HINTS FOR SOLUTIONS OF PROBLEMS

Chapter I

1. We are interested in odd p's such that $\left(\frac{m}{p}\right) = +1$. Factor m as $\prod_j p_j^{k_j}$. Then quadratic reciprocity gives $\left(\frac{m}{p}\right) = \prod_j \left(\frac{p_j}{p}\right)^{k_j} = \prod_{k_j \text{ odd}} \left(\frac{p_j}{p}\right) = \prod_{k_j \text{ odd}} (-1)^{\frac{1}{4}(p-1)(p_j-1)} \left(\frac{p}{p_j}\right)$. We consider $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$ separately. For $p \equiv 1 \bmod 4$, the set in question consists of those p's for which $\left(\frac{p}{p_j}\right)$ is -1 for an even number of those k_j's that are odd. This is the union over all such systems of minus signs of the intersection over j of the finitely many arithmetic progressions for which the residue $\left(\frac{p}{p_j}\right)$ equals the j^{th} sign. For a single system of minus signs, the result is an arithmetic progression of the form $k \prod_{k_j \text{ odd}} p_j + b$ by the Chinese Remainder Theorem. Each of these contains a nonempty set of primes by Dirichlet's Theorem, and hence P is nonempty.

For $p \equiv 3 \bmod 4$, if $\prod_{k_j \text{ odd}} (-1)^{\frac{1}{2}(p_j-1)}$ is $+1$, then the set in question is of the same form as above. If $\prod_{k_j \text{ odd}} (-1)^{\frac{1}{2}(p_j-1)}$ is -1, then the set in question consists of those p's for which $\left(\frac{p}{p_j}\right)$ is -1 for an odd number of those k_j's that are odd, and this again is the finite union of arithmetic progressions.

2. For (a), the proof of necessity of Theorem 1.6b remains valid when the prime p is replaced by the integer m. For (b), the first paragraph of the proof of the sufficiency of Theorem 1.6b handles matters if m is odd.

3. For $D = -56$, H has order 4, but H' has order 3 because $3x^2 \pm 2xy + 5y^2$ are improperly equivalent but not properly equivalent. A 3-element set has no group structure such that a 4-element group maps homomorphically onto it.

4. For (a), the product of any two integers representable as $ax^2 + bxy + cy^2$ is representable by the class of the square, which is the class of the inverse because the class is assumed to have order 3. The class of the inverse is the class of $(a, -b, c)$, and this represents the same integers as (a, b, c).

For (b), we seek reduced triples. These are (a, b, c) with $|b| \le a \le c$ and with $b^2 - 4ac = D = -23$, and we know that $3ac \le |D|$ and that b has the same parity as D. Hence b is odd, and the inequalities $3b^2 \le 3a^2 \le 3ac \le 23$ show that $|b| = 1$. For $|b| = 1$, we have $1 - 4ac = -23$ and $ac = 6$. Since $a \le c$, the possibilities with $|b| = 1$ are $(1, \pm 1, 6)$ and $(2, \pm 1, 3)$. Since $(1, 1, 6)$ and $(1, -1, 6)$ are properly equivalent by Proposition 1.7, $|b| = 1$ leads to just the three possibilities $(1, 1, 6)$, $(2, 1, 3)$, and $(2, -1, 3)$. Proposition 1.7 shows that these lie in distinct proper equivalence classes, and thus $h(-23) = 3$.

For (c), the general theory shows that $(1, 1, 6)$ corresponds to the identity class, and therefore the other two reduced forms are in classes of order 3.

For (d), we first track down what happens to the forms. If we write $\sim$ for proper equivalence, then we have

$$\begin{aligned}(2, 1, 3)(2, 1, 3) &\sim (2, 1, 3)(3, -1, 2) \sim (2, 5, 6)(3, 5, 4)\\ &= (6, 5, 2) \sim (2, -5, 6) \sim (2, -1, 3),\end{aligned}$$

and the last form is improperly equivalent to $(2, 1, 3)$. The next step is to interpret this chain with actual variables. If the initial variables are x_1, y_1, x_2, y_2, then the change at the first step from $(2, 1, 3)$ to $(3, -1, 2)$ comes from $x_2 = y_2'$, $y_2 = -x_2'$ while leaving x_1 and y_1 unchanged as $x_1 = x_1'$, $y_1 = y_1'$. The change at the second step from $(2, 1, 3)$ to $(2, 5, 6)$ and from $(3, -1, 2)$ to $(3, 5, 4)$ comes from the translations $x_1' = x_1'' + y_1''$, $y_1' = y_1''$, $x_2' = x_2'' + y_2''$, $y_2' = y_2''$. The multiplication step comes from Proposition 1.9 and is given by $x_3 = x_1''x_2'' - 2y_1''y_2''$ and $y_3 = 2x_1''y_2'' + 3x_2''y_1'' + 5y_1''y_2''$. And so on. The final result is that

$$(2x_1^2 + x_1y_1 + 3y_1^2)(2x_2^2 + x_2y_2 + 3y_2^2) = 2X^2 + XY + 3Y^2,$$

where $X = x_1(-x_2 + y_2) + y_1(x_2 + 2y_2)$ and $Y = y_1(x_2 - y_2) + x_1(x_2 + y_2)$.

5. The equality $\begin{pmatrix} 1 & 0 \\ -a^{-1}b & 1 \end{pmatrix}\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}\begin{pmatrix} 1 & -a^{-1}b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2a & -b \\ -b & 2c \end{pmatrix}$ shows this.

6. For reduced forms we seek (a, b, c) with $a > 0, c > 0, |b| \le a \le c$. We know that $3ac \le |D| = 67$, and D odd implies b odd. From $3b^2 \le 3a^2 \le 3ac \le 67$, we obtain $3b^2 \le 67$ and $|b| \le 4$. So $|b|$ is 1 or 3. For $|b| = 1$, $\frac{1}{4}(b^2 - D) = \frac{1}{4}(b^2 + 67) = 17$; then $17 = ac$, and $a = 1$ and $c = 17$. Since $(1, 1, 17)$ is properly equivalent to $(1, -1, 17)$ by Proposition 1.7, we obtain only one proper equivalence class from this pair. For $|b| = 3$, $\frac{1}{4}(b^2 - D) = \frac{1}{4}(9 + 67) = 19$ forces $ac = 19$ and then $a = 1$ and $c = 19$. Then $|b| \le a$ is not satisfied. So $|b| = 3$ gives no proper equivalence classes, and $h(-67) = 1$.

7. The 6 cycles are

$$\begin{aligned}&(1, 8, -15),\ (-15, 7, 2),\ (2, 7, -15),\ (-15, 8, 1);\\ &(-1, 8, 15),\ (15, 7, -2),\ (-2, 7, 15),\ (15, 8, -1);\\ &(3, 8, -5),\ (-5, 7, 6),\ (6, 5, -9),\ (-9, 4, 7),\ (7, 3, -10),\ (-10, 7, 3);\\ &(-3, 8, 5),\ (5, 7, -6),\ (-6, 5, 9),\ (9, 4, -7),\ (-7, 3, 10),\ (10, 7, -3);\\ &(5, 8, -3),\ (-3, 7, 10),\ (10, 3, -7),\ (-7, 4, 9),\ (9, 5, -6),\ (-6, 7, 5);\\ &(-5, 8, 3),\ (3, 7, -10),\ (-10, 3, 7),\ (7, 4, -9),\ (-9, 5, 6),\ (6, 7, -5).\end{aligned}$$

8. The form $(1, 1, 12)$ corresponds to the identity class, the classes of $(2, \pm 1, 6)$ are inverses of one another, and the classes of $(3, \pm 1, 4)$ are inverses of one another. The

group structure has to be cyclic, and any element other than the identity can be taken as a generator. Let us take a to be the class of $(2, 1, 6)$. We are to identify a^2. The form $(2, 1, 6)$ is aligned with itself (having the same b component), it has $j = 6/2 = 3$, and the composition formula of Proposition 1.9 leads to $(2 \cdot 2, 1, j) = (4, 1, 3)$. This is properly equivalent to $(3, -1, 4)$, and we do not have to follow through the algorithm of Theorem 1.6a to identify the product in our list. The result is that $a \leftrightarrow (2, 1, 6)$, $a^2 \leftrightarrow (3, -1, 4)$, $a^3 = (a^2)^{-1} \leftrightarrow (3, 1, 4)$, $a^4 = a^{-1} \leftrightarrow (2, -1, 6)$, and $a^5 = 1 \leftrightarrow (1, 1, 12)$.

10. For (a), the result is known for n prime by Theorem 1.2. By induction and the definition of the Jacobi symbol, it is enough to handle $n = ab$ when a and b can be handled. We have $\frac{1}{2}(n-1) = \frac{1}{2}(ab-1) = \frac{1}{2}b(a-1) + \frac{1}{2}(b-1) \equiv \frac{1}{2}(a-1) + \frac{1}{2}(b-1) \bmod 2$, the last step following because b is odd. Therefore $(-1)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(a-1)+\frac{1}{2}(b-1)} = \left(\frac{-1}{a}\right)\left(\frac{-1}{b}\right) = \left(\frac{-1}{n}\right)$, the last step following by Problem 9a.

For (b), we argue similarly, and the key computation is $\frac{1}{8}(n^2-1) = \frac{1}{8}(a^2b^2-1) = \frac{1}{8}b^2(a^2-1) + \frac{1}{8}(b^2-1) \equiv \frac{1}{8}(a^2-1) + \frac{1}{8}(b^2-1) \bmod 2$, the last step following because b^2 is odd.

11. Allowing primes to appear more than once, write factorizations of m and n as $m = \prod_{i=1}^r p_i$ and $n = \prod_{j=1}^s q_j$. Then Theorem 1.2 gives $\left(\frac{m}{n}\right) = \prod_{j=1}^s \prod_{i=1}^r \left(\frac{p_i}{q_j}\right) = \prod_{j=1}^s \prod_{i=1}^r \left(\frac{q_j}{p_i}\right)(-1)^{\frac{1}{2}(p_i-1)\frac{1}{2}(q_j-1)} = \left(\frac{n}{m}\right)(-1)^{\sum_{j=1}^s \sum_{i=1}^r \frac{1}{2}(p_i-1)\frac{1}{2}(q_j-1)}$. Since

$$\textstyle\sum_{j=1}^s \sum_{i=1}^r \frac{1}{2}(p_i-1)\frac{1}{2}(q_j-1) = \left[\sum_{j=1}^s \frac{1}{2}(q_j-1)\right]\left[\sum_{i=1}^r \frac{1}{2}(p_i-1)\right]$$

and since $\sum_{j=1}^s \frac{1}{2}(q_j-1) \equiv \frac{1}{2}(n-1) \bmod 2$ and $\sum_{i=1}^r \frac{1}{2}(p_i-1) \equiv \frac{1}{2}(m-1) \bmod 2$ by the same argument as in Problem 10a, the required formula follows.

12. For (a), choose by Dirichlet's Theorem a sufficiently large prime p that is $\equiv 3 \bmod 8$ and is in particular $\equiv 3 \bmod 4$. If 8 divides $|G|$, then the fact that $|G|$ divides $p+1$ implies that 8 divides $p+1$. So $p \equiv -1 \bmod 8$. Since p was chosen with $p \equiv 3 \bmod 8$, this is a contradiction. So 8 cannot divide $|G|$.

For (b), choose by Dirichlet's Theorem a sufficiently large prime p that is $\equiv 7 \bmod 12$ and is in particular $\equiv 3 \bmod 4$. If 3 divides $|G|$, then 3 divides $p+1$. Thus $p \equiv -1 \bmod 3$. Since also $p \equiv 3 \bmod 4$, $p \equiv 11 \bmod 12$. But p was chosen with $p \equiv 7 \bmod 12$. This is a contradiction, and 3 cannot divide $|G|$.

For (c) with an odd prime $q > 3$ given, choose by Dirichlet's Theorem a sufficiently large prime p that is $\equiv 3 \bmod 4q$ and is in particular $\equiv 3 \bmod 4$. If q divides $|G|$, then q divides $p+1$, and $p+1 \equiv 0 \bmod q$. Meanwhile, $p \equiv 3 \bmod 4q$ implies that $p+1 \equiv 4 \bmod 4q$ and $p+1 \equiv 4 \bmod q$, contradiction. So q cannot divide $|G|$.

13. For (a), choose by Dirichlet's Theorem a sufficiently large prime p that is $\equiv 5 \bmod 12$ and is in particular $\equiv 2 \bmod 3$ and $\equiv 1 \bmod 4$. If 4 divides $|G|$, then 4 divides $p+1$, which is $\equiv 2 \bmod 4$. So 4 cannot divide $|G|$.

For (b), choose by Dirichlet's Theorem a sufficiently large prime p that is $\equiv$ 2 mod 9 and is in particular $\equiv 2 \bmod 3$. If 9 divides $|G|$, then 9 divides $p+1$, which is $\equiv 3 \bmod 9$. So 9 cannot divide $|G|$.

For (c) with an odd prime $q > 3$ given, choose by Dirichlet's Theorem a sufficiently large prime p that is $\equiv 2 \bmod 3q$ and is in particular $\equiv 2 \bmod 3$. If q divides $|G|$, then q divides $p+1$, which is $\equiv 3 \bmod 3q$ and hence is $\equiv 3 \bmod q$. So q cannot divide $|G|$.

14. The integers in $\langle a, r\rangle$ are exactly the multiples of a, since such an integer n has to be of the form $n = ca + dr$ for integers c and d. This equation says that $n = ca$ and $0 = dr$, since 1 and r are linearly independent over $\mathbb{Q}$. The integer $N(s) = s\sigma(s)$ is in I because s is in I and $\sigma(s)$ is in R, and thus $N(s)$ has to be a multiple of a.

15. Write $I = \langle a, r\rangle$ with $a > 0$ an integer and r in I by Lemma 1.19b. As in the previous problem, the integer a is characterized uniquely in terms of I as the least positive integer in I. Put $r = b + g\delta$ for suitable integers b and g. Without loss of generality, we may assume that $g > 0$. Using the division algorithm and possibly replacing b by $b - na$ for some integer n, we may assume that $0 \le b < a$.

With these conventions in place, let us see that g necessarily divides a. The fact that $a\delta$ has to be in I means that $a\delta$ has an expansion $a\delta = c_1 a + c_2(b + g\delta)$ with integer coefficients. Then $a\delta = c_2 g\delta$, and g must divide a.

In particular, $0 < g \le a$ is forced. To see that b and g are uniquely determined, let $\{a, b' + g'\delta\}$ be another such $\mathbb{Z}$ basis. Since $b' + g'\delta = c_1 a + c_2(b + g\delta)$ and since symmetrically we have $b + g\delta = c_1' a + c_2'(b' + g'\delta)$, we obtain $g' = c_2 g = c_2 c_2' g'$. Therefore $|c_2| = 1$. Meanwhile, we must have

$$c_1 a + c_2 b = b' \qquad \text{and} \qquad c_2 g\delta = g'\delta.$$

The second of these equations shows that $c_2 > 0$. Thus $c_2 = 1$. Finally $c_1 a = b' - b$ with $0 \le b < a$ and $0 \le b' < a$ forces $b' - b = 0$. Therefore a, b, and g are uniquely determined.

To complete the proof, we need to see that g divides b and that ag divides $N(b+g\delta)$. Since $a\delta$ is in I, $a\delta = c_1'' a + c_2''(b + g\delta)$. Hence $c_2'' g = a$ and $c_1'' a + c_2'' b = 0$. Substituting the first of these equations into the second gives $c_1'' c_2'' g + c_2'' b = 0$. Since $c_2'' \ne 0$ from the equality $c_2'' g = a$, $c_1'' g + b = 0$. Thus g divides b.

To see that ag divides $N(b + g\delta)$, we use the fact that $g\sigma(\delta)(b + g\delta)$ is in I to write $bg\sigma(\delta) + \delta\sigma(\delta)g^2 = d_1 ag + d_2 g(b + g\delta)$ for some integers d_1 and d_2. Then $N(b + g\delta) = b^2 + bg(\delta + \sigma(\delta)) + \delta\sigma(\delta)g^2 = b^2 + bg\delta + d_1 ag + d_2 g(b + g\delta)$. Equating coefficients of δ and 1 gives

$$0 = bg + d_2 g^2 \qquad \text{and} \qquad N(b + g\delta) = b^2 + d_1 ag + d_2 bg.$$

Since $g > 0$, the first of these equations gives $d_2 = -bg^{-1}$. Substituting into the second equation gives

$$N(b + g\delta) = b^2 + d_1 ag - (bg^{-1})bg = d_1 ag,$$

and we see that ag divides $N(b + g\delta)$.

