field, and of course is a PID. Choose a non-zero $a \in M$, and write $a = \pi_1 \cdots \pi_t$ as a product of irreducibles. Note that $t \geq 1$ since a is a non-unit. Since M is prime, we see there is some $\pi_i \in M$. Since R is a UFD, (π_i) is a prime ideal; since R is a Dedekind domain, (π_i) is maximal. This implies $M = (\pi_i)$. Thus all maximal ideals of R are principal. This means all prime ideals of R are principal, and hence R is a PID by Theorem 26.12.

[29.3] Suppose $A \leq R$ is an ideal maximal with regards to $A^{-1} \not\subset R$. If A is not prime, then there exists ideals $B, C > A$ with $BC \leq A$. By maximality, $B^{-1}, C^{-1} \subset R$. Now if $x \in (BC)^{-1}$, then $xC \subset B^{-1} \subset R$, and hence $x \in C^{-1}$. This shows $(BC)^{-1} \subset R$; but $A^{-1} \subset (BC)^{-1}$, and this contradiction shows A must be prime.

[29.4] Let $M \leq R$ be a maximal ideal, with non-zero $x \in M$. By hypothesis we have

$$(x) = M_1 \cdots M_t$$

for maximal ideals $M_1, \dots, M_t$. Since $M_1 \cdots M_t \subset M$, and M is prime, we must have some $M_i = M$; we will assume $M_1 = M$. Since (x) is invertible (indeed, $(x)^{-1} = (x^{-1})$), we see that

$$M(M_2 \cdots M_t)(x^{-1}) = R$$

and hence M is invertible. Thus all maximal ideals of R are invertible. Since all nonzero ideals are products of maximal ideals by hypothesis, all nonzero ideals are invertible. By Theorem 29.6, R is a Dedekind domain.

[29.5] Let $S = R_M$. By [28.10], S is integrally closed. By Corollary 26.19, S is Noetherian. Suppose $(0) < P < Q$ are prime ideals of S . By parts (c) and (f) of Lemma 26.18,

$$(0) < P \cap R < Q \cap R$$

is a strict ascending chain of prime ideals of R . This is impossible because R is a Dedekind domain (all nonzero prime ideals are maximal), and hence no such chain exists in S . Thus we have shown S is a Dedekind domain.

If $M = R \setminus P$ for a prime ideal $P < R$, then by Lemma 26.18(g), $P^E \leq S$ is the unique maximal ideal of S , and hence the unique nonzero prime ideal. By Corollary 29.12, S is a PID.

[29.6] Let $E = \mathbb{Q}[\alpha_1, \dots, \alpha_n]$, a finite algebraic extension over $\mathbb{Q}$. If S is the ring of integers in E , then $S \leq R$ and S is a Dedekind domain, and E is its field of fractions (this is Theorem 29.17). $A \cap S \leq S$ is a proper ideal (it doesn't contain 1), and thus by Lemma 29.20, there is a $\beta \in E$ with $\beta\alpha_i \in S$ for all i , but not all $\beta\alpha_i$ are in $A \cap S$. Since $\beta\alpha_i \in S \leq R$, we see $\beta\alpha_i \in A \cap S$ if and only if $\beta\alpha_i \in A$, so we are done.

[29.7] Let $P_1, \dots, P_t$ be the non-principal prime ideals of R . By finite approximation, choose $x_i \in R$ for $1 \leq i \leq t$ such that

$$(x_i) = P_i Q_1 \cdots Q_m$$

where $m \geq 0$ and the Q_j are (not necessarily distinct) principal prime ideals. In particular, $x_i \notin P_k$ for $k \neq i$. If $Q_j = (y_j)$ for $y_j \in R$, then the above yields

$$(x_i \prod y_j^{-1}) = P_i$$

and so P_i is principal. Since we now have that all prime ideals of R are principal, Theorem 26.12 shows R is a PID.

[29.8]

- (a) Let $f_A(P) = e$ and $f_B(P) = f$, and assume without loss of generality $e \leq f$. Since $A \not\subset P^{e+1}$ by Lemma 29.14, and $A \leq A + B$, we see that $f_{A+B}(P) \leq e$. But both A and B are contained in P^e , and hence so is $A + B$. This shows $f_{A+B}(P) = e$, as desired.