16. We are to show that $\mathbb{Z}a + \mathbb{Z}(b + g\delta)$ is closed under multiplication by arbitrary members of R. It is enough to treat multiplication by 1 and by δ. There is no problem for 1. Since $\delta + \sigma(\delta)$ is in $\mathbb{Z}$, it is enough to show that there exist integers c_1, c_2, d_1, d_2 with

$$\delta a = c_1 a + c_2(b + g\delta) \qquad \text{and} \qquad \sigma(\delta)(b + g\delta) = d_1 a + d_2(b + g\delta).$$

In view of the assumed divisibility, we can put $c_2 = ag^{-1}, c_1 = -bg^{-1}, d_2 = -bg^{-1}$, and $d_1 = N(b + g\delta)(ag)^{-1}$. Then the first equation is certainly satisfied, and the question concerning the second equation, once we have multiplied it by g, is whether we have an equality

$$g\sigma(\delta)(b + g\delta) \stackrel{?}{=} N(b + g\delta) - b^2 - bg\delta.$$

The left side is $N(b + g\delta) - b(b + g\delta)$, and thus equality indeed holds.

17. From Section 7 the relevant formula is $N(I) = |\sqrt{D}\,|^{-1}|r_1\sigma(r_2) - \sigma(r_1)r_2|$. Here we can take $r_1 = a$ and $r_2 = c + d\delta$. Substitution gives

$$\begin{aligned} N(I) &= |\sqrt{D}\,|^{-1}|a||\sigma(c + d\delta) - (c + d\delta)| \\ &= |\sqrt{D}\,|^{-1}|a||c + d\sigma(\delta) - c - d\delta| = |\sqrt{D}\,|^{-1}|ad||\sigma(\delta) - \delta|. \end{aligned}$$

The expression $|\sqrt{D}\,|^{-1}|\sigma(\delta) - \delta|$ arose in Section 7 in the computation of $N(R)$ and was shown to be 1. Thus $N(I) = |ad|$.

18. For (a), the algorithm of Section IV.9 of *Basic Algebra* shows how to align matters so as to compute the quotient of a free abelian group by a subgroup when the subgroup is given by generators. The given relationship between the generators a and $b + g\delta$ of Problem 15 with the $\mathbb{Z}$ basis of R is

$$\begin{pmatrix} a \\ b+g\delta \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & g \end{pmatrix} \begin{pmatrix} 1 \\ \delta \end{pmatrix}.$$

The procedure is to do row and column operations on the coefficient matrix to bring it into diagonal form. Since g divides b, a column operation replaces the b by 0. We obtain a diagonal matrix with diagonal entries a and g, and the quotient group is identified as $(\mathbb{Z}/a\mathbb{Z}) \oplus (\mathbb{Z}/g\mathbb{Z})$. Thus ag is identified as the number of elements in the quotient group R/I. Problem 17 identified ag as $N(I)$, and thus $N(I)$ is the number of elements in R/I.

For (b), the inclusion $I \subseteq J$ induces a quotient mapping of the finite group R/I onto R/J. As a homomorphic image of R/I, R/J must have an order that divides the order of R/I. In view of (a), $N(J)$ divides $N(I)$. The equality $I = J$ holds if and only if the quotient mapping is one-one, and this happens, because of the finite cardinalities, if and only if $N(J) = N(I)$.

19. The relevant arguments for the first three parts of this problem already appear in Chapters VIII and IX of *Basic Algebra*, and thus we can be brief. For (a), the Chinese Remainder Theorem (Theorem 8.27 of *Basic Algebra*) shows that $R/IJ \cong R/I \times R/J$, and then $N(IJ) = N(I)N(J)$ by Problem 18a. For (b), the inductive argument for $(**)$ in the proof of Theorem 9.60 of *Basic Algebra* shows that $\dim_{\mathbb{Z}/p\mathbb{Z}} R/P^e = ef$, and thus $|R/P^e| = p^{ef}$. For (c), Corollary 8.63 of *Basic Algebra* and Problem 18a above together show that $N(I) = \prod_{j=1}^n N(P_j^{k_j})$ if $I = \prod_{j=1}^n P_j^{k_j}$ is the unique factorization of the ideal I. Since $N(P_j^{k_k}) = N(P_j)^{k_j}$ by (b), $N(I) = \prod_{j=1}^n N(P_j)^{k_j}$, and (c) follows immediately.

For (d), we use Problem 15 to write $I = \langle a, b + g\delta\rangle$; then

$$I\sigma(I) = (a^2, a(b + g\delta), a(b + g\sigma(\delta)), N(b + g\delta)).$$

Each of the generators on the right side lies in the principal ideal (ag). In fact, a^2 is in (ag) because g divides a, $a(b + g\delta)$ and $a(b + g\sigma(\delta))$ are in (ag) because g divides b, and $N(b+g\delta)$ is in (ag) because ag divides $N(b+g\delta)$. Therefore $I\sigma(I) \subseteq (ag)$. Since $N(I) = ag$ by Problem 17, Problem 19c shows that $N(I\sigma(I)) = N((ag))$. Then $I\sigma(I) = (ag) = (N(I))$ by Problem 18b.

20. The only ideal I with $N(I) = 1$ is $I = R$. Problem 19c therefore shows that a nontrivial factorization of $(p)R$ leads to a nontrivial factorization of its norm, which is p^2. This factorization must be $p^2 = p \cdot p$, and thus I factors nontrivially at most into two factors, each with norm p.

21. For (a), we use Problem 15 to write a nontrivial factor I of $(2)R$ as $I = \langle a, b + g\delta\rangle$. Problem 17 shows that $2 = N(I) = ag$ with g dividing a. Therefore $a = 2$ and $g = 1$. So the only possible factors are of the form $I = \langle 2, b + \delta\rangle$ with $0 \le b < a = 2$. Thus $b = 0$ or $b = 1$. When D is odd, we have $\mathrm{Tr}(\delta) = 1$ and $N(\delta) = \frac{1}{4}(1 - m)$. Then $N(b + \delta) = b^2 + b\,\mathrm{Tr}(\delta) + N(\delta) = b^2 + b + \frac{1}{4}(1 - m) \equiv \frac{1}{4}(1 - m) \bmod 2$. If $m \equiv 5 \bmod 8$, then we see that 2 does not divide $N(b + \delta)$, and thus $(2)R$ cannot have a nontrivial factor.

For (b), we again have $N(b + \delta) = b^2 + b\,\mathrm{Tr}(\delta) + N(\delta) = b^2 + b + \frac{1}{4}(1 - m) \equiv \frac{1}{4}(1 - m) \bmod 2$, and the condition $m \equiv 1 \bmod 8$ makes the right side 0. Thus 2 divides $N(b+\delta)$, and $\langle 2, \delta\rangle$ and $\langle 2, 1+\delta\rangle$ are both ideals by Problem 16. The product of these ideals is $\langle 2, \delta\rangle\langle 2, 1 + \delta\rangle = (4, 2\delta, 2(1 + \delta), \delta^2)$ and contains $(2)R$ because $2 = 2(1 + \delta) - 2\delta$. Moreover, the product has norm 4 by Problems 17 and 19c, and this matches the norm of $(2)R$. Thus Problem 18b shows that $\langle 2, \delta\rangle\langle 2, 1+\delta\rangle = (2)R$.

For (c) and (d), $\delta = -\sqrt{m}$. Thus $N(b + \delta) = b^2 + b\,\mathrm{Tr}(\delta) + N(\delta) = b^2 - m = b - \frac{1}{4}D$. If $D/4 \equiv 3 \bmod 4$, then $b - \frac{1}{4}D$ is divisible by 2 for $b = 1$. If $D/4 \equiv 2 \bmod 4$, then $b - \frac{1}{4}D$ is divisible by 2 for $b = 0$. With b taking on the appropriate value in the two cases, $\langle 2, b + \delta\rangle$ is an ideal by Problem 16. The square of this ideal is $(4, 2(b + \delta), (b - \sqrt{m}\,)^2) = (4, 2(b + \delta), b^2 + m - 2m\sqrt{b}\,)$. The definition of b makes $b^2 + m$ even in every case, and hence $\langle 2, b + \delta\rangle^2 \supseteq (2)R$. Since the norms of the ideals on the two sides are both 4, the two ideals must be equal.

22. Arguing as in the previous problem, we see that any nontrivial factor of $(p)R$ must have norm p and therefore must be given by $\langle p, x+\delta\rangle$ for some x such that p divides $N(x+\delta) = x^2 + x\,\mathrm{Tr}(\delta) + N(\delta)$.

For (a), $\mathrm{Tr}(\delta) = 1$ and $N(\delta) = \frac{1}{4}(1-m) = \frac{1}{4}(1-D)$, and the condition is that p divide $x^2 + x + \frac{1}{4}(1-D)$. This means that $x^2 + x + \frac{1}{4}(1-D) \equiv 0 \bmod p$ is to have a solution. When this happens, Problem 16 ensures that $\langle p, x+\delta\rangle$ is an ideal. Then $\langle p, x+\sigma(\delta)\rangle$ is an ideal as well, and the product of the two is $(p^2, p(x+\delta), p(x+\sigma(\delta)), N(x+\delta))$. Since p divides $N(x+\delta)$, this product ideal is contained in $(p)R$. The product ideal and $(p)R$ both have norm p^2, and therefore they are equal.

For (b), $\mathrm{Tr}(\delta) = 0$ and $N(\delta) = -m = -D/4$, and the condition is that p divide $x^2 - D/4$. This means that $x^2 - D/4 \equiv 0 \bmod p$ is to have a solution. When this happens, Problem 16 ensures that $\langle p, x+\delta\rangle$ is an ideal. Then $\langle p, x+\sigma(\delta)\rangle$ is an ideal as well, and the product of the two is $(p^2, p(x+\delta), p(x+\sigma(\delta)), N(x+\delta))$. Since p divides $N(x+\delta)$, this product ideal is contained in $(p)R$. The product ideal and $(p)R$ both have norm p^2, and therefore they are equal.

For (c), the respective conditions for factorization in (a) and (b) are that $x^2 + x + \frac{1}{4}(1-D) \equiv 0 \bmod p$ and $x^2 - D/4 \equiv 0 \bmod p$ be solvable. In both cases the quadratic expression on the left side has discriminant D. Hence factorization occurs if and only if D is a square modulo p.

23. In both cases we are assuming that $(p)R$ has a factor $I = \langle p, x+\delta\rangle$ with $0 \le x < p$. Using Problem 15, let us write $\sigma(I) = \langle p, x+\sigma(\delta)\rangle = \langle p, y+\delta\rangle$ with $0 \le y < p$. Choose integers c and d with $x + \sigma(\delta) = cp + d(y+\delta)$. Since $\sigma(\delta) = \mathrm{Tr}(\delta) - \delta$, the equation is $x + \mathrm{Tr}(\delta) - \delta = cp + dy + d\delta$, and we obtain $x + \mathrm{Tr}(\delta) = cp + dy$ and $-\delta = d\delta$. Thus $d = -1$, $x + \mathrm{Tr}(\delta) = cp - y$, and $cp = x + y + \mathrm{Tr}(\delta)$. From $0 \le x < p$ and $0 \le y < p$, we have $0 \le x + y + \mathrm{Tr}(\delta) \le 2(p-1) + \mathrm{Tr}(\delta) \le 2p - 1$. So c in the equation $cp = x + y + \mathrm{Tr}(\delta)$ has to be 1 or 0, and the equation is $x + y = p - \mathrm{Tr}(\delta)$ or $x + y = -\mathrm{Tr}(\delta)$. The condition that $\sigma(I) = I$ is the condition that $x = y$, hence that $2x = p - \mathrm{Tr}(\delta)$ or $2x = -\mathrm{Tr}(\delta)$. When D is odd, this says that $x = \frac{1}{2}(p-1)$; when D is even, it says that $x = 0$.

24. Since $\sigma(\langle p, x+\delta\rangle) = \langle p, x+\sigma(\delta)\rangle$, the two factors are the same if and only if $\sigma(I) = I$. Problem 23 says that the latter equality holds for D odd if and only if $x = \frac{1}{2}(p-1)$ and that it holds for D even if and only if $x = 0$. In the two cases we know from Problem 14 that p divides $N(x+\delta) = x^2 + x\,\mathrm{Tr}(\delta) + N(\delta)$.

When D is odd, this result says that p divides $x^2 + x + \frac{1}{4}(1-D)$, hence that it divides $4x^2 + 4x + (1-D) = (2x+1)^2 - D$. Then p divides D if and only if p divides $2x+1$, if and only if $x = \frac{1}{2}(p-1)$.

When D is even, we know from Problem 14 that p divides $x^2 - m$. Hence p divides $4(x^2 - m) = 4x^2 - D = (2x)^2 - D$. Then p divides D if and only if p divides $2x$, if and only if $x = 0$.

25. Theorem 1.14 shows that the genus group G is the quotient of the abelian group H modulo its subgroup of squares. The subgroup of squares consists of the elements

in the product of the cyclic subgroups of orders $2^{k_1-1}, \dots, 2^{k_r-1}, q_1^{l_1}, \dots, q_s^{l_s}$, and the quotient is the product of r copies of a cyclic group of order 2. Thus G has order 2^r. The subgroup of elements of H whose order divides 2 is the product of the 2-element subgroups of the cyclic groups of orders $2^{k_1}, \dots, 2^{k_r}$. It is a product of r copies of a cyclic group of order 2 and hence is abstractly isomorphic to G.

26. If P is a nonzero prime ideal, then so is $\sigma(P)$. Since $\sigma^2 = 1$, the mapping $P \mapsto \sigma(P)$ is a permutation of order 2 on the nonzero prime ideals. Evidently the prime ideals of type (i) above are permuted in 2-cycles, and the prime ideals of types (ii) and (iii) are left fixed.

If a nonzero ideal I has prime factorization $I = \prod_i P_i^{k_i}$, then $\sigma(I) = \prod_i \sigma(P_i)^{k_i}$. When $\sigma(I) = I$, we can match the factors and their exponents. We conclude that the factorization of I is as

$$I = \Big(\prod_{\substack{\text{pairs } (P_i, \sigma(P_i)) \\ \text{of type (i)}}} (P_i \sigma(P_i))^{k_i} \Big) \Big(\prod_{\substack{\text{ideals } P_i \\ \text{of type (ii)}}} P_i^{k_i} \Big) \Big(\prod_{\substack{\text{ideals } P_i \\ \text{of type (iii)}}} P_i^{k_i} \Big).$$

Each factor in the first product is of the form $(N(P_i))^{k_i}$ by Problem 19d, each factor in the second product is of the form $(p)^{k_i}$ for some prime p not dividing D, and each P_i^2 contributing to the third factor is of the form (p) for some prime p dividing D. The result follows.

27. For (a), the only nontrivial step in the displayed formula is the third equality, which follows because $x\sigma(x) = N(x) = 1$ by hypothesis. If we take $y = (1+x)^{-1}$, then the displayed formula gives $x = (1+x)(1+\sigma(x))^{-1} = y^{-1}\sigma(y)$ as required.

For (b), the equality $\sigma(y)y^{-1} = x$ remains valid when y is replaced by ny with $n \in \mathbb{Z}$, and thus we may take y to be in R. Now let y and z be in R with $\sigma(z)z^{-1} = x = \sigma(y)y^{-1}$. Then $\sigma(zy^{-1}) = zy^{-1}$, and zy^{-1} is in $\mathbb{Q}$. Among all $y \in R$ with $\sigma(y)y^{-1} = x$, let y_0 be one with $|N(y)|$ as small as possible; y_0 exists because $|N(y)|$ is an integer in each case. If $\sigma(z)z^{-1} = x$, write $z = u + v\delta$, $y_0 = a + b\delta$, and $zy_0^{-1} = p/q$ with $\mathrm{GCD}(p, q) = 1$. Then $qu + qv\delta = qz = py_0 = pa + pb\delta$, and we obtain $qu = pa$ and $qv = pb$. Therefore q divides a and b, and $q^{-1}y_0 = q^{-1}a + q^{-1}b\delta$ is in R. Then $y = q^{-1}y_0$ is another element in R with $\sigma(y)y^{-1} = x$, and it contradicts the minimal choice of $|N(y_0)|$ unless $|q| = 1$. We conclude that $z = \pm py_0$.

28. In (a), $N(I^2) = N((x))$ says that $N(I)^2 = |N(x)|N(R) = |N(x)|$. Therefore $N(x^{-1}N(I)) = |N(x)|^{-1}N((N(I)) = |N(x)|^{-1}N(I)^2 = 1$, and $xN(I)^{-1}$ has norm 1.

In (b), Problem 27b gives us $y_0 \in R$ with $\sigma(y_0)y_0^{-1} = xN(I)^{-1}$. Then we compute that $\sigma((y_0)I) = \sigma(y_0)\sigma(I) = y_0xN(I)^{-1}\sigma(I) = y_0N(I)^{-1}(x)\sigma(I) = y_0N(I)^{-1}I^2\sigma(I) = y_0N(I)^{-1}((N(I))I = y_0I$.

For (c), suppose $N(y_0) > 0$. Then Problem 26a shows that $(y_0)I = (a)J_S$ for some $a \in \mathbb{Z}$, and this gives the required strict equivalence. If $N(y_0) < 0$, then $N(y_0\sqrt{m}) > 0$, and $\sigma((y_0\sqrt{m})I) = (y_0\sqrt{m})I$; Problem 26a shows that $(y_0\sqrt{m})I = (a)J_S$ for some $a \in \mathbb{Z}$, and this gives the required strict equivalence.

29. For (a), since $m < 0$ and m is neither -1 nor -3, the possible units are $\varepsilon = \pm 1$. The equality $\sigma(x) = \varepsilon x$ says that x is in $\mathbb{Z}$ if $\varepsilon = +1$, and it says that x is in $\mathbb{Z}\sqrt{m}$ if $\varepsilon = -1$.

For (b), when $m = -1$ or $m = -3$, we have $D = -4$ or $D = -3$; thus $g = 0$, and there is nothing to prove. For other values of $m < 0$, consider J_S. Then $N(J_S) = \prod_{p \in S} p$, and this is some divisor D' of D with no repeated factors. Let us write $J_S = \langle a, b + g\delta \rangle$ by Problem 15. Then $ag = D'$ and g divides a. Since D' is square free, $a = D'$ and $g = 1$. If J_S is principal, then (a) shows that $J_S = (c)$ for an integer c or $J_S = (d\sqrt{m})$ for an integer d.

Suppose $J_S = (c)$. Then $b + \delta = rc$ for some $r \in R$. Write $r = x + y\delta$ for integers x and y. Then $b + \delta = cx + cy\delta$ shows that $1 = cy$ and hence that c divides 1. Thus $J_S = R$, and the set S is empty.

Suppose $J_S = (d\sqrt{m})$. Then $b + \delta = dx\sqrt{m} + dy\delta\sqrt{m}$ for some integers x and y. If D is odd, then the equation reads $b + \frac{1}{2}(1 - \sqrt{m}) = dx\sqrt{m} + dy\frac{1}{2}(1 - \sqrt{m})\sqrt{m}$. This implies that $-\frac{1}{2}\sqrt{m} = d(x + \frac{1}{2}dy)\sqrt{m}$, hence that $-1 = d(2x + 1)$. Therefore $d = 1$, $J_S = (\sqrt{m}) = (\sqrt{D})$, $N(J_S) = |D|$, and $S = E$. If D is even, then the equation reads $b - \sqrt{m} = dx\sqrt{m} - dym$, and we obtain $-1 = dx$. So $d = 1$, $J_S = (\sqrt{m})$, $N(J_S) = m = D/4 = D'$. This is the product of all prime divisors of D if $D/4 \equiv 2 \bmod 4$ and all of them but 2 if $D/4 \equiv 3 \bmod 4$.

For (c), let E' be a subset of g members of E, and assume that the element of E that is not in E' is not 2 unless $D = -4$. If S and S' are two subsets of E', then $J_S J_{S'} = (n)J_T$, where $n = \prod_{p \in S \cap S'} p$ and $T = (S - S') \cup (S' - S)$. If J_S and $J_{S'}$ represent the same genera, then $J_S J_{S'}$ is principal, and J_T must be principal. The set T can be empty only if $S = S'$, and it has to be a subset of E' and thus cannot be all of E. According to (b), the only way that J_T can be principal is thus that $S = S'$ or that all of the conditions D even, $D/4 \equiv 2 \bmod 4$, and $T = E' = E - \{2\}$ are satisfied. In the latter case the construction of E' shows that $D = -4$, T is empty, and $S = S'$. Thus the ideals J_S for $S \subseteq E'$ represent distinct genera in every case.

For (d), the roots of unity are $\pm\varepsilon_1^k$. Since $N(\varepsilon_1) = -1$, the roots of unity of norm 1 are the $\pm\varepsilon_1^{2n}$. So suppose that $\varepsilon = \pm\varepsilon_1^{2n}$. Put $\varepsilon_0 = \varepsilon_1^n$. Then $\varepsilon_0\sigma(\varepsilon_0) = N(\varepsilon_0) = (-1)^n$, and $\sigma(\varepsilon_1^n x) = \sigma(\varepsilon_0)\sigma(x) = \sigma(\varepsilon_0)\varepsilon x = (-1)^n\varepsilon_0^{-1}\varepsilon x = \pm(-1)^n\varepsilon_1^{-n}\varepsilon_1^{2n}x = \pm(-1)^n\varepsilon_1^n x = s\varepsilon_1^n x$ with $s = \pm(-1)^n$. If $s = +1$, then $\varepsilon_1^n x$ is in $\mathbb{Z}$, while if $s = -1$, then $\varepsilon_1^n x$ is in $\mathbb{Z}\sqrt{m}$. Then the same steps as in (b) and (c) finish the argument.

For (e), the four mentioned ideals are principal, and we have $(1) = J_S$ for S empty and $(\sqrt{m}) = J_S$ for S equal to the set of prime divisors of m. For these two ideals, $N(1) > 0$ and $N(\sqrt{m}) < 0$. Consider (y_0^+) and (y_0^-). The ideal (y_0^+) has $\sigma((y_0^+)) = (\sigma(y_0^+)) = (y_0^+\varepsilon_1) = (y_0^+)$, and hence it is of the form $(n)J_S$ for some S. Then $y_0^+ = nr$ for some $r \in R$, and it follows that $n^{-1}y_0^+$ is in R. This contradicts the minimality of $|N(y_0^+)|$ unless $|n| = 1$. Hence $(y_0^+) = J_S$ for some S. Similarly $(y_0^-) = J_S$ for some S. Thus all four principal ideals are of the form J_S.

Let us see that the four principal ideals are distinct. Neither ideal (y_0^+) nor (y_0^-) can equal (1). In fact, if (y_0^+) were to equal (1), then y_0^+ would be a unit ε, and we

would have $\varepsilon_1 = \sigma(y_0^+)(y_0^+)^{-1} = \sigma(\varepsilon)\varepsilon^{-1} = \varepsilon^{-2}$, in contradiction to the fact that ε_1 is fundamental. Similarly (y_0^-) cannot equal (1).

Since $\sigma(y_0^+\sqrt{m})(y_0^+\sqrt{m})^{-1} = -\sigma(y_0^+)\sqrt{m}\,(y_0^+)^{-1}(\sqrt{m})^{-1} = -\sigma(y_0^+)(y_0^+)^{-1}$ $= -\varepsilon_1$, the definition of y_0^- shows that $y_0^+\sqrt{m} = ny_0^-$ for some integer n. Passing to norms gives $-mN(y_0^+) = n^2N(y_0^-)$. Therefore $N(y_0^+)$ and $N(y_0^-)$ have opposite sign.

We have seen that two of the four elements 1, y_0^+, y_0^-, $\sqrt{m}$ have positive norm, two have negative norm, and the two of positive norm generate distinct principal ideals. To see that the two of negative norm generate distinct ideals, we consider separately the cases $N(y_0^-) < 0$ and $N(y_0^+) < 0$. If $N(y_0^-) < 0$, we use the equation $-mN(y_0^+) = n^2N(y_0^-)$ proved in the previous paragraph. If $(y_0^-) = (\sqrt{m})$, then cancellation gives $N(y_0^+) = +1$; then y_0^+ is a unit, and we have seen that it cannot be. If $N(y_0^+) < 0$, we use the definition of y_0^+ in the same way as in the previous paragraph to obtain $-mN(y_0^-) = n^2N(y_0^+)$ for some integer n. Cancellation shows that $N(y_0^-) = +1$; then y_0^- is a unit, and we have seen that it cannot be. Thus the four principal ideals are distinct.

Now suppose that (x) is any principal ideal fixed by σ. As in the statement of the problem, we have $\sigma(x) = \varepsilon x$ for some unit ε. The most general unit is of the form $\varepsilon = \pm\varepsilon_1^n$. We shall produce constructively the element of Problem 27 corresponding to ε. Put $y_{0,n} = \varepsilon_1^{n/2}$ if n is even and $y_{0,n} = \varepsilon_1^{(n+1)/2}y_0$ if n is odd. For n even we have

$$\sigma(y_{0,n}x) = \sigma(y_{0,n})\varepsilon x = \pm\sigma(\varepsilon_1^{n/2})\varepsilon_1^n x = \pm\varepsilon_1^{-n/2}\varepsilon_1^n x = \pm y_{0,n}x,$$

and for n odd we have

$$\begin{aligned}\sigma(y_{0,n}x) = \sigma(y_{0,n})\varepsilon x &= \pm\sigma(\varepsilon_1^{(n+1)/2}y_0)\varepsilon_1^n x = \pm\varepsilon_1^{-(n+1)/2}\sigma(y_0)\varepsilon_1^n x \\ &= \pm\varepsilon_1^{(n-1)/2}\sigma(y_0)x = \pm\varepsilon_1^{(n-1)/2}y_0\varepsilon_1 x = \pm y_{0,n}x.\end{aligned}$$

Thus $\sigma(y_{0,n}x) = \pm y_{0,n}x$ for all n. Therefore $y_{0,n}x$ is in $\mathbb{Z}$ or in $\mathbb{Z}\sqrt{m}$, depending on the sign $\pm$. Depending on the sign, $|N(y_{0,n}x)| = |N(y_{0,n})||N(x)|$ thus is either the square of an integer or m times the square of an integer. If n is even, then $|N(y_{0,n})| = 1$, and $|N(x)|$ is therefore either the square of an integer or m times the square of an integer. Since $|N(x)|$ is the value of the norm of (x), there are only two possible S's for which this can happen. If n is odd, then $|N(y_{0,n})| = a$ for a certain square-free integer > 1, as we have seen. Therefore $|N(x)|$ has to be either a^{-1} times the square of an integer or ma^{-1} times the square of an integer. So there are only two possible S's in this case. Thus there are only four possible S's in all cases, and these have been accounted for. So the number of principal ideals among the J_S's is exactly four. To complete the proof, we now argue as in (c) but consider only possibilities for which the product of two J_S's is n^2 times one of the two J_S's given by a principal ideal with a generator of positive norm.

30. Since D is fundamental, (a_1, b_1, c_1) is automatically primitive. Then Lemma 1.10 produces a properly equivalent form that represents some integer a relatively prime to D. The rest follows from the argument in the second paragraph of the proof of sufficiency in Theorem 6b.

31. For (a), choose an integer r such that $b + 2ar = kD$ for some integer k; this is possible because $\mathrm{GCD}(D, 2a) = 1$. Then the translation $x = x' + ry'$, $y = y'$ leads from $ax^2+bxy+cy^2$ to $ax'^2+kDx'y'+c'y'^2$ for some c'. The discriminant of the new form is still $D = k^2D^2 - 4ac'$, and thus $4ac' \equiv 0 \bmod D$. Since $\mathrm{GCD}(4a, D) = 1$, $c' \equiv 0 \bmod D$.

For (b), b has to be even because $D = b^2 - 4ac$ is even. Write $b = 2\bar{b}$. Choose an integer s such that $\bar{b} + as = kD$ for some k; this is possible because $\mathrm{GCD}(a, D) = 1$. Then the translation $x = x' + sy'$, $y = y'$ leads from $ax^2 + bxy + cy^2$ to $ax'^2 + 2kDx'y' + c'y'^2$ for some c'. The discriminant of the new form is $D = 4k^2D^2 - 4ac'$, where $c' = (4a)^{-1}D(4k^2D - 1) = a^{-1}(D/4)(4k^2D - 1)$. Modulo D, this expression is $-\bar{a}(D/4)$, where $\bar{a}$ is an integer with $\bar{a}a \equiv 1 \bmod D$. Here a is odd, and hence $a^2 \equiv 1 \bmod 8$. If 2^u is the exact power of 2 dividing D, then $\bar{a}a \equiv 1 \bmod 2^u$, and hence $\bar{a} \equiv a \bmod 2^u$. If p is any odd prime dividing D, then p divides $D/4$, and hence $\bar{a}(D/4) \equiv 0 \equiv a(D/4) \bmod p$. Therefore $\bar{a}(D/4) \equiv a(D/4) \bmod D$, and we conclude that $c' \equiv -a(D/4) \bmod D$.

32. For (a), clearing fractions in the expression $ax^2 + kDxy + lDy^2 = r$ yields $au^2+kDuv+lDv^2 = rw^2$. Suppose a prime p divides $\mathrm{GCD}(w, D)$. Then p divides au^2. Since $\mathrm{GCD}(a, D) = 1$, p divides u. Referring back to the equation, we see that p^2 divides au^2 and $kDuv$, hence divides lDv^2. Thus p divides lv^2. The discriminant is $D = k^2D^2 - 4alD$, and divisibility of l by p would force p^2 to divide the left side D. Hence p does not divide l, and p must divide v. Then p divides both u and v, in contradiction to the minimality of the common denominator w. We conclude that $\mathrm{GCD}(w, D) = 1$. Taking the equation $au^2 + kDuv + lDv^2 = rw^2$ modulo D gives $au^2 \equiv rw^2 \bmod D$. Since r and w are relatively prime to D, so is u. Thus we can rewrite this congruence as $a \equiv d^2r \bmod D$ for some integer d relatively prime to D.

For (b), the same argument gives $a' \equiv d'^2r \bmod D$. Since d is relatively prime to D, we can rewrite the congruence for a as $r \equiv d^{-2}a \bmod D$, and then $a' \equiv d'^2r \equiv (d^{-1}d')^2a \bmod D$.

For (c), the given forms are properly equivalent over $\mathbb{Z}$ to (a, kD, lD) and to $(a', k'D, l'D)$, respectively, by Problem 31a. Proper equivalence over $\mathbb{Q}$ means that the two forms take on the same rational values, one of which is the integer a'. Part (b) therefore shows that $a' = as^2 + nD$ for some integers s and n, necessarily with $\mathrm{GCD}(s, D) = 1$. Modulo D, the forms are given by ax^2 and $a'x'^2$, and the first can be transformed into the second by the substitution $x = sx'$, $y = s^{-1}y'$, where s^{-1} is the multiplicative inverse of s in $\mathbb{Z}/D\mathbb{Z}$. In fact, substitution into ax^2 gives $a(sx')^2 = (as^2)x'^2 \equiv a'x'^2 \bmod D$. This substitution is given by the matrix $\begin{pmatrix} s & 0 \\ 0 & s^{-1} \end{pmatrix}$ in $\mathrm{SL}(2, \mathbb{Z}/D\mathbb{Z})$.

33. Part (a) is almost the same as Problem 32a. Clearing fractions leads to

$au^2 + kDuv + (lD - a(D/4))v^2 = rw^2$, and the argument that no odd prime p divides GCD(w, D) is the same. Suppose that 2 divides w. The equation modulo 4 is then $au^2 - a(D/4)v^2 \equiv 0 \bmod 4$ with $D/4$ congruent to 2 or 3 modulo 4. Since 2 divides w, at least one of u and v must be odd. If $D/4 \equiv 3 \bmod 4$, the congruence becomes $a(u^2 + v^2) \equiv 0 \bmod 4$, which is impossible with at least one of u and v odd. If $D/4 \equiv 2 \bmod 4$, the congruence becomes $a(u^2 + 2v^2) \equiv 0 \bmod 4$, which again is impossible with at least one of u and v odd. Thus GCD$(w, D) = 1$. Taking the equation modulo D and using the invertibility of r and w modulo D, we have $ar^{-1}w^{-2}(u^2 - (D/4)v^2) \equiv 1 \bmod D$.

For (b), let p be an odd prime divisor of D. The above congruence then becomes $ar^{-1}w^{-2}u^2 \equiv 1 \bmod p$. Similarly with the second form, there is some w' prime to D such that $a'r^{-1}w'^{-2}u'^2 \equiv 1 \bmod p$. Comparing the two expressions, we see that a modulo p is the product of a' and an invertible square.

For (c), the above congruence becomes $ar^{-1}w^{-2}(u^2+v^2) \equiv 1 \bmod 4$. This forces $u^2 + v^2 \equiv 1 \bmod 4$. Since w has to be odd, $w^2 \equiv 1 \bmod 4$. Hence $ar^{-1} \equiv 1 \bmod 4$. Similarly $a'r^{-1} \equiv 1 \bmod 4$, and therefore $a \equiv a' \bmod 4$.

For (d), the above congruence becomes $ar^{-1}(u^2 - (D/4)v^2) \equiv 1 \bmod 8$, since w is odd. If $D/4 \equiv 2 \bmod 8$, we obtain $ar^{-1}(u^2 - 2v^2) \equiv 1 \bmod 8$. Here u has to be odd, and thus $ar^{-1}(1 - 2v^2) \equiv 1 \bmod 8$. If v is even, this says that $a \equiv r \bmod 8$; if v is odd, it says that $a \equiv -r \bmod 8$. Putting this conclusion together with a similar conclusion about the second form, we obtain $a' \equiv \pm a \bmod 8$.