(b) As above assume $f_A(P) = e \leq f = f_B(P)$. Define an ideal $I \leq R$ such that $f_I(P)$ is $\max(f_A(P), f_B(P))$ for all nonzero prime ideals P . Then $I \leq A \cap B$, and this shows $f_{A \cap B}(P) \leq f$ since $I \not\subset P^{f+1}$ by Lemma 29.14. But $A \cap B \leq B \leq P^f$, and so also $f_{A \cap B}(P) \geq f$. This shows $f_{A \cap B}(P) = f$, and in general $f_{A \cap B}(P) = \max(f_A(P), f_B(P))$.

(c) We have

$$f_{AB}(P) = f_A(P) + f_B(P) = \min(f_A(P), f_B(P)) + \max(f_A(P), f_B(P)) = f_{A+B}(P) + f_{A \cap B}(P)$$

Since this holds for all nonzero prime ideals, unique factorization shows that we have $AB = (A + B)(A \cap B)$.

[29.9] Of course all nonzero primes in a Dedekind domain R are maximal, so that their powers are primary by Corollary 26.15. Let $I \leq R$ be a primary ideal, and suppose

$$I = \prod P_i^{e_i}$$

Then from $I \leq P_1$ we see that $\sqrt{I} \leq P_1$. But $\sqrt{I}$ is prime by Lemma 26.14, and since nonzero primes are maximal we have $\sqrt{I} = P_1$. Applying this reasoning to $I \leq P_i$ with $i > 1$ shows $P_1 = \sqrt{I} = P_i$. Thus $I = P_1^{e_1}$ is a power of a prime ideal.

[29.10] Let $\mathcal{X} = \{x_1, \dots, x_m\} \subset M$ be an R -linearly independent subset of M , and also let $\mathcal{Y} = \{y_1, \dots, y_n\} \subset M$ be a weak generating set. We will show $m \leq n$, which solves the problem if we take $\mathcal{Y}$ to be a minimal weak generating set.

For each $1 \leq i \leq m$, choose nonzero $r_i \in R$ and $a_{ij} \in R$ such that

$$r_i x_i = \sum_{j=1}^n a_{ij} y_j$$

Let F be the fraction field of R , and let F^m have basis $\{e_i\}$ and F^n have basis $\{f_j\}$. Define an F -linear map $g : F^m \rightarrow F^n$ by setting

$$g(e_i) = \sum_{j=1}^n a_{ij} f_j$$

Suppose $\sum b_i e_i \in \ker(g)$, and by clearing denominators we can assume the $b_i \in R$. Then we have $\sum \sum b_i a_{ij} f_j = 0$, and by the linear independence of the $\{f_j\}$ this means $\sum b_i a_{ij} = 0$ for all $1 \leq j \leq n$. But in M we have

$$\sum_{i=1}^m b_i r_i x_i = \sum_{i=1}^m \sum_{j=1}^n b_i a_{ij} y_j = \sum_{j=1}^n \sum_{i=1}^m b_i a_{ij} y_j = 0$$

Since $\mathcal{Y}$ is R -linearly independent, we have $b_i r_i = 0$ for all $1 \leq i \leq m$. Since R is a domain and $r_i \neq 0$, this means $b_i = 0$ for all i . Thus the kernel of g is trivial, and it is an injective map. This of course means $m \leq n$, as desired.

[29.11] Let $\mathcal{X} = \{x_1, \dots, x_n\}$ be a minimal weak generating set of M . For $m \in M$, we have nonzero $r \in R$ such that

$$rm = \sum_{i=1}^n a_i x_i$$

Define a map $\Phi : M \rightarrow F^n$ by $\Phi(m) = (\frac{a_1}{r}, \dots, \frac{a_n}{r})$. To see this is well-defined, suppose there's a nonzero $s \in R$ with $sm = \sum b_i x_i$. Then we have

$$\sum_{i=1}^n r b_i x_i = rsm = \sum_{i=1}^n s a_i x_i$$

and this means $rb_i = sa_i$ for all $1 \leq i \leq n$, since $\mathcal{X}$ is R -linearly independent. This easily implies $\Phi(m)$ is well-defined.

We now show Φ is R -linear. Clearly $s\Phi(m) = \Phi(sm)$. If $n \in M$ with $sn = \sum b_i x_i$, then

$$\begin{aligned} rs(m+n) &= \sum (sa_i + rb_i)x_i \\ \Phi(m+n) &= \left(\frac{sa_1 + rb_1}{rs}, \dots, \frac{sa_n + rb_n}{rs} \right) \\ &= \Phi(m) + \Phi(n) \end{aligned}$$

So all that's left is to show Φ is injective. But if $\Phi(m) = 0$, then all the $a_i = 0$, so that $rm = 0$. Since M is torsion-free, this means $m = 0$. Thus M is isomorphic to the R -submodule $\Phi(M) \leq F^n$.