If $D/4 \equiv 6 \bmod 8$, we obtain $ar^{-1}(u^2 + 2v^2) \equiv 1 \bmod 8$. Here u has to be odd, and thus $ar^{-1}(1 + 2v^2) \equiv 1 \bmod 8$. If v is even, this says that $a \equiv r \bmod 8$; if v is odd, it says that $a \equiv 3r \bmod 8$. Putting this conclusion together with a similar conclusion about the second form, we obtain $a' \equiv a \bmod 8$ or $a' \equiv 3a \bmod 8$.

For (e), we shall assemble a member of SL$(2, \mathbb{Z}/D\mathbb{Z})$ one prime at a time and use the Chinese Remainder Theorem. For odd primes p dividing D, choose s_p with $a' \equiv s_p^2 a \bmod p$, and introduce the matrix $M_p = \left(\begin{smallmatrix} s_p & 0 \\ 0 & s_p^{-1} \end{smallmatrix}\right)$ in SL$(2, \mathbb{Z}/p\mathbb{Z})$. If $D/4 \equiv 3 \bmod 4$, introduce the matrix $M_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in SL$(2, \mathbb{Z}/4\mathbb{Z})$. If $D/4 \equiv 2 \bmod 4$, let $M_2 = \left(\begin{smallmatrix} 1 & 6 \\ 1 & 7 \end{smallmatrix}\right)$ in SL$(2, \mathbb{Z}/8\mathbb{Z})$ if $D/4 \equiv 6 \bmod 8$, and let $M_2 = \left(\begin{smallmatrix} 1 & 2 \\ 1 & 3 \end{smallmatrix}\right)$ in SL$(2, \mathbb{Z}/8\mathbb{Z})$ if $D/4 \equiv 2 \bmod 8$. The Chinese Remainder Theorem produces a unique matrix with entries in $\mathbb{Z}/D\mathbb{Z}$ that is congruent to M_p modulo each odd prime divisor of D and is congruent to M_2 modulo the power of 2 dividing D. Call this matrix $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. It has determinant 1 modulo D and hence lies in SL$(2, \mathbb{Z}/D\mathbb{Z})$. Then substitution of $x = \alpha x' + \beta y'$ and $y = \gamma x' + \delta y'$ into the form $a(x^2 - (D/4)y^2)$ modulo D leads to the form $a'(x^2 - (D/4)y^2)$ modulo D.

34. These problems establish a function from the set of equivalence classes of binary quadratic forms over $\mathbb{Z}$ with discriminant D, the equivalence relation being proper equivalence over $\mathbb{Q}$, *onto* the set of equivalence classes of binary quadratic forms over $\mathbb{Z}$ with discriminant D, the equivalence relation being proper equivalence

over $\mathbb{Z}/D\mathbb{Z}$. The number of elements in the domain has to be $\geq$ the number of elements in the range.

35. The steps in solving Problems 32 and 33 involve relating a to r modulo each prime power dividing D. These relationships are the same as the relationships between a and r' if the form modulo D represents r' and $\mathrm{GCD}(r', D) = 1$, and the relationships are transitive. Thus the genus characters take the same values at r as they do at r', and they take the same values at a as well.

36. Multiplication is the operation on proper equivalence classes of forms that corresponds to composition of aligned representatives of the classes, and composition is defined in such a way that the set of values of the composition is the set of products of a value of one form by a value of the other. The values are unaffected by proper equivalence over $\mathbb{Z}$.

37. For (a), $D/4$ has an odd number $2t + 1$ of prime factors $4k + 3$. Use of the Jacobi symbol with a odd and p varying over the prime divisors of $D/4$ gives

$$\prod_p \left(\tfrac{a}{p}\right) = \prod_{p=4k+1} \left(\tfrac{a}{p}\right) \prod_{p=4k+3} \left(\tfrac{a}{p}\right) = \xi(a)^{2t+1} \prod_{p=4k+1} \left(\tfrac{p}{a}\right) \prod_{p=4k+3} \left(\tfrac{p}{a}\right) = \xi(a)\left(\tfrac{D/4}{a}\right).$$

Therefore

$$\xi(a) \prod_p \left(\tfrac{a}{p}\right) = \left(\tfrac{D/4}{a}\right) = \left(\tfrac{2}{a}\right)^2 \left(\tfrac{D/4}{a}\right) = \left(\tfrac{D}{a}\right).$$

For (b) and (c), say that the number of prime factors $4k + 3$ of $D/8$ is t. With p varying over the odd prime divisors of D, the same computation as above gives $\prod_p \left(\tfrac{a}{p}\right) = \xi(a)^t \left(\tfrac{D/8}{a}\right)$. Then $\left(\tfrac{D}{a}\right) = \left(\tfrac{2}{a}\right)\left(\tfrac{D/8}{a}\right) = \eta(a)\xi(a)^t \prod_p \left(\tfrac{a}{p}\right)$. One easily checks that t is even if $D/4 \equiv 2 \bmod 8$ and is odd if $D/4 \equiv 6 \bmod 8$, and the result follows.

38. For each odd prime divisor p of D, choose a residue r_p modulo p such that $\left(\tfrac{r_p}{p}\right) = s_p$. If D is even, choose an odd residue r_2 modulo 8 such that $\alpha(r_2) = s_2$. The Chinese Remainder Theorem produces an integer b prime to D such that $b \equiv r_p \bmod p$ for the odd p's and $b \equiv r_2 \bmod 8$. For this integer b and every $k \geq 0$, we have $\left(\tfrac{b+kD}{p}\right) = r_p$ for each odd p and $\alpha(b + kD) = s_2$. Dirichlet's Theorem says that $b + kD$ is a prime q for a suitable choice of k, and this prime q has the required properties.

39. Problem 37 showed that the product of the genus characters for an odd integer a such that $\mathrm{GCD}(a, D) = 1$ is $\left(\tfrac{D}{a}\right)$. Using the genus characters at $a = q$, we see that $\left(\tfrac{D}{q}\right) = 1$. Theorem 1.6b shows that q is primitively representable by some form (q, b, c) of discriminant D. The values of the genus characters for this form are their values on q, and we have arranged that these values are the various numbers s_p. Since there are $g + 1$ genus characters and the first g of them can be specified arbitrarily and still give a similarity class modulo D, there are at least 2^g similarity classes modulo D.

40. Problem 29 shows that the number of classes of type (i) is exactly 2^g. Problems 30–33 show that equivalence of type (i) implies equivalence of type (ii), and they therefore give a mapping of the set of classes of type (i) onto the set of classes of type (ii). The definition of "similar modulo D" immediately implies that equivalence of type (ii) implies equivalence of type (iii), and therefore we obtain a mapping of the set of classes of type (ii) onto the set of classes of type (iii). Finally Problem 39 shows that there are at least 2^g classes of type (iii). The result follows.

Chapter II

1. The unital left $\mathbb{C}G$ modules correspond (via the universal mapping property of a group algebra) to representations of G on complex vector spaces. The theory in Chapter VII of *Basic Algebra* shows that every representation splits as the direct sum of irreducible representations, which correspond to simple left $\mathbb{C}G$ modules. Hence every unital left $\mathbb{C}G$ module is semisimple. The left regular representation of G, which corresponds to the left $\mathbb{C}G$ module $\mathbb{C}G$, decomposes as the sum of irreducible representations, each irreducible representation occurring as many times as its degree. The sum of all the irreducible subspaces of a given isomorphism type gives one of the factors $M_n(\mathbb{C})$ of $\mathbb{C}G$, and every factor arises this way.

2. For (a), $\operatorname{rad} A = (\mathbb{C} + \mathbb{C}X)(X^2 + 1)$, and S will be the sum of two copies of $\mathbb{C}$. Finding S requires some computation. We can identify $A/(\operatorname{rad} A)$ with the quotient $\mathbb{C}[X]/(X^2 + 1)$, and direct computation shows that the two idempotents in this notation having sum 1 are $\frac{1}{2i}(X + i)$ and $-\frac{1}{2i}(X - i)$. The proof of Proposition 2.23 shows how to lift these to idempotents in A. For the first one, put $a = \frac{1}{2i}(X + i)$ and $b = 1 - a = -\frac{1}{2i}(X - i)$, and observe that $(ab)^2 = 0$. The proposition gives the formula $e = \sum_{k=0}^{2} \binom{4}{k} a^{4-k} b^k = a^4 + 4a^3 b$, the term for $k = 2$ being 0. Then $e = a^3(a + 4b) = \frac{1}{16}(X + i)^3(-3X + 5i)$. So one contribution to S comes from $\mathbb{C}e$; the other will come from the complex conjugate in the form of $\mathbb{C}f$, where $f = \frac{1}{16}(X - i)^3(-3X - 5i)$.

We can check directly that e is an idempotent. In fact,

$$e^2 - e = e\big[\tfrac{1}{16}(X + i)^3(-3X + 5i) - 1\big].$$

The polynomial in square brackets vanishes at $X = i$, and so does its derivative. Thus the polynomial is divisible by $(X - i)^2$, and $e^2 - e = (X + i)^3(-3X + 5i) \times [(X - i)^2 Q(X)]$ is divisible by $(X^2 + 1)^2$.

For (b), the answer is yes. This problem anticipates Problem 5 below. The algebra S is spanned linearly by its idempotents, and Problem 5 shows that the idempotents are determined uniquely in the commutative case.

For (c), $\operatorname{rad} A = (\mathbb{R} + \mathbb{R}X)(X^2 + 1)$. Call the subalgebra S_0. This subalgebra will be a 2-dimensional real subalgebra isomorphic to $\mathbb{C}$. To find it, we can go through

the proof of Theorem 2.17 or we can use the Galois group. The latter method is a good bit easier. Thus we seek those members of S as in (a) that are fixed by complex conjugation. Since $S = \mathbb{C}e + \mathbb{C}\bar{e}$, the result is that $S_0 = \mathbb{R}(e + \bar{e}) + i\mathbb{R}(e - \bar{e})$. This is unique; in fact, any choice of S_0 has the property that $S_0 \otimes_{\mathbb{R}} \mathbb{C}$ is an S for (a), and we know that the S for (a) is unique.

3. Since $\operatorname{rad} A$ is a nilpotent ideal of A, $(\operatorname{rad} A) \otimes_F B$ is a nilpotent ideal of $A \otimes_F B$, and therefore $(\operatorname{rad} A) \otimes_F B \subseteq \operatorname{rad}(A \otimes_F B)$. For the reverse inclusion Proposition 2.31 shows that $\operatorname{rad}(A \otimes_F B) = I \otimes_F B$ for some two-sided ideal of A. If $(\operatorname{rad}(A \otimes_F B))^n = 0$ and $a_1, \ldots, a_n$ are in I, then $(a_1 \otimes 1) \cdots (a_n \otimes 1)$ must be 0, and hence $a_1 \cdots a_n = 0$. Therefore $I \subseteq \operatorname{rad} A$, and $\operatorname{rad}(A \otimes_F B) \subseteq (\operatorname{rad} A) \otimes_F B$.

4. For (a), suppose on the contrary that there is an infinite sequence $M_1, M_2, \ldots$ of distinct maximal ideals. Then we obtain a decreasing sequence of ideals $R \supseteq M_1 \supseteq M_1M_2 \supseteq M_1M_2M_3 \supseteq \cdots$, and the Artinian property shows that $M_1 \cdots M_n = M_1 \cdots M_nM_{n+1}$ for some n. Since M_{n+1} is prime and $M_{n+1} \supseteq M_1 \cdots M_n$, M_{n+1} contains M_j for some j with $1 \le j \le n$. By maximality, $M_n = M_j$, and we have a contradiction.

In (b), every element of $\operatorname{rad} R$ is nilpotent because $\operatorname{rad} R$ is nilpotent. Conversely if $x \in R$ is nilpotent with $x^n = 0$, then Rx is nilpotent with $(Rx)^n = 0$, since $a_1xa_2x \cdots a_nx = a_1a_2 \cdots a_nx^n = 0$ for any $a_1, \ldots, a_n \in R$. Thus $Rx \subseteq \operatorname{rad} R$, and the nilpotent element x lies in $\operatorname{rad} R$. This proves (b), and (c) follows because R is semisimple if and only if $\operatorname{rad} R = 0$.

For (d), R semisimple implies that R is a product of full matrix rings over division rings. Commutativity implies that the matrices are all of size 1-by-1 and the division rings are all fields.

5. If e' is a second representative, then $e' = e + r$ with $r \in \operatorname{rad} R$. If n is an odd integer large enough to have $r^n = 0$, then

$$0 = r^n = (e' - e)^n = \sum_{k=0}^{n} (-1)^k \tbinom{n}{k} (e')^{n-k} e^k = e' + \sum_{k=1}^{n-1} (-1)^k \tbinom{n}{k} e'e - e$$
$$= e' + \Big(\sum_{k=0}^{n} (-1)^k \tbinom{n}{k} \Big) e'e - e'e + e'e - e = e' + 0 - e'e + e'e - e = e' - e.$$

6. Let $M_1, \ldots, M_n$ be the finitely many maximal ideals, and put $N = M_1 \cdots M_n$. Nakayama's Lemma says that if I is any ideal contained in all maximal ideals, then the only finitely generated unital R module M having the property that $IM = M$ is $M = 0$. The Artinian property shows that $N^{k+1} = N^k$ for some k. We take $I = N$ and $M = N^k$ in Nakayama's Lemma. The R module M is finitely generated because Artinian implies Noetherian (Theorem 2.15), and hence Nakayama's Lemma shows that $N^k = 0$.

7. Let the maximal ideals be $M_1, \ldots, M_n$, and let $(M_1 \cdots M_n)^k = 0$. If P is a prime ideal, then $P \supseteq 0 = (M_1 \cdots M_n)^k$. Since P is prime, P contains one of the factors. Thus $P \supseteq M_j$ for some j.

8. It helps to have a multiplication table available. If the rows index a factor on the left and the columns index a factor on the right, then the resulting products are given by $\begin{pmatrix} R & M & 0 \\ 0 & 0 & M \\ 0 & 0 & S \end{pmatrix}$.

If I_2 is a left ideal of S and I_1 is a left R submodule of $R \oplus M$ containing MI_2, then $RI_2 = 0$, $MI_2 \subseteq I_1$, and $SI_2 \subseteq I_2$. Also, $RI_1 \subseteq I_1$, $MI_1 = 0$, and $SI_1 = 0$. Thus $AI_1 \subseteq I_1$ and $AI_2 \subseteq I_1 \oplus I_2$. Consequently $I_1 \oplus I_2$ is a left ideal of A.

In the reverse direction if J is a left ideal in A, then $I_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} J \subseteq R \oplus M$ and $I_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} J \subseteq S$ are such that $J = I_1 \oplus I_2$. Also, $r \in R$ implies $\begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} J = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} rJ \subseteq I_1$, while $(M \oplus S)I_1 = 0$; and $s \in S$ implies $\begin{pmatrix} 0 & 0 \\ 0 & s \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} J = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} sJ \subseteq I_2$, while $RI_2 = 0$ and $m \in M$ implies $\begin{pmatrix} 0 & m \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} J = \begin{pmatrix} 0 & m \\ 0 & 0 \end{pmatrix} J \subseteq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & m \\ 0 & 0 \end{pmatrix} J \subseteq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} J = I_1$.

9. For (a), suppose A is left Noetherian. The table produced in the solution of Problem 8 shows that $M \oplus S$ and $R \oplus M$ are two-sided ideals of A, and the respective quotient rings are R and S. As quotients of a left Noetherian ring, R and S have to be left Noetherian. If $\{M_i\}$ is an ascending chain of R submodules of M, then $\left\{\begin{pmatrix} 0 & M_i \\ 0 & 0 \end{pmatrix}\right\}$ is an ascending chain of left ideals of A, by Problem 8. The latter must be constant from some point on, and then the same thing is true for $\{M_i\}$.

Conversely suppose that R and S are left Noetherian and that the left R module M satisfies the ascending chain condition. If $\{J_i\}$ is an ascending chain of left ideals of A, then the corresponding sequence $\{(I_2)_i\}$ is an ascending chain of left ideals in S, and $\{(I_1)_i\}$ is an ascending chain of left R submodules of $R \oplus M$ containing MI_2. Since S is left Noetherian, $\{(I_2)_i\}$ is constant from some point on. Since $R = (R \oplus M)/M$ and M satisfy the ascending chain condition for their left R submodules, so does $R \oplus M$, and therefore $\{(I_1)_i\}$ is constant from some point on.