[29.12]

- (a) If $m, n \in T$, then there exists nonzero $r, s \in R$ with $rm = sn = 0$. So $rs(m+n) = 0$, and $m+n \in T$. For any $a \in R$, of course $r(am) = a(rm) = 0$, so $am \in T$, and T is an R -submodule of M .

Now suppose $\bar{x} \in M/T$ is such that for nonzero $r \in R$, $r\bar{x} = 0$. Then $rx \in T$, so there's a non-zero $s \in R$ with $srx = 0$. Since R is a domain, this implies $x \in T$, so that $\bar{x} = 0$. In other words, M/T is torsion-free.

- (b) The map $M \rightarrow M/T$ is surjective, and M/T is a finitely-generated torsion-free module over R , so is projective by Corollary 29.28. By Lemma 14.28, we see there is an isomorphism ϕ of M/T into M , so that $M = \phi(M/T) \oplus T$. Hence T is a direct summand of M .

- (c) T is a finitely generated R -module since M is Noetherian; say $T = \langle t_1, \dots, t_m \rangle$. If we choose nonzero $r_i \in R$ such that $r_i t_i = 0$, then $Tr_1 \cdots r_m = 0$.

[29.13]

Suppose P/PQ is a principal ideal of R , so that $P = PQ + aR$ for some $a \in R$. Let $X = \{x \in R \mid ax \in Q\}$, which is clearly an ideal. We have

$$PX = (PQ + aR)X = PQX + aX \subset Q$$

Since Q is prime and $P \not\leq Q$, we have $X \leq Q$, and thus $PX \leq PQ$. Now let $q \in Q \leq P$ and write $q = z + ar$ with $z \in PQ$ and $r \in R$. Since $ar = q - z \in Q$ we see that $r \in X \leq Q$. Then $ar \in PQ$ so that $q = z + ar \in PQ$. We have then shown $Q \leq PQ$, so that we have equality: $Q = PQ$.

If R is a Noetherian domain, then Q is a finitely generated R -module, and from $Q = PQ$ we have by Lemma 27.11 that there exists $x \in P$ with $Q(1 - x) = 0$. Since $x \neq 1$ and R is a domain, this implies $Q = \{0\}$.

[29.14] We ignore the case R is a field, which is trivial. Let $I \leq R$ be any nonzero ideal. Then for nonzero $a \in I$, we have $R/(a)$ is a PIR, and hence $I/(a)$ is generated by a single element. This shows I is generated by at most two elements, and since I was arbitrary we've shown R is Noetherian. If $Q \leq R$ is a prime ideal that is not maximal, it is properly contained in some maximal ideal P . If PQ is non-zero, R/PQ is a PIR and the previous problem shows $Q = \{0\}$. So (0) is the only non-maximal prime ideal.

For a maximal ideal $P \leq R$, let $A = \{x \in F \mid xP \subset R\}$, where F is the fraction field of R . By definition, $PA \subset R$, and it is an ideal, since A is an R -module and P an ideal. Since $1 \in A$, we see that $P \leq PA$, so by maximality either $PA = P$ or $PA = R$. We want to show the latter always happens, so we will assume $PA = P$ and reach a contradiction. By hypothesis R/P^2 is a PIR, and we can write $P = P^2 + aR$ for some $a \in R$. We then have

$$P \geq PA = (P^2 + aR)A = P(PA) + aA$$

so that $aA \leq P$. Let $U = \{x \in R \mid xP \subset aA\}$; by Lemma 29.7, U is an ideal of R properly containing aA , and by definition $UP \leq aA$. But we now have our contradiction:

$$UP = U(P^2 + aR) = (UP)P + aU \leq a(AP) + aU \leq aR$$

and this shows $a^{-1}U \subset A$, so that $U \leq aA$, contradicting the construction of U . So we now have that $PA = R$ and hence all nonzero prime ideals of R are invertible. If R has non-invertible ideals, let I be a maximal such one, which as we've just seen cannot be prime. Let $A, B > I$ with $AB \leq I$. Then A and B are invertible, so

$$I < A = A(BB^{-1}) = (AB)B^{-1} \leq IB^{-1} \leq BB^{-1} \leq R$$

Again by maximality IB^{-1} is invertible (say with inverse C), so that $I(B^{-1}C) = R$ and I is invertible. This contradiction shows R has no non-invertible nonzero ideals. Theorem 29.6 then shows R is a Dedekind domain.