10. In view of Problem 9a, showing that A is left Noetherian amounts to showing that R and S are (left) Noetherian and M satisfies the ascending chain condition for its left R submodules. The ring S is Noetherian by assumption, and R is a field, hence is Noetherian. The action of R on M is the action of a field on itself, and the R submodules are trivial. In view of Problem 9b, A fails to be right Noetherian if the ascending chain condition fails for the right S submodules of $M = R$. If the ascending chain condition were to hold, then R would be a finitely generated S module, and the only denominators needed for members of the full field R of fractions would be those dividing the product of the denominators of the generators; these fractions are already in S, and hence S would equal R, contradiction.

The analogs of the results of Problem 9 for the Artinian case show that A fails to be either left or right Artinian if S is not Artinian. If s is a nonunit in S, then the chain of principal ideals $\{(s^k)\}$ is properly descending, since $(s^k) = (s^{k+1})$ implies $\varepsilon s^k = s^{k+1}$ for some unit ε and since the hypothesis that S is an integral domain

allows us to cancel and obtain $\varepsilon = s$, contradiction.

11. Since R and S are fields, they are left and right Noetherian and Artinian. In view of Problem 9, we are to show that $M = R$ satisfies both chain conditions for its left R modules and neither chain condition for its right S modules. Since R is a field, $M = R$ has only trivial R submodules and satisfies both chain conditions. For the S action on R, we are to examine the S vector subspaces of S. Since $\dim_S R$ is infinite, there exist both a properly increasing sequence of such subspaces and a properly decreasing one. Hence neither chain condition is satisfied.

12. For (a), the vector-space dimension over $\mathbb{F}$ is certainly 4, and computation shows that A is closed under products. The choices $a = 1$ and $b = 0$ show that A has an identity.

For (b), let $x \neq 0$ be in a two-sided ideal I. If $x = \begin{pmatrix} a & 0 \\ 0 & \sigma(a) \end{pmatrix}$, then x is invertible, and hence $I = A$. Otherwise suppose that some matrix $x = \begin{pmatrix} a & b \\ r\sigma(b) & \sigma(a) \end{pmatrix}$ with $b \neq 0$ is in I. With c as in the statement of the problem, $cx - xc = \begin{pmatrix} 0 & 2b\sqrt{m} \\ -2r\sigma(b)\sqrt{m} & 0 \end{pmatrix}$ is in I; this matrix is invertible since $b \neq 0$, and thus $I = A$.

To see that A is central, let x be in the center. The computation $0 = cx - xc$ shows that $b = 0$. Thus x is of the form $\begin{pmatrix} a & 0 \\ 0 & \sigma(a) \end{pmatrix}$. Such an x does not commute with $\begin{pmatrix} 0 & 1 \\ r & 0 \end{pmatrix}$ unless $a = \sigma(a)$, in which case x is in F.

13. The determinant is $a\sigma(a) - rb\sigma(b) = N_{K/F}(a) - rN_{K/F}(b)$ and equals 0 for a given r if and only if some pair $(a, b) \neq (0, 0)$ has $N_{K/F}(a) = rN_{K/F}(b)$. Since $r \neq 0$, both a and b are nonzero, and this equality then holds if and only if $r = N_{K/F}(ab^{-1})$.

In other words, some nonzero member of A has determinant 0 if r is a norm, and then A cannot be a division algebra. Conversely if r is not a norm, then every nonzero member of A is invertible as a matrix. Computation of the inverse matrix shows that it has the correct form to be in A. Hence A is a division algebra.

When A is not a division algebra, it is anyway finite-dimensional and central simple and has to be of the form $M_n(D)$ for some n and some division algebra D over F such that $\dim M_n(D) = 4$. The dimensional formula says that $n^2 \dim_F D = 4$. Since $n \neq 1$, we must have $n = 2$ and $D = F$.

14. The isomorphism follows from the computation $\begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ r\sigma(b) & \sigma(a) \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & bc \\ rc^{-1}\sigma(b) & \sigma(a) \end{pmatrix} = \begin{pmatrix} a & bc \\ r'\sigma(c)\sigma(b) & \sigma(a) \end{pmatrix} = \begin{pmatrix} a & bc \\ r'\sigma(bc) & \sigma(a) \end{pmatrix}$.

15. Direct computation.

16. If K is a maximal subfield, then $\dim_F K = 2$. Since the characteristic is not 2, $K = F(\sqrt{m})$ for some nonsquare $m \in F$. Define $i \in K$ be to $\sqrt{m}$.

The map $f : K \to D$ given by $f(a + bi) = a - bi$ is an algebra homomorphism into the central simple algebra D. So the Skolem–Noether Theorem produces $j \in D$ with $j(a + bi)j^{-1} = a - bi$ for all $a + bi$ in K, necessarily with j invertible.

As in the proof of Theorem 2.50, $j^2 = r$ lies in F. Define $k = ij$. Then $k^2 = ijij = i(jij^{-1})j^2 = i(-i)j^2 = -rm$, and $-rm = k^2 = ijk$ implies that $k = -rm(j^{-1})(i^{-1}) = -rm(r^{-1}j)(m^{-1}i) = -ji$.

Let us check the multiplication table for $\{1, i, j, k\}$. We know that $i^2 = m$, $j^2 = r$, $k^2 = -rm$, $ij = k$, and $ji = -k$. In addition, we have

$$\begin{aligned} jk &= jij = (jij^{-1})j^2 = (-i)r = -ri, \\ kj &= ijj = i(j^2) = ri, \\ ki &= iji = i(jij^{-1})j = i(-i)j = -mj, \\ ik &= iij = (i^2)j = mj. \end{aligned}$$

Hence the F linear map φ from A into the given central simple algebra is an algebra homomorphism sending 1 into 1. Since A is simple, φ is one-one. Since A and the given algebra both have dimension 4, φ is onto. Thus φ is an algebra isomorphism. (We did not have to check directly that $\{1, i, j, k\}$ is linearly independent over F.)

17. A is an algebra by routinely checking that it is closed under multiplication. Manifestly A has an identity and has dimension 9 over F. If I is a nonzero two-sided ideal in A, let $x = a + bj + cj^2$ be nonzero in I, and assume that x is chosen in I such that as few of the coefficients a, b, c are nonzero as possible. Possibly by multiplying x by j or j^2 on the right, we may assume that $a \neq 0$. Choose $d \in K$ with $d, \sigma(d)$, and $\sigma^2(d)$ distinct. Computation shows that $dx - xd$ has one fewer nonzero coefficient. By minimality we must have $dx - xd = 0$; hence x must have had just one nonzero coefficient. Such an x is invertible, and thus 1 is in I and $I = A$. Hence A is simple. To see that A has just F as center, we test a general element $x = a + bj + cj^2$ for commutativity with both $d \in K$ and the element j, and we find that $b = c = 0$ and $a = \sigma(a) = \sigma^2(a)$.

18. Since A is finite-dimensional central simple, $A \cong M_n(D)$ for some n and some central division algebra D over F. Then $9 = \dim A = n^2 \dim_F D$, and the only possibilities are that $n = 3$ and $D = F$, or that $n = 1$. In the first case, $A \cong M_3(F)$, and in the second case, A is a division algebra. In the first case any column of A (when viewed as $M_3(F)$) is a 3-dimensional left A module; in the second case A has no proper nonzero left A modules.

19. Left multiplication by K makes A into a K vector space, and the left K submodules of A are the K vector subspaces. The F dimension of such a subspace is 3 times the F dimension. Hence the left K submodules of A are the subspaces of K dimension 1, which consist of all left K multiples of any nonzero vector.

Let $x = a_0 + b_0 j + c_0 j^2$ be nonzero in A. Then Kx is a left A module if and only if jx lies in Kx. Here $jx = \sigma(a_0)j + \sigma(b_0)j^2 + \sigma(c_0)j^3 = r\sigma(c_0) + \sigma(a_0)j + \sigma(b_0)j^2$. This equals dx for some $d \in K$ if and only if

$$r\sigma(c_0) = da_0, \quad \sigma(a_0) = db_0, \quad \text{and} \quad \sigma(b_0) = dc_0. \tag{$*$}$$

Combining the second and third equations gives the necessary condition that $\sigma^2(a_0) = \sigma(db_0) = \sigma(d)\sigma(b_0) = \sigma(d)dc_0$. Applying σ gives the necessary condition $a_0 = \sigma^3(a_0) = \sigma(\sigma(d)dc_0) = \sigma^2(d)\sigma(d)\sigma(c_0) = \sigma^2(d)\sigma(d)r^{-1}da_0 = N_{K/F}(d)r^{-1}a_0$. Thus it is necessary that some $d \in K$ have $N_{K/F}(d) = r$. Conversely if $d \in K$ has $N_{K/F}(d) = r$, then $x_0 = 1 + d^{-1}j + d^{-1}\sigma(d)^{-1}j^2$ has $a_0 = 1$, $b_0 = d^{-1}$, and $c_0 = d^{-1}\sigma(d)^{-1}$, and we observe that the conditions $(*)$ are satisfied; thus Kx_0 is a left A submodule.

Chapter III

1. For (a), define $f : A \times K \to \mathrm{End}_{B^o} A$ by $f(a, c)(a') = aa'c$ just as in the proof of Theorem 3.3. The verification that the action of right multiplication by $b \in B$ commutes with $f(a, c)$, i.e., that $f(a, c)$ is in $\mathrm{End}_{B^o} A$, uses that B commutes with K, and the verification that the extended map $f : A \otimes_F K \to \mathrm{End}_{B^o} A$ respects multiplication uses that K is commutative; otherwise the argument is the same as with Theorem 3.3. The algebra $A \otimes_F K$ is central simple over K, and B is an algebra over K because B contains K. Since $A \otimes_F K$ is simple, f is one-one.

For (b), let V be the unique-up-to-isomorphism simple finite-dimensional left B module. If the left B module B is the direct sum of m copies of V, then the proof of Theorem 2.2 shows that $B^o \cong \mathrm{End}_B B \cong M_m(D^o)$, where D^o is the central division algebra over K given by $D^o = \mathrm{End}_B V$. Hence $B \cong M_m(D)$. If V^o denotes the unique-up-to-isomorphism simple finite-dimensional left B^o module and if $D'^o = \mathrm{End}_{B^o}(V^o)$, then we have $B \cong \mathrm{End}_{B^o}(B^o) \cong M_{m'}(D'^o)$, and it follows that $m = m'$ and $D' \cong D^o$.

Since $B \subseteq A$, A is a right B module, hence a left B^o module, and A has to be the direct sum of some number n of copies of V^o. Then the same argument gives an isomorphism $\mathrm{End}_{B^o} A \cong M_n(D'^o) \cong M_n(D)$. The Double Centralizer Theorem gives $\dim_F A = (\dim_F B)(\dim_F K)$, and thus $\dim_K A = \dim_F B = (\dim_F K)(\dim_K B) = (\dim_F K)(m \dim_K V)$. Meanwhile, $\dim_K A = n \dim_K V$ and thus $n \dim_K V = (\dim_F K)(m \dim_K V)$. So $n = m \dim_F K$. Consequently $\dim_F \mathrm{End}_{B^o} A = n^2 \dim_F D = m^2(\dim_F D)(\dim_F K)^2 = (\dim_F B)(\dim_F K)^2 = (\dim_F A)(\dim_F K) = \dim_F(A \otimes_F K)$, and the map f in (a) is onto.

For (c), application of (b) and an isomorphism from above gives $A \otimes_F K \cong \mathrm{End}_{B^o}(A) \cong M_n(D)$, and we have seen that $B \cong M_m(D)$. Thus $A \otimes_F K$ and B lie in the same Brauer equivalence class in $\mathcal{B}(K)$.

2. Take the product over σ of the equality $\rho(a(\sigma, \tau))a(\rho, \sigma\tau) = a(\rho, \sigma)a(\rho\sigma, \tau)$, and get $\rho\big(\prod_\sigma a(\sigma, \tau)\big)\prod_\sigma a(\rho, \sigma) = \prod_\sigma a(\rho, \sigma)\prod_\sigma a(\sigma, \tau)$. Canceling gives $\rho\big(\prod_\sigma a(\sigma, \tau)\big) = \prod_\sigma a(\sigma, \tau)$. Thus $\prod_\sigma a(\sigma, \tau)$ is fixed by every member of the Galois group and is in $F^\times$.

3. Proposition 3.32 and Theorem 3.31 show that $H^{2k}(\mathrm{Gal}(K/F), K^\times) \cong H^2(\mathrm{Gal}(K/F), K^\times)$ for $k \geq 1$ and $H^{2k+1}(\mathrm{Gal}(K/F), K^\times) \cong H^1(\mathrm{Gal}(K/F), K^\times)$

for $k \geq 0$. Then Corollary 3.34 gives $H^{2k} \cong F^\times \big/ N_{K/F}(K^\times)$ for all $k \geq 1$, and Theorem 3.17 gives $H^{2k+1} = 0$ for all $k \geq 0$. Finally H^0 is the subgroup of elements in $K^\times$ fixed by $\mathrm{Gal}(K/F)$, and this is $F^\times$.

4. For (a), it is shown in Chapter IX of *Basic Algebra* that $\mathbb{Q}(e^{2\pi i/p})$ is a Galois extension of $\mathbb{Q}$ with cyclic Galois group of order $p-1$ whenever p is prime. Here $p = 7$. Complex conjugation is a member of the Galois group of order 2, and K is the subfield fixed by this subgroup. Hence K has degree $6/2 = 3$ over $\mathbb{Q}$, and its Galois group is the quotient of a cyclic group of order 6 by the subgroup of order 2, hence is cyclic of order 3. The powers $\zeta^1, \ldots, \zeta^6$ form a basis of the $\mathbb{Q}$ vector space $\mathbb{Q}(\zeta)$, and the sums of them with their images under complex conjugation span K. These sums are τ_1, τ_2, τ_3. Since there are only 3 such sums, they must be linearly independent over $\mathbb{Q}$. Put $\tau_k = \zeta^k + \zeta^{-k}$. Then τ_k depends only on k mod 7, and $\tau_k = \tau_{-k}$. Hence the only τ_k's that are not any of τ_1, τ_2, τ_3 are the ones with $k \equiv 0$ mod 7. The members of the Galois group of $\mathbb{Q}(\zeta)$ carry ζ to ζ^k for $1 \leq k \leq 6$ and therefore carry τ_1 to τ_k, τ_2 to τ_{2k}, and τ_3 to τ_{3k}. None of $k, 2k, 3k$ is divisible by 7, and the result follows.

For (b), let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ have $\sigma(\tau_1) = \tau_2$, $\sigma(\tau_2) = \tau_3$, and $\sigma(\tau_3) = \tau_1$. For $x \in K$, we have $N_{K/\mathbb{Q}}(x) = x\sigma(x)\sigma^2(x)$. With $x = a\tau_1 + b\tau_2 + \tau_3$, we get 27 terms when everything is expanded out, and they are the ones listed.

For (c), $\tau_1 + \tau_2 + \tau_3 = -1$ because $\sum_{j=-3}^{3} \zeta^j = 0$. Next, $\tau_1\tau_2 = (\zeta^1 + \zeta^{-1}) \times (\zeta^2 + \zeta^{-2}) = \zeta^3 + \zeta^{-3} + \zeta^{-1} + \zeta^1 = \tau_1 + \tau_3$, and the other two identities on the second line are similar. Finally $\tau_1^2 = (\zeta^1 + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = \tau_2 + 2$, and the other two identities are similar.

For (d), let $\alpha, \beta, \gamma, \delta$ be the expressions involving τ_1, τ_2, τ_3 on the right side in (b). First we have $\tau_1^3 = \tau_1^2\tau_1 = (\tau_2 + 2)\tau_1 = \tau_1\tau_2 + 2\tau_1 = 3\tau_1 + \tau_3$. Summing this expression and similar expressions for τ_2^3 and τ_3^3 gives $\alpha = 4(\tau_1 + \tau_2 + \tau_3) = -4$. Second $\beta = \tau_1\tau_2\tau_3 = (\tau_1 + \tau_3)\tau_3 = \tau_2 + \tau_3 + \tau_1 + 2 = 1$. In (d), the coefficient of abc is $\alpha + 3\beta = -4 + 3 = -1$, and the coefficient of $a^3 + b^3 + c^3$ is $\beta = 1$. Third $\tau_1^2\tau_2 = \tau_1(\tau_1 + \tau_3) = (\tau_2 + 2) + (\tau_2 + \tau_3) = \tau_3 + 2\tau_2 + 2$. Similarly $\tau_2^2\tau_3 = \tau_1 + 2\tau_3 + 2$ and $\tau_3^2\tau_1 = \tau_2 + 2\tau_1 + 2$. The sum is $\gamma = 3(\tau_1 + \tau_2 + \tau_3) + 6 = 3$. Fourth $\tau_1\tau_2^2 = \tau_1(\tau_3 + 2) = \tau_2 + \tau_3 + 2\tau_1$. Similarly $\tau_2\tau_3^2 = \tau_1 + \tau_3 + 2\tau_2$ and $\tau_3\tau_1^2 = \tau_1 + \tau_2 + 2\tau_3$. The sum is $\delta = 4(\tau_1 + \tau_2 + \tau_3) = -4$.

For (e), the norm modulo 3 is $(a^3 + b^3 + c^3) - abc - (a^2c + ab^2 + bc^2)$, and this is $\equiv (a + b + c) - abc - (a^2c + ab^2 + bc^2)$ mod 3. Any nonzero square is $\equiv 1$ mod 3, and we consider cases. If 3 does not divide abc, then $a^2 \equiv b^2 \equiv c^2 \equiv 1$ mod 3, and the norm is $\equiv -abc \not\equiv 0$ mod 3. If 3 divides a but not bc, then $b^2 \equiv c^2 \equiv 1$ mod 3, and the norm is $\equiv (b + c) - b \equiv c \not\equiv 0$ mod 3. If 3 divides a and b but not c, then the norm is $\equiv c \not\equiv 0$ mod 3, while if 3 divides a and c but not b, then the norm is $\equiv b \not\equiv 0$ mod 3. The case that 3 divides all of a, b, c is excluded by the condition that $\mathrm{GCD}(a, b, c) = 1$, and all other cases are handled by symmetry. Thus in all cases the norm is not divisible by 3.

For (f), let x, y, z be members of $\mathbb{Q}$ not all 0. Choose integers a, b, c and relatively

prime integers n and d such that $x = n^{-1}da$, $y = nd^{-1}db$, $z = nd^{-1}c$, and $\mathrm{GCD}(a, b, c) = 1$. Then $N_{K/\mathbb{Q}}(x\tau_1 + y\tau_2 + z\tau_3) = d^{-3}n^3 N_{K/\mathbb{Q}}(a\tau_1 + b\tau_2 + c\tau_3)$. Applying (e) and supposing that 3 is a norm, we obtain $3 = d^{-3}n^3(3k + (1 \text{ or } 2))$ for some integer k. Thus $3d^3 = n^3(3k + (1 \text{ or } 2))$. This equality forces n to divide d, and we may therefore take $n = 1$. Thus $3d^3 = 3k + (1 \text{ or } 2)$. The left side is divisible by 3, and the right side is not. Hence 3 is not a norm.

5. For (a), Dirichlet's Theorem (Theorem 1.21) says that there are infinitely many primes of the form $p = kn + 1$. For any such p, n divides $p - 1$. For (b) with this p, the Galois group of $\mathbb{Q}(e^{2\pi i/p})/\mathbb{Q}$ is cyclic of order $p - 1$ and has a cyclic subgroup of order $(p - 1)/n$. The corresponding subfield is a Galois extension of $\mathbb{Q}$ of degree n with cyclic Galois group.

6. For $0 \le k < n$ and $0 \le l < n$, we have $x_{\sigma^k} x_{\sigma^l} = j^k j^l = j^{k+l}$. Meanwhile, $x_{\sigma^{k+l}}$ equals j^{k+l} if $k + l < n$ and equals j^{k+l-n} if $k + l \ge n$. So $x_{\sigma^k} x_{\sigma^l} = x_{\sigma^{k+l}}$ if $k + l < n$ and $x_{\sigma^k} x_{\sigma^l} = j^n x_{\sigma^{k+l-n}} = r x_{\sigma^{k+l-n}}$ if $k + l \ge n$. Thus $a(\sigma^k, \sigma^l)$ has the stated value.

7. It is just a question of checking that $c_{\sigma^k}\sigma^k(c_{\sigma^l}) = a(\sigma^k, \sigma^l)c_{\sigma^{k+l}}$ with $a(\sigma^k, \sigma^l)$ as in the previous problem.

8. We have $\partial_0(1, \sigma^k) = 1 - \sigma^k$ and thus

$$f_0\partial_0(1, \sigma^k) = 1 - \sigma^k = (\sigma - 1)(-(1 + \sigma + \cdots + \sigma^{k-1})).$$

If we put $f_1(1, \sigma^k) = -(1+\sigma+\cdots+\sigma^{k-1})$, then we have $Tf_1(1, \sigma^k) = f_0\partial_0(1, \sigma^k)$ for all k.

Next, for $k \le l$, we have $\partial_1(1, \sigma^k, \sigma^l) = (\sigma^k, \sigma^l) - (1, \sigma^l) + (1, \sigma^k) = \sigma^k(1, \sigma^{l-k}) - (1, \sigma^l) + (1, \sigma^k)$. Then $f_1\partial_1(1, \sigma^k, \sigma^l)$ equals

$$-\sigma^k(1 + \sigma + \cdots + \sigma^{l-k-1}) + (1 + \sigma + \cdots + \sigma^{l-1}) - (1 + \sigma + \cdots + \sigma^{k-1}) = 0.$$

For $k > l$, the term (σ^k, σ^l) is replaced by $\sigma^k(1, \sigma^{n+l-k})$. Thus $\partial_1(1, \sigma^k, \sigma^l) = \sigma^k(1, \sigma^{n+l-k}) - (1, \sigma^l) + (1, \sigma^k)$. Then $f_1\partial_1(1, \sigma^k, \sigma^l)$ is

$$\begin{aligned} &-\sigma^k(1 + \sigma + \cdots + \sigma^{n+l-k-1}) + (1 + \sigma + \cdots + \sigma^{l-1}) - (1 + \sigma + \cdots + \sigma^{k-1}) \\ &\quad = -(1 + \sigma + \cdots + \sigma^{n+l-1}) + (1 + \sigma + \cdots + \sigma^{l-1}) \\ &\quad = \sigma^l(-(1 + \sigma + \cdots + \sigma^{n-1})). \end{aligned}$$

If we define f_2 as in the problem, then in the two cases we have

$$\begin{aligned} k \le l: &\qquad Nf_2(1, \sigma^k, \sigma^l) = (1 + \sigma + \cdots + \sigma^{n-1})(0) = 0 = f_1\partial_1(1, \sigma^k, \sigma^l), \\ k > l: &\qquad Nf_2(1, \sigma^k, \sigma^l) = (1 + \sigma + \cdots + \sigma^{n-1})(-\sigma^l) = f_1\partial_1(1, \sigma^k, \sigma^l). \end{aligned}$$

9. To ψ in $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, K^\times)$, the chain map of the previous problem associates $\psi \circ f_2$ in $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G(\{(1, g_1, g_2)\}), K^\times)$, and then the corresponding member of $C^2(G, K^\times)$ is $\Phi_2(\psi f_2)$ whose value at (g_1, g_2) is $\psi f_2(1, g_2, g_1g_2)$. That is, $\Phi_2(\psi f_2)(\sigma^k, \sigma^l) = \psi f_2(1, \sigma^k, \sigma^{k+l})$, and this by Problem 8 is $\psi(0)$ if $k + l < n$ and is $\psi(-\sigma^{k+l-n}) = \psi(\sigma^{k+l-n})^{-1}$ if $k + l \ge n$.

10. Taking Proposition 3.32 into account, we see that the mapping whose kernel gives the cocycles is $\mathrm{Hom}(T, 1) : \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, K^\times) \to \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, K^\times)$. Here $\mathrm{Hom}(T, 1)\psi = \psi \circ T$. We are identifying ψ with $\psi(1)$ and also $\psi \circ T$ with $\psi(T(1)) = \psi(\sigma - 1) = (\sigma - 1)\psi(1)$ in additive notation. Hence the effect of $\mathrm{Hom}(T, 1)$ is to carry y to $\sigma(y)y^{-1}$ in multiplicative notation. A necessary and sufficient condition for $\sigma(y)y^{-1}$ to be 1 is that y be in $F^\times$, since the subgroup of $K^\times$ fixed by G is $F^\times$.

11. Since $\psi(0) = 1$ and $\psi(\sigma^{k+l-n}) = \sigma^{k+l-n}\psi(1) = \psi(1) = r^{-1}$, the member a of $C^2(G, K^\times)$ that corresponds to ψ has

$$a(\sigma^k, \sigma^l) = \begin{cases} 1 & \text{if } k + l < n, \\ r & \text{if } k + l \geq n, \end{cases}$$

and this is the 2-cocycle of Problem 6.

12. Corollary 3.34 and Theorem 3.14 combine to give us a group isomorphism $\mathcal{B}(K/F) \cong F^\times \big/ N_{K/F}(K^\times)$, and the above problems show that the element r of $F^\times$ used in defining A corresponds under this isomorphism to the coset of r^{-1}. Hence the order of the Brauer equivalence class of A equals the order of the coset of r, as required.

If A is not a division algebra, then $A \cong M_m(D)$ for some central division algebra D over F and for some integer $m > 1$. Here $\dim_F D = (n/m)^2 < n^2$. Corollary 3.15 then gives the contradiction that the order of the Brauer equivalence class of D, which is the same as the order of the class of A, divides n/m, which in turn is $< n$.

13. The Skolem–Noether Theorem shows that the image matrices under two different isomorphisms φ and ψ have to be conjugate to one another, say with $\varphi = C^{-1}\psi C$. Then

$$\begin{aligned} \det(\varphi(X1 - a \otimes 1)) &= \det(C^{-1}\psi(C(X1 - a \otimes 1))) \\ &= (\det C)^{-1} \det(\psi(X1 - a \otimes 1))(\det C) \\ &= \det(\psi(X1 - a \otimes 1)). \end{aligned}$$

14. Let $B = A \otimes_F K$. The left B module B is semisimple and is the direct sum of n isomorphic simple modules of dimension n. On each the operation of $a \otimes 1$ has characteristic polynomial $\det(X1 - a \otimes 1)$, and the characteristic polynomial for the direct sum of the spaces is the product of the characteristic polynomials.

15. Arguing by contradiction, we may assume that the statement is false for some monic $P = P(X)$ and that P has the lowest possible degree among all monic polynomials for which the assertion is false. Factor P over K into powers of distinct irreducible polynomials as $P = P_1^{d_1} \cdots P_k^{d_k}$. The n-fold product of $P_1^{d_1} \cdots P_k^{d_k}$ with itself is in $F[X]$ by assumption and is therefore invariant under $\mathrm{Gal}(K/F)$. Consequently for each $\sigma \in \mathrm{Gal}(K/F)$ and each P_i, there exists some P_j such that $P_j = \sigma(P_i)$. It follows that if H is the subgroup of $G = \mathrm{Gal}(K/F)$ fixing P_1, then

$Q = \prod_{\sigma H \in G/H} \sigma P_1$ is the product of distinct irreducible factors of P and hence divides P. The polynomial Q is fixed by every member of G and hence is monic in $F[X]$. Thus $Q \neq P$. Then Q^n is in $F[X]$, and hence $(P/Q)^n$ is in $F[X]$. The fact that P is not in $F[X]$ implies that $Q \neq P$. Therefore $\deg(P/Q) < \deg P$. By the minimal choice of $\deg P$, P/Q is in $F[X]$. Therefore $P = (P/Q)Q$ is in $F[X]$, contradiction.

16. For a matrix m with entries in a field, passing to a larger field does not change $\det(X1 - m)$. Suppose we start with two finite Galois extensions K_1 and K_2 of F that split A. Let K_1 be a splitting field for a polynomial $g_1 \in F[X]$, and let K_2 be a splitting field for $g_2 \in F[X]$. Define K to be a splitting field for $g_1 g_2$. Then K is a finite Galois extension of F, and we can regard it as containing both K_1 and K_2. Applying the first sentence of this paragraph first to K_1 and K and then to K_2 and K, we see that the reduced characteristic polynomial is the same over K_1 as it is over K_2.

17. The formulas for $\mathrm{Nrd}_{A/F}(ab)$ and $\mathrm{Nrd}_{A/F}(1)$ follow from properties of determinants. From Problem 14 we observe that $\det a = (-1)^{n^2} \det(-a)$ and $\det(-\varphi(a \otimes 1)) = (-1)^n \det(\varphi(a \otimes 1))$. Substituting $X = 0$ into the formula therefore gives us $N_{A/F}(a) = \det a = (-1)^{n^2} \det(-a) = (-1)^{n^2} \det(-\varphi(a \otimes 1))^n = (-1)^{n^2}((-1)^n)^n \det(\varphi(a \otimes 1))^n = \det(\varphi(a \otimes 1))^n = \mathrm{Nrd}_{A/F}(a)^n$. If a is invertible, then $1 = \mathrm{Nrd}_{A/F}(1) = \mathrm{Nrd}_{A/F}(aa^{-1}) = \mathrm{Nrd}_{A/F}(a)\mathrm{Nrd}(a^{-1})$ shows that $\mathrm{Nrd}_{A/F}(a)$ is nonzero. Conversely if $\mathrm{Nrd}_{A/F}(a) \neq 0$, then $\mathrm{Nrd}_{A/F}(a) \neq 0$ and hence $\det L(a) \neq 0$. If $P(X)$ is the algebra polynomial of $L(a)$, then the Cayley–Hamilton Theorem shows that $P(L(a)) = 0$. Since $\det L(a) \neq 0$, $P(X)$ has a nonzero constant term. Therefore we can separate the constant term in the equation $P(L(a)) = 0$ to exhibit an identity of the form $L(a)Q(L(a)) = 1$ for some polynomial $Q(X)$, and the element $Q(a)$ is a 2-sided inverse to a in A. This proves (a), and the conclusion about division algebras is immediate.

18. The definition gives

$$\begin{aligned} m(dx_\rho) &= \sum_\mu \mu(d)a(\mu, \rho)E_{\mu,\mu\rho}, \\ m(cx_\tau) &= \sum_\sigma \sigma(c)a(\sigma, \tau)E_{\sigma,\sigma\tau}, \\ m\big((dx_\rho)(cx_\tau)\big) &= m\big(d\rho(c)a(\rho, \tau)x_{\rho\tau}\big) = \sum_\mu \mu\big(d\rho(c)a(\rho, \tau)\big)a(\mu, \rho\tau)E_{\mu,\mu\rho\tau}. \end{aligned}$$

Also we have

$$\begin{aligned} m(dx_\rho)m(dx_\rho) &= \sum_{\mu,\sigma} \mu(d)a(\mu, \rho)\sigma(c)a(\sigma, \tau)E_{\mu,\mu\rho}E_{\sigma,\sigma\tau} \\ &= \sum_\mu \mu(d)\mu\rho(c)a(\mu, \rho)a(\mu\rho, \tau)E_{\mu,\mu\rho\tau}. \end{aligned}$$

This matches $m\big((dx_\rho)(cx_\tau)\big)$ by the cocycle relation for a.

For the reduced norm we have two one-one F algebra homomorphisms of A into $M_n(K)$, one via the mapping m above and one by the embedding $A \to A \otimes_F 1 \subseteq A \otimes_F K \cong M_n(K)$, and these are conjugate by the Skolem–Noether Theorem. Hence the determinant gives the same result in the two cases. The determinant in the second case gives the reduced norm, and hence it must give the reduced norm in the first case.

19. The algebra $\mathbb{H}$ can be realized as all complex matrices $x = \left(\begin{smallmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{smallmatrix}\right)$, and $\mathrm{Nrd}_{\mathbb{H}/\mathbb{R}}(x) = |\alpha|^2 + |\beta|^2$ and $N_{\mathbb{H}/\mathbb{R}}(x) = (|\alpha|^2 + |\beta|^2)^2$ as a special case of Problem 18.

20. Let D be a finite-dimensional central division algebra over F, say with $\dim_F D = n^2$. Choose a basis $\{x_k\}$ of D over F, and expand elements of D as $x = \sum_{j=1}^{n^2} c_j x_j$. The function $P(c_1, \ldots, c_{n^2}) = \mathrm{Nrd}_{D/F}\left(\sum_{j=1}^{n^2} c_j x_j\right)$ is easily checked to be a homogeneous polynomial of degree n in n^2 variables, and condition (C1) says that it has a nontrivial zero if $n < n^2$. In this case the corresponding member x of D would be a nonzero element of D that fails to be invertible, and there is no such element. We conclude that $n < n^2$ is false, and that means that $n = 1$. Therefore F is the only finite-dimensional central division algebra over F, and $\mathcal{B}(F) = 0$.

Chapter IV

1. For (a), every free abelian group of finite rank is in the category, and such groups provide enough projectives.

Let $I = F \oplus T$ be a decomposition of an injective I as the direct sum of a free abelian group F of rank k and a torsion group T. The sequence $0 \to F \oplus T \to 2F \oplus T \to (\mathbb{Z}/2\mathbb{Z})^k \to 0$ is exact but not split unless $k = 0$, and thus $F = 0$. Thus every injective in the category is a finite group, and no infinite group in the category embeds into an injective.