[29.15] R is a Dedekind domain, and pR is a proper ideal (since $1/p$ is not an algebraic integer), so we can write $pR = \prod P_i^{e_i}$ for $1 \leq i \leq t$. Now for any such i , $P_i \cap \mathbb{Z}$ contains p , but does not contain 1; this means $P_i \cap \mathbb{Z} = (p)$ since that is a maximal ideal of $\mathbb{Z}$. In other words, P_i lies over $(p) \leq \mathbb{Z}$. If $i \neq j$, by Theorem 28.18 there is a $\sigma \in \text{Gal}(E/\mathbb{Q})$ such that $P_i^\sigma = P_j$. Since $p^\sigma = p$ and $R^\sigma = R$ (by Lemma 28.10), we see that $P_j^{e_i}$ is also a factor of pR ; by unique factorization this shows all the e_i are equal, as desired.

Chapter 30

[30.1] Let $\mathcal{X}$ be a collection of subset of E^n whose intersection is empty. We will show for some finite subset $\mathcal{A} \subset \mathcal{X}$ the intersection is empty. This is the contrapositive of the usual closedness criterion for compactness. We will write $\mathcal{J}$ for the collection of ideals of elements of $\mathcal{X}$, letting $X_\alpha \in \mathcal{X}$ correspond to $J_\alpha \in \mathcal{J}$.

If $X := \bigcap \mathcal{X}$ is empty, then it must be (by Corollary 30.9) that the ideal $\text{Pol}(X)$ is all of $F[x_1, \dots, x_n]$, and in particular it contains 1. Let $J = \sum \mathcal{J}$. Then $\text{Zer}(J) = \bigcap \text{Zer}(\mathcal{J})$ (this is proved in Lemma 30.1), and $X_\alpha = \text{Zer}(J_\alpha)$ (this is Lemma 30.4). In other words,

$$X = \bigcap_{\alpha} X_\alpha = \bigcap_{\alpha} \text{Zer}(J_\alpha) = \text{Zer}(J)$$

Since $\sqrt{J} = \text{Pol}(X)$ by the Nullstellensatz, we see $1 \in \sqrt{J}$, implying $1 \in J$. There is then a *finite* sum of elements that equals 1, and those finite elements are sourced from finitely many $J_1, \dots, J_m \in \mathcal{J}$. If $X_1, \dots, X_m \in \mathcal{X}$ are the corresponding algebraic subsets, then

$$\bigcap_{i=1}^m X_m = \bigcap_{i=1}^m \text{Zer}(J_i) = \text{Zer}(J_1 + \dots + J_m) = \text{Zer}((1)) = \emptyset$$

And $\mathcal{A} = \{X_1, \dots, X_m\}$ is the finite subset we needed.

[30.2] Let $A \subset E^n$ be an algebraic subset; since E^n is finite, so is A . If $x_1 \in A$, let M_1 be the minimal algebraic subset of x_1 afforded by Theorem 30.15, and note $M_1 \cap A$ is algebraic containing x_1 , so by minimality, $M_1 \subset A$. Choosing $x_2 \in A \setminus M_1$, we can then construct $M_2 \subset A$, etc. Doing this finitely many times will exhaust all of A , yielding

$$A = M_1 \cup M_2 \cup \dots \cup M_m$$

If we assume A is irreducible, we must have $m = 1$ so that A is a minimal algebraic subset.

[30.3] Since R is a commutative finitely generated algebra over a field F , R is actually a quotient of $S := F[x_1, \dots, x_n]$ for some $n \geq 0$: $\theta : S \rightarrow R$. Let $P \leq S$ be a prime ideal containing $\ker(\theta)$. Then by Theorem 30.13, P is an intersection of maximal ideals, all of them necessarily containing $\ker(\theta)$. This shows that in R , all prime ideals are intersections of maximal ideals. Since $J(R)$ is the intersection of all maximal ideals and $\sqrt{(0)}$ is the intersection of prime ideals, we've shown $J(R) \leq \sqrt{(0)}$. But then every element of $J(R)$ is nilpotent, so $J(R)$ is a nil ideal.

[30.4] $E := S/M$ is a field, with canonical homomorphism $\theta : S \rightarrow E$. We have

$$F := \theta(R) \cong R/(R \cap M)$$

And $F \leq E$ is a field by hypothesis. Since $E = F[\theta(s_1), \dots, \theta(s_n)]$, Zariski's Theorem 30.8 shows E/F is algebraic, and hence a finite extension. If $R \subset T \subset S$ is a unitary subring, then

$\theta(T) \cong T/(T \cap M)$ is at least an integral domain contained in E , and containing F . $\theta(T)$ is then an integral domain that is finite dimensional over F , so by Lemma 17.1 $\theta(T)$ is a field. Since $\theta(T) \cong T/(T \cap M)$, we see $T \cap M$ is a maximal ideal of T .

[30.5] By the Nullstellensatz and Theorem 30.11, $\text{Pol}(A)$ must be a minimal nonzero prime ideal (this relies on all prime ideals being radical). Let $f \in \text{Pol}(A)$ be nonzero, and write f as $f_1 \cdots f_m$ for irreducible f_i . Since $\text{Pol}(A)$ is prime, we must have $f_i \in \text{Pol}(A)$ for some i . But then (f_i) is a prime ideal, so by minimality $\text{Pol}(A) = (f_i)$. Since $A = \text{Zer}(\text{Pol}(A))$ by Lemma 30.4, we're done.

[30.6] Let $I = (f, g) \leq F[x, y]$. We know that I has finitely many isolated primes $P_1, \dots, P_m$; assume they are all maximal. Note this implies $P_1 \cap \cdots \cap P_m = P_1 \cdots P_m$ by [26.16]. Now I is contained in infinitely many maximal ideals by hypothesis (and Corollary 30.17). If M is one of those maximal ideals not among the P_i , then $P_1 \cdots P_m \leq M$, and since M is prime, this implies $P_i \leq M$ for some i . But P_i is maximal, implying $P_i = M$. This contradiction shows not all of the P_i are maximal; let $I \leq P$ where P is a non-maximal prime ideal.

Since $F[x, y]$ has Krull dimension 2, a non-maximal non-zero prime ideal is minimal over 0. As proved in the previous problem, this implies $P = (h)$ is principal. Then from $f, g \in P$ we see h divides both f and g .

[30.7] Since $(I/IM)M = \{0\}$, we see that we can regard I/IM as an R/M -module. Since I is finitely generated as an R -module, I/IM is a finitely-generated R/M -module, hence a finite vector space over R/M . But R/M is finitely generated (as a ring) over F [note $F \cap M = \{0\}$], so by Zariski's Theorem 30.8 R/M is a finite extension over F . Putting this all together, I/IM is finite dimensional over R/M , which is finite dimensional over F , so I/IM is finite dimensional over F .

[30.8]

- (a) Let L be the field of fractions of the domain R/P . Since R/P is generated as a ring over F by the images of $x_1, \dots, x_n$ in the quotient R/P , L is generated as a field over F by these same images, so by Lemma 24.4 the transcendence degree of L over F is at most n .

Now let $\vec{x} = (\bar{x}_1, \dots, \bar{x}_n) \in L^n$. Then

$$f(\vec{x}) = f(\bar{x}_1, \dots, \bar{x}_n) = \overline{f(x_1, \dots, x_n)} = 0$$

if and only if $f \in P$, so $P = \text{Pol}(\vec{x})$.

- (b) For a prime ideal $P \leq R$, construct L as in part (a), with transcendence degree $m \leq n$ over F , and let $\bar{L}$ be the algebraic closure of L . Then there exists a subfield $K \leq L$ which is purely transcendental over F , and $\bar{L}/K$ is algebraic. Similarly, E has a subfield M with M/F purely transcendental and E/M algebraic. Since $K \cong F(y_1, \dots, y_m)$ and $M \cong F(t_1, \dots, t_r)$ with $r \geq n \geq m$, we can F -linearly embed K into M , and then Theorem 17.30 extends that embedding to an F -linear embedding of $\bar{L}$ into E . Since L

is embedded F -linearly, part (a) shows there's a point $\vec{x} \in L^n \subset E^n$ with $\text{Pol}(\vec{x}) = P$. Note F -linearity guarantees $\text{Pol}(\vec{x})$ is the same whether computed over L or E .