For (b), every abelian group and in particular every torsion abelian group is a subgroup of a divisible group. The torsion subgroup of the divisible group is still divisible and is still an injective, and thus every group in the category embeds in an injective in the category.

Let P be a projective in the category mapping onto $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ by a homomorphism τ, and let x be an element of P with $\tau(x) = 1$. If g is a generator of a cyclic group G of order 2^k, then there is a homomorphism φ of G onto $\mathbb{Z}/2\mathbb{Z}$ with $\varphi(g) = \tau(x) = 1$. Since P is projective, there exists a homomorphism $\sigma : P \to G$ with $\varphi\sigma = \tau$, and then we have $1 = \tau(x) = \varphi\sigma(x)$. Then $\sigma(x) = g^m$ for some odd integer m, and this has order 2^k. Hence x has order at least 2^k. Since k is arbitrary, x must have infinite order. But all groups in the category are torsion groups, and P therefore cannot exist.

2. Let p be a prime, and let $\mathcal{C}$ be the category of all abelian groups that are the underlying additive group of a vector space over the field of p elements. This category

coincides with the category of all direct sums of copies of $\mathbb{Z}/p\mathbb{Z}$. Every such abelian group is projective and injective for the category.

3. Every unital left R module is the direct sum of simple R modules. Hence every short exact sequence splits, and every module is both projective and injective for $\mathcal{C}_R$.

4. For (a), let I be injective. Given $x \in I$ and $a \neq 0$ in R, let $B = C = R$, let $\tau : R \to I$ have $\tau(r) = rx$, and let $\varphi : R \to R$ have $\varphi(r) = ra$. Setting up Figure 4.4, we obtain $\sigma : R \to I$ with $\tau = \sigma\varphi$. If we put $y = \sigma(1)$ and evaluate both sides at 1, then we obtain $x = \tau(1) = \sigma(\varphi(1)) = \sigma(a) = a\sigma(1) = ay$, as required.

For (b), suppose that the unital left R module I is divisible. Suppose that J is an ideal of R, and write $J = (a)$. Let $\varphi : J \to I$ be an R homomorphism. Since I is divisible, there exists y in I with $ay = \varphi(a)$. Then φ extends to the R homomorphism Φ with $\Phi(1) = y$. By Proposition 4.15, I is injective.

5. Proposition 4.20 shows that there exists an injective I_0 containing an isomorphic copy $\overline{M}$ of M. Problem 4 shows that I_0 is divisible, and hence $I_1 = I_0/\overline{M}$ is divisible. By Problem 4, I_1 is injective. Then $0 \to M \to I_0 \to I_1 \to 0$ is an injective resolution of M.

6. If a module M in $\mathcal{C}$ is given, we form the appropriate kind of resolution X in $\mathcal{C}$ needed to compute the derived functors of G, and the same X will be appropriate for computing the derived functors of $F \circ G$. The derived functors of G come from the homology or cohomology of $G(X)$ with $G(M)$ removed, and the derived functors of $F \circ G$ come similarly from $F(G(X))$. Thus the result follows from Proposition 4.4.

7. If a module M in $\mathcal{C}$ is given, we form the appropriate kind of resolution X in $\mathcal{C}$ needed to compute the derived functors of $G \circ F$ on M. Then $F(X)$ is the appropriate kind of resolution for computing the derived functors of G on $F(M)$, and the result follows.

8. For n odd, $H^n(G, M)$ is the cohomology of the complex

$$\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) \xleftarrow{N} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) \xleftarrow{T} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M),$$

while for n even, $H^n(G, M)$ is the cohomology of the complex

$$\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) \xleftarrow{T} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M) \xleftarrow{N} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M).$$

This proves the isomorphisms concerning cohomology. For n odd $H_n(G, M)$ is the homology of the complex

$$\mathbb{Z}G \otimes_{\mathbb{Z}G} M \xrightarrow{N} \mathbb{Z}G \otimes_{\mathbb{Z}G} M \xrightarrow{T} \mathbb{Z}G \otimes_{\mathbb{Z}G} M,$$

while for n even, $H_n(G, M)$ is the homology of the complex

$$\mathbb{Z}G \otimes_{\mathbb{Z}G} M \xrightarrow{T} \mathbb{Z}G \otimes_{\mathbb{Z}G} M \xrightarrow{N} \mathbb{Z}G \otimes_{\mathbb{Z}G} M.$$

This proves the isomorphisms concerning homology.

9. For (a), let $T_{AB} : \mathrm{Hom}_{\mathcal{D}}(F(A), B) \to \mathrm{Hom}_{\mathcal{C}}(A, G(B))$ be the natural isomorphism. Naturality in B says for any $\psi : B \to B'$ that we have

$$\mathrm{Hom}_{\mathcal{C}}(1_A, G(\psi)) \circ T_{AB} = T_{AB'} \circ \mathrm{Hom}_{\mathcal{D}}(1_{F(A)}, \psi)$$

on $\mathrm{Hom}_{\mathcal{D}}(F(A), B)$. Let P be projective in $\mathcal{C}$. We are to prove that $F(P)$ is projective in $\mathcal{D}$, thus to prove that $\mathrm{Hom}_{\mathcal{D}}(F(P), \cdot)$ is exact. We need to show that whenever $\psi : B \to B'$ is onto in $\mathcal{D}$, then $\mathrm{Hom}_{\mathcal{D}}(1_{F(P)}, \psi)$ is onto. By hypothesis, $G(\psi) : G(B) \to G(B')$ is onto in $\mathcal{C}$. The displayed equation with $A = P$ has $\mathrm{Hom}_{\mathcal{C}}(1_P, G(\psi))$ onto, and T_{PB} and $T_{PB'}$ are given as isomorphisms. Therefore $\mathrm{Hom}_{\mathcal{D}}(1_{F(P)}, \psi)$ is onto, as we were to show. The proof of (b) is similar.

10. Conclusion (a) follows from the natural isomorphism $\mathrm{Hom}_S(P_R^S A, B) = \mathrm{Hom}_S(S \otimes_R A, B) \cong \mathrm{Hom}_R(A, \mathcal{F}_S^R B)$. Conclusion (b) follows from Problem 9a with $F = P_R^S$ and $G = \mathcal{F}_S^R$, since $\mathcal{F}_S^R$ is exact and therefore carries onto maps to onto maps. For (c), $P_R^S A$ is given by the tensor product $S \otimes_R A$, and this tensor product is an exact functor of A if S is projective as a right R module, by Proposition 4.19a.

For (d), part (c) says that $M \mapsto P_R^S M$ is an exact functor. Taking it to be F in Problem 7a and G to be $\mathrm{Hom}_S(\cdot, N)$, we have $\mathrm{Ext}_S^k(P_R^S M, N) = G^k(F(M))$. Problem 7a says that this is equal to $(G \circ F)^k$. Since $(G \circ F)(M) = \mathrm{Hom}_S(P_R^S M, N) \cong \mathrm{Hom}_R(M, \mathcal{F}_S^R N)$ has $(G \circ F)^k(M) = \mathrm{Ext}_R^k(M, \mathcal{F}_S^R N)$, we obtain $\mathrm{Ext}_S^k(P_R^S M, N) \cong \mathrm{Ext}_R^k(M, \mathcal{F}_S^R N)$.

For (e), (b) shows that the chain complex $P_R^S X$ is projective over $P_R^S M$, and we are assuming that Y is exact (and projective) over $P_R^S M$. Theorem 4.12 says that the identity map on $P_R^S M$ extends to a chain map $f : P_R^S X \to Y$ that is unique up to homotopy. Dropping the terms in degree -1 and applying the functor $\mathrm{Hom}_S(\cdot, N)$ to the diagram gives us a cochain map from the complex $\mathrm{Hom}_S(Y, N)$ to the complex $\mathrm{Hom}_S(P_R^S X, N) \cong \mathrm{Hom}_R(X, \mathcal{F}_S^R N)$. Thus we get homomorphisms on cohomology $\mathrm{Ext}_S^*(P_S^R M, N) \to \mathrm{Ext}_R^*(M, \mathcal{F}_S^R N)$.

11. Conclusion (a) follows from the natural isomorphisms $\mathrm{Hom}_S(A, I_R^S B) = \mathrm{Hom}_S(A, \mathrm{Hom}_R(S, B)) \cong \mathrm{Hom}_R(S \otimes_S A, B) \cong \mathrm{Hom}_R(\mathcal{F}_S^R A, B)$. Conclusion (b) follows from Problem 9b because $\mathcal{F}_S^R$ is exact and therefore carries one-one maps to one-one maps. For (c), $I_R^S = \mathrm{Hom}_R(S, \cdot)$ is exact if S is projective as a right R module, by Proposition 4.19a.

For (d), part (c) says that $M \mapsto I_R^S M$ is an exact functor. Taking it to be F in Problem 7b and G to be $\mathrm{Hom}_S(M, \cdot)$, we have $\mathrm{Ext}_S^k(M, I_R^S N) = G^k(F(N))$. Problem 7b says that this is equal to $(G \circ F)^k$. Since $(G \circ F)(N) = \mathrm{Hom}_S(M, I_R^S N) \cong \mathrm{Hom}_R(\mathcal{F}_S^R M, N)$ has $(G \circ F)^k(M) = \mathrm{Ext}_R^k(\mathcal{F}_S^R M, N)$, we obtain $\mathrm{Ext}_S^k(N, I_R^S N) \cong \mathrm{Ext}_R^k(\mathcal{F}_S^R M, N)$.

For (e), (b) shows that the cochain complex $I_R^S X$ is injective over $I_R^S N$, and we are assuming that Y is exact (and injective) over $I_R^S N$. Theorem 4.16 says that the identity map on $I_R^S N$ extends to a cochain map $f : Y \to I_R^S X$ that is unique up to

homotopy. Dropping the terms in degree -1 and applying the functor $\mathrm{Hom}_S(M, \cdot)$ to the diagram gives us a cochain map from the complex $\mathrm{Hom}_S(M, Y)$ to the complex $\mathrm{Hom}_S(M, I_R^S X) \cong \mathrm{Hom}_R(\mathcal{F}_S^R M, X)$. Thus we get homomorphisms on cohomology $\mathrm{Ext}_S^*(M, I_S^R N) \to \mathrm{Ext}_R^*(\mathcal{F}_S^R M, N)$.

12. For (a), the definition of Φ_q is

$$(\Phi_q \varphi)(g_1, \ldots, g_q) = \varphi(1, g_1, g_1 g_2, \ldots, g_1 \cdots g_q)$$

for $\varphi \in \mathrm{Hom}_{\mathbb{Z}G}(F_q, M)$. Putting $f = \Phi_q \varphi$ gives $(\rho^* f)(g_1, \ldots, g_q) = \rho^*(\Phi_q \varphi) = \Phi_q(\varphi \circ \rho) = (\Phi_q \varphi) \circ \rho$, as asserted.

For inflation the groups are $(G, G') = (G, G/H)$, and the map ρ is the quotient map; the effect is given by $(\mathrm{Inf} f)(g_1, \ldots, g_q) = f(g_1 H, \ldots, g_q H)$ for f in $C^q(G/H, M^H)$. For restriction the groups are $(G, G') = (H, G)$, and the map is the inclusion; the effect is given by $(\mathrm{Res}\psi)(h_1, \ldots, h_q) = \psi(h_1, \ldots, h_q)$ for $\psi \in C^q(G, M)$.

For (b), let f be in $C^1(G/H, M^H)$. Then $\mathrm{Res}(\mathrm{Inf}(f))(h) = \mathrm{Inf}(f)(h) = f(hH) = f(H)$. The condition for f to be a cocycle is that $\delta_1 f = 0$, i.e., that $f(uv) = f(u) + u(f(v))$ for u and v in G/H. Taking u and v to be the identity coset H shows that $f(H) = 0$.

For (c), let $f \in C^1(G/H, M^H)$ be a cocycle. Then $\mathrm{Inf}(f)(g) = f(gH)$. If this is a coboundary in $C^1(G, M)$, then there exists $\psi \in M$ with $\delta_0 \psi = f$, i.e., with $f(gH) = g\psi - \psi$ for all g. The left side depends only on the coset gH, and hence so must the right side. Then it follows that $gh\psi = g\psi$ for all $h \in H$ and that ψ is in M^H. Then the formula $f(gH) = g\psi - \psi$ exhibits f as a coboundary in $C^1(G/H, M^H)$.

For (d), let f be a cocycle in $C^1(G, M)$ such that $\mathrm{Res} f$ is a coboundary in $C^1(H, M)$. The formula is $(\mathrm{Res} f)(h) = f(h)$, and the coboundary condition shows that there is some $\psi \in M^H$ with $f(h) = h\psi - \psi$ for $h \in H$. Since ψ is in M^H, $f(h) = 0$ for all $h \in H$. The cocycle condition on f is that $f(uv) = f(u) + u(f(v))$ for all u and v in G. Taking v to be in H shows that $f(gh) = f(g)$ for all $h \in H$. Taking instead u to be in H shows that $f(hg) = h(f(g))$ for all $h \in H$. Since H is normal, $h(f(g)) = f(g)$ for all $h \in H$. Therefore f takes values in M^H and is Inf of the cocycle $\bar{f}$ in $C^1(G/H, M^H)$ given by $\bar{f}(gH) = f(g)$.

13. For (a), we have $(g_0 \varphi_m)(g) = \varphi_m(g g_0) = g g_0 m = \varphi_{g_0 m}(g)$, and $m \mapsto \varphi_m$ is a $\mathbb{Z}G$ homomorphism. Suppose that $\varphi_m = 0$. Then $gm = 0$ for all g and in particular for $g = 1$. Therefore $m = 0$, and $m \mapsto \varphi_m$ is one-one. Then it follows that the sequence is exact.

For (b), we know that $\mathbb{Z}G$ as an abelian group is free abelian. Then Problem 11d shows that $H^k(G, B) = \mathrm{Ext}_{\mathbb{Z}G}^k(\mathbb{Z}, B) = \mathrm{Ext}_{\mathbb{Z}G}^k(\mathbb{Z}, I_{\mathbb{Z}}^{\mathbb{Z}G}(\mathcal{F}_{\mathbb{Z}G}^{\mathbb{Z}} M)) \cong \mathrm{Ext}_{\mathbb{Z}}^k(\mathbb{Z}, \mathcal{F}_{\mathbb{Z}G}^{\mathbb{Z}} M)$. Since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \cdot)$ is exact from $\mathcal{C}_{\mathbb{Z}}$ to itself, $\mathrm{Ext}_{\mathbb{Z}}^k(\mathbb{Z}, \mathcal{F}_{\mathbb{Z}G}^{\mathbb{Z}} M) = 0$ for $k \geq 1$.

For (c), a $\mathbb{Z}$ basis of $\mathbb{Z}G$ consists of all 1-tuples (g) with $g \in G$, and a $\mathbb{Z}$ basis of $\mathbb{Z}H$ consists of all (h) with $h \in H$. Let $\{v\}$ be a set of representatives of the cosets of

G/H, and let A be the free abelian group on $\{v\}$. The $\mathbb{Z}$-bilinear map $(v, (h)) \mapsto (vh)$ extends to a homomorphism of $A \otimes_{\mathbb{Z}} \mathbb{Z}H$ into $\mathbb{Z}G$ that is manifestly onto, and it is one-one because $\sum n_i(v_i h_i) = 0$ implies $n_i = 0$ for all i. Thus it is an isomorphism.

For (d), use of (c) gives $\mathcal{F}_{\mathbb{Z}G}^{\mathbb{Z}H} B \cong \mathcal{F}_{\mathbb{Z}G}^{\mathbb{Z}H} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, M) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathcal{F}_{\mathbb{Z}G}^{\mathbb{Z}H}(\mathbb{Z}G), M)$ $\cong \mathrm{Hom}_{\mathbb{Z}}(A \otimes_{\mathbb{Z}} \mathbb{Z}H, M) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}H, \mathrm{Hom}_{\mathbb{Z}}(A, M))$, and then $H^k(H, \mathcal{F}_{\mathbb{Z}G}^{\mathbb{Z}H} B) = 0$ for $k \geq 1$ by the same argument as in (b).

For (e), the long exact sequence for $\mathrm{Ext}_H^*(\mathbb{Z}, \cdot)$ that comes from the short exact sequence in (a) shows that $0 \to H^0(H, M) \to H^0(H, B) \to H^0(H, N) \to H^1(H, M)$ is exact. The right member is assumed to be 0, and the three middle members are isomorphic to M^H, B^H, and N^H.