[30.9]

- (a) Suppose A is algebraic and $A = \text{Zer}(\text{Pol}(\vec{x}))$ for $\vec{x} \in A$. If $A = B \cup C$ for algebraic subsets $B, C \subset A$, assume $\vec{x} \in B$. Then

$$B = \text{Zer}(\text{Pol}(B)) \supset \text{Zer}(\text{Pol}(\vec{x})) = A$$

This shows A cannot be written as a union of two proper algebraic subsets, so A is irreducible.

- (b) By Theorem 30.15, we know there exists a minimal algebraic subset M containing $\vec{x}$, and we must have $M \subset A$. The reasoning in the previous part shows $A = M$. Conversely, let M be the minimal algebraic subset containing $\vec{x}$. Then M contains $\text{Zer}(\text{Pol}(\vec{x}))$, which is irreducible by Lemma 30.14 and Theorem 30.11. Minimality then implies $M = \text{Zer}(\text{Pol}(\vec{x}))$.
- (c) Assume E is infinite. We show below that $\text{Pol}(E^n) = (0)$, which is a prime ideal, so E^n is irreducible. By hypothesis, it has a generic point $\vec{x} \in E^n$. Then

$$(0) = \text{Pol}(E^n) = \text{Pol}(\text{Zer}(\text{Pol}(\vec{x}))) = \text{Pol}(\vec{x})$$

and thus $\vec{x} = (x_1, \dots, x_n)$ is a set of n elements in E algebraically independent over F . Thus the transcendence degree of E over F is at least n .

We prove $\text{Pol}(K^n) = (0)$, for any infinite field K , by induction on n . The case $n = 1$ follows from the fact a polynomial in $K[x]$ can have only finitely many roots. Assume then it's true for n , and consider $f \in K[x_1, \dots, x_n, x_{n+1}]$; assume for contradiction that f vanishes on all of K^{n+1} . If $(a_1, \dots, a_n) \in K^n$ is any point then $f(a_1, \dots, a_n, x) \in K[x]$ has infinitely many zeroes, so is the zero polynomial. Write

$$f(x_1, \dots, x_n, x_{n+1}) = \sum_{i=0}^r g_i(x_1, \dots, x_n) x_{n+1}^i \in K(x_1, \dots, x_n)[x_{n+1}]$$

We have shown that $g_i(a_1, \dots, a_n) = 0$ for all i ; since the tuple $(a_1, \dots, a_n) \in K^n$ was arbitrary, the induction hypothesis shows $g_i \equiv 0$ for all i , and hence $f \equiv 0$, as desired.

- (d) Let $A \subset E^n$ be an irreducible algebraic subset, so that $P := \text{Pol}(A)$ is a prime ideal. By part (b) of [30.8], there exists a point $\vec{x} \in E^n$ with $\text{Pol}(\vec{x}) = P$. So we have

$$A = \text{Zer}(\text{Pol}(A)) = \text{Zer}(P) = \text{Zer}(\text{Pol}(\vec{x}))$$

[30.10]

Of course $\sqrt{I} \leq \text{Pol}(\text{Zer}(I))$. We can write $\sqrt{I}$ as the finite intersection of prime ideals $P_1, \dots, P_m$. Write $P_i = \text{Pol}(A_i)$. Then from $I \leq P_i$ for each i we have

$$\text{Pol}(\text{Zer}(I)) \leq \text{Pol}(\text{Zer}(P_i)) = \text{Pol}(\text{Zer}(\text{Pol}(A_i))) = \text{Pol}(A_i) = P_i$$

Thus $\text{Pol}(\text{Zer}(I)) \leq \cap P_i = \sqrt{I}$, and so we have equality.

[30.11] Write V for A as an F -vector space, so that $\dim(V) = n$. For $x \in A$, we write $\tau_x : V \rightarrow V$ for the F -linear map $v \mapsto (v)x$, the latter product taking place in A . We will also write $B \leq \text{End}_F(V) \cong M_n(F)$ for the F -vector space of these induced F -linear maps.

By hypothesis, τ_x is singular, since there exists $y \in A$ with $yx = 0$. Thus B consists of singular matrices, and of course $\dim(B) = \dim(A) = n$. Theorem 30.19 then applies, so there exists $Z \in B$ which is a nonzero nilpotent matrix, with $Z^n = 0$. If $z \in A$ is the corresponding element of z , then this says $(y)\tau_z^n = 0$ for all y . Writing out what this means, we see

$$(\cdots ((y)z) \cdots)z = 0$$

where there are n right multiplications by z taking place.