For (f), consider the $\mathbb{Z}$ bilinear map $(1, (g)) \mapsto (gH)$ of $\mathbb{Z} \times \mathbb{Z}G$ into $\mathbb{Z}(G/H)$, and extend it to a $\mathbb{Z}$ linear map of $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}G$ into $\mathbb{Z}(G/H)$. The group H acts trivially on $\mathbb{Z}$ on the right, and it acts on $\mathbb{Z}(G/H)$ by left translation. Let h be in H. The passage $Z \times \mathbb{Z}G \to \mathbb{Z}(G/H)$ has $(1h, (g)) \mapsto (gH)$ and $(1, h(g)) \mapsto h(gH) = (gH)$; thus the group homomorphism $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}G \to \mathbb{Z}(G/H)$ descends to a homomorphism of $\mathbb{Z} \otimes_{\mathbb{Z}H} \mathbb{Z}G$ into $\mathbb{Z}(G/H)$. This is certainly onto. To see that it is one-one, let $\sum_i n_i 1 \otimes (g_i) \mapsto 0$. Then $\sum_i n_i(g_i H) = 0$, and for each coset representative v in G, $\sum_{g_i \in vH} n_i(g_i) = 0$. So $\sum_i n_i(h_i^{-1} v) = 0$, and $\big(\sum_i n_i(h_i^{-1})\big)(v) = 0$. Then $\sum_i n_i(h_i^{-1}) = 0$ in $\mathbb{Z}H$ because (v) is invertible in $\mathbb{Z}G$, and it follows that the map is one-one.

For (g), (f) gives $B^H = \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, M)) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z} \otimes_{\mathbb{Z}H} \mathbb{Z}G, M) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}(G/H), M)$, and the same argument as in (b) shows that $H^k(G/H, B^H) = 0$ for $k \geq 1$.

Conclusion (h) is immediate because $q \geq 2$ and because all the cohomology associated with B has been shown to be 0 in degrees ≥ 1.

The commutativity in conclusion (i) follows because the inflation and restriction mappings are clearly functorial. The vertical mappings have been shown to be isomorphisms in (h). To see via induction that the top row is exact, we have to verify that $H^k(H, N) = 0$ for $k \leq q - 2$; but $H^k(H, N) \cong H^{k+1}(H, M)$ for all $k \geq 1$, and $H^{k+1}(H, M)$ is assumed to be 0 for $k + 1 \leq q - 1$. Therefore the bottom row is exact, and the induction is complete.

14-16. These problems are routine verifications.

17. Part (a) follows because $R \otimes_R A$ is naturally isomorphic to A. For (b), $F \otimes_R A \cong \bigoplus_{s \in S} (F_s \otimes_R A)$ and $1_F \otimes f$ corresponds to $\bigoplus (1_{F_s} \otimes f)$. The values of the various R homomorphisms are in the various spaces $F_s \otimes_R B$, whose sum is direct, and thus the kernel of $1_F \otimes f$ is the direct sum of the kernels. Then (b) follows. For (c), we see from (a) and (b) that free R modules are flat. In $\mathcal{C}_R$, every projective is a direct summand of a free module, and thus (c) follows by a second application of (b).

18. Consider $1 \otimes f : M \otimes_R A \to M \otimes_R B$. Any element of $\ker(1 \otimes f)$ is a finite sum $\sum m_i \otimes a_i$, and this lies in $\ker((1 \otimes f)\big|_{M_F})$, where F is the finite set of indices in question. Thus $\ker(1 \otimes f) \neq 0$ implies $\ker((1 \otimes f)\big|_{M_F}) \neq 0$ for some F. The

converse is immediate because $\ker((1 \otimes f)\big|_{M_F}) \subseteq \ker(1 \otimes f)$ for all F.

19. The long exact sequence for tensor product over R is of the form

$$\cdots \to \operatorname{Tor}_1^R(A, F) \to \operatorname{Tor}_1^R(A, B) \to A \otimes_R K \to A \otimes_R F \to A \otimes_R B \to 0,$$

and $\operatorname{Tor}_1^R(A, F) = 0$ because F is projective for $\mathcal{C}_R$. This establishes the exactness of the sequence in the problem. If A is flat, then

$$0 \to \operatorname{Tor}_1^R(A, B) \to A \otimes_R K \to A \otimes_R F \to A \otimes_R B \to 0$$

is exact for each B, and $\operatorname{Tor}_1^R(A, B)$ must be 0 for each B. Conversely if $\operatorname{Tor}_1^R(A, B)$ is 0 for each B, then $A \otimes_R (\cdot)$ is an exact functor by Proposition 4.3. Hence A is flat by definition.

20. On the one hand, the long exact sequence associated to tensoring the short exact sequence given in (a) by B is of the form

$$0 \to \operatorname{Tor}_1^R(M, B) \to \operatorname{Tor}_1^R(T(M), B) \to F \otimes_R B \to M \otimes_R B \to T(M) \otimes_R B \to 0,$$

since F free implies $\operatorname{Tor}_1^R(F, B) = 0$. On the other hand, the given short exact sequence splits, and tensoring it by B must directly produce a short exact sequence

$$0 \to F \otimes_R B \to M \otimes_R B \to T(M) \otimes_R B \to 0.$$

Thus $\ker(F \otimes_R B \to M \otimes_R B) = 0$, and we must therefore have

$$\operatorname{image}(\operatorname{Tor}_1^R(T(M), B) \to F \otimes_R B) = \ker(F \otimes_R B \to M \otimes_R B) = 0.$$

Consequently $0 \to \operatorname{Tor}_1^R(M, B) \to \operatorname{Tor}_1^R(T(M), B) \to 0$ is exact. This proves (a).

For (b), Problem 18 shows that M is flat if and only if each M_F is flat, and (a) in combination with Problem 19 shows that each M_F is flat if and only if each $T(M_F)$ is flat. Now suppose that M is flat, so that $T(M_F)$ is flat for each finite subset F of M. This is true in particular for each finite subset F' of $T(M)$, and $T(M_{F'}) = M_{F'} = (T(M))_{F'}$. Hence Problem 18 shows that $T(M)$ is flat. Conversely suppose that $T(M)$ is flat. Then $T(M)_{F'}$ is flat for each finite subset F' of $T(M)$. Let F be a finite subset of M. Then M_F is a finitely generated R submodule, and the structure theorem shows that $T(M_F)$ is finitely generated. Let F' be a set of generators for it. Then $T(M_F) = M_{F'} = T(M)_{F'}$. This is flat by Problem 18, since $T(M)$ is flat, and the first sentence of this paragraph allows us to conclude that M is flat.

For (c), $T(M) \neq 0$ means that $am = 0$ for some nonzero $a \in R$ and $m \in M$. Let $i : (a) \to R$ be the inclusion, which is one-one. Then $i \otimes 1 : (a) \otimes_R M \to R \otimes_R M \cong M$ has $(i \otimes 1)(a \otimes m) = am = 0$. Thus the one-one map i is carried to the map $i \otimes 1$ that is not one-one, and tensoring with M is not exact. So M is not flat.

For (d), if M is flat, then $T(M) = 0$ by (c). Conversely if $T(M) = 0$, then $T(M)$ is flat, and (b) shows that M is flat.

21. Since $\partial'_{p,q}$ and $\partial''_{p,q}$ both lower $p+q$ by 1, they both carry E_{p+q} to E_{p+q-1}. Also, the hypotheses give $(\partial'_{p,q}+\partial''_{p,q})^2 = \partial'_{p-1,q}\partial'_{p,q} + \partial'_{p,q-1}\partial''_{p,q} + \partial''_{p-1,q}\partial'_{p,q} + \partial''_{p,q-1}\partial''_{p,q} = 0$, and we have a chain complex.

22. We compute that $\partial'_{p-1,q}\partial'_{p,q} = (\alpha_{p-1}\otimes 1)(\alpha_p\otimes 1) = \alpha_{p-1}\alpha_p\otimes 1 = 0$, $\partial'_{p,q-1}\partial''_{p,q} + \partial''_{p-1,q}\partial'_{p,q} = (\alpha_{p-1}\otimes 1)(-1)^p(1\otimes\beta_q) + (-1)^{p-1}(1\otimes\beta_q)\times(\alpha_p\otimes 1) = (-1)^p(\alpha_p\otimes\beta_q) - (-1)^p(\alpha_p\otimes\beta_q) = 0$, and that $\partial''_{p,q-1}\partial''_{p,q} = (-1)^p(1\otimes\beta_{q-1})(-1)^p(1\otimes\beta_q) = 1\otimes\beta_{q-1}\beta_q = 0$.

23. The formulas for $\partial'_{p,q}$ and $\partial''_{p,q}$ show that $\ker\partial'_{p,q} = \ker\alpha_p\otimes_R D_q$ and that $\ker\partial''_{p,q} = C_p\otimes_R\ker\beta_q$. Since $\partial'_{p,q}E_{p,q}$ and $\partial''_{p,q}E_{p,q}$ lie in independent spaces, $\ker(\partial'_{p,q}+\partial''_{p,q}) = \ker\partial'_{p,q}\cap\ker\partial''_{p,q} = \ker\alpha_p\otimes_R\ker\beta_q$. Similarly $\partial'_{p+1,q}(E_{p+1,q}) = \alpha_{p+1}(C_{p+1})\otimes_R D_q$ and $\partial''_{p,q+1}(E_{p,q+1}) = C_p\otimes_R\beta_{q+1}(D_{q+1})$, and hence

$$\operatorname{image}(\partial'_{p+1,q}+\partial''_{p,q+1}) = \alpha_{p+1}(C_{p+1})\otimes_R D_q + C_p\otimes_R\beta_{q+1}(D_{q+1}).$$

Thus if c is in C_p, d is in D_q, c' is in $\alpha_{p+1}(C_{p+1})$, and d' is in $\beta_{q+1}(D_{q+1})$, then $(\partial'_{p,q}+\partial''_{p,q})\big((c+c')\otimes(d+d')\big)$ is the sum of $(\partial'_{p,q}+\partial''_{p,q})(c\otimes d)$ and three terms that are in $\operatorname{image}(\partial'_{p+1,q}+\partial''_{p,q+1})$. Consequently we obtain a well-defined homomorphism of $H_p(C)\otimes_R H_q(D)$ into $H_{p+q}(E)$.

24. Let ∂' and ∂'' be the boundary operators; these satisfy $\partial'\partial'' = -\partial''\partial'$. Let a be a cycle in $E_{-1,k}$, i.e., let $\partial''a = 0$. Since $\partial'a = 0$, the exactness for ∂' produces $c_{0,k}\in E_{0,k}$ with $a = \partial'c_{0,k}$. Since $\partial''a = 0$, this has $\partial'\partial''c_{0,k} = -\partial''\partial'c_{0,k} = -\partial''a = 0$. Now suppose inductively on $i\ge 0$ that $j\ge 0$ is defined by $i+j=k$ and that $c_{i,j}\in E_{i,j}$ is given with $\partial'\partial''c_{i,j} = 0$. By the assumed exactness, $\partial'\partial''c_{i,j} = 0$ implies $\partial''c_{i,j} = \partial'c_{i+1,j-1}$ for some $c_{i+1,j-1}\in E_{i+1,j-1}$, and then $\partial'\partial''c_{i+1,j-1} = -\partial''\partial'c_{i+1,j-1} = -\partial''\partial''c_{i,j} = 0$. The induction leads us nonuniquely to $c_{k,0}\in E_{k,0}$ such that $\partial'\partial''c_{k,0} = 0$. Define $b\in E_{k,-1}$ by $b = \partial''c_{k,0}$, and then $\partial'b = 0$. The result of the construction is therefore that we pass nonuniquely from the cocycle $a\in E_{-1,k}$ for ∂'' to a cocycle $b\in E_{k,-1}$ for ∂'.

Inverting the steps and the choices, we see that we can pass from b back to a. Thus if we can address the nonuniqueness, then the isomorphism in homology will have been established. We are to show that if $a\in E_{-1,k}$ at the start is a boundary relative to ∂'', then any system of choices leads to a result $b\in E_{k,-1}$ that is a boundary for ∂'. Since a is assumed to be a boundary for ∂'', $a = \partial''a'$ with $a'\in E_{-1,k+1}$. The element a' has $\partial'a' = 0$, and thus $a' = -\partial'a_{0,k+1}$ for some $a_{0,k+1}\in E_{0,k+1}$. Meanwhile, the above construction makes $a = \partial'c_{0,k}$. So $\partial'\partial''a_{0,k+1} = -\partial''\partial'a_{0,k+1} = \partial''a' = a = \partial'c_{0,k}$. By exactness, $c_{0,k} - \partial''a_{0,k+1} = \partial'b_{1,k}$ for some $b_{1,k}\in E_{1,k}$. This proves that $c_{0,k}$ is of the form $c_{0,k} = \partial''a_{0,k+1} + \partial'b_{1,k}$ with $a_{0,k+1}\in E_{0,k+1}$ and $b_{1,k}\in E_{1,k}$. (Note that this form for $c_{0,k}$ already implies that $\partial'\partial''c_{0,k} = 0$.)

Now suppose inductively on $i\ge 0$ that $j\ge 0$ is defined by $i+j=k$ and that $c_{i,j}\in E_{i,j}$ is given with $c_{i,j} = \partial''a_{i,j+1} + \partial'b_{i+1,j}$. The constructed element $c_{i+1,j-1}\in E_{i+1,j-1}$ has $\partial''c_{i,j} = \partial'c_{i+1,j-1}$ for some $c_{i+1,j-1}\in E_{i+1,j-1}$. Thus

$\partial' c_{i+1,j-1} = \partial''\partial' b_{i+1,j} = -\partial'\partial'' b_{i+1,j}$, and $c_{i+1,j-1} + \partial'' b_{i+1,j} = \partial' b_{i+2,j-1}$. If we put $a_{i+1,j} = -b_{i+1,j}$, then we have $c_{i+1,j-1} = \partial'' a_{i+1,j} + \partial' b_{i+2,j-1}$, and the induction goes through to $i = k$. Consequently any choice of $c_{k,0}$ obtained starting from the boundary a is of the form $c_{k,0} = \partial'' a_{k,1} + \partial' b_{k+1,0}$. The final step is to define $b = \partial'' c_{k,0}$, and then we have $b = \partial''\partial' b_{k+1,0} = -\partial'\partial'' b_{k+1,0}$, and b is exhibited as a boundary relative to ∂'.

25. Since each C_p is projective for $p \geq 0$, $C_p \otimes_R D$ is exact. Similarly $C \otimes_R D_q$ is exact for $q \geq 0$. The hypotheses of Problem 24 are satisfied, and the two homologies match.

26. $H_0(C) = H_0(C') = H_0(D) = \mathbb{Z}/2\mathbb{Z}$, and $H_p(C) = H_p(C') = H_p(D) = 0$ for $p \neq 0$. $H_0(C \otimes_{\mathbb{Z}} D) = H_0(C' \otimes_{\mathbb{Z}} D) = \mathbb{Z}/2\mathbb{Z}$, $H_1(C \otimes_{\mathbb{Z}} D) = 0$ and $H_1(C' \otimes_{\mathbb{Z}} D) = \mathbb{Z}/2\mathbb{Z}$, $H_p(C \otimes_{\mathbb{Z}} D) = H_p(C' \otimes_{\mathbb{Z}} D) = 0$ for $p \notin \{0, 1\}$.

27. Let $Z_p = \ker \partial'_p \subseteq C_p$, $B_p = \text{image}\, \partial'_{p+1} \subseteq C_p$, and $B'_p = B_{p-1}$. Since R is a principal ideal domain, Problem 20 shows that flat is equivalent to torsion free. Modules of the complex C are flat by assumption, hence torsion free. Modules of Z and B' are R submodules of these, hence are torsion free, hence are flat.

28. The long exact sequence in homology shows that

$$\text{Tor}_1^R(B', D) \to Z \otimes_R D \to C \otimes_R D \to B' \otimes_R D \to 0$$

is exact. Since B' is flat, Problem 19 shows that $\text{Tor}_1^R(B', D) = 0$.

29. For (a), the boundary map on $B'_p \otimes_R D_q$ in $B' \otimes_R D$ is $\partial' \otimes 1 + (-1)^p (1 \otimes \partial'')$, and $\partial' = 0$ on boundaries in B'_p.

For (b), tensoring with B' is an exact functor, since B' is flat. Therefore the exactness of $0 \to \overline{Z} \to D \xrightarrow{\partial''} \overline{B}' \to 0$ implies the exactness of

$$0 \to (B' \otimes_R \overline{Z})_n \to (B' \otimes_R D)_n \xrightarrow{(1 \otimes \partial'')_n} (B' \otimes_R \overline{B}')_n \to 0$$

for each n. From the exactness of this sequence, we can read off that $\ker(1 \otimes \partial'')_n$ within $(B' \otimes_R D)_n$ is $(B' \otimes_R \overline{Z})_n$ and that $\text{image}(1 \otimes \partial'')_n$ on $(B' \otimes_R D)_n$ is $(B' \otimes_R \overline{B}')_n$, which is the same thing as $(B' \otimes_R \overline{B})_{n-1}$.

For (c), the results of (b) show that

$$H_n(B' \otimes_R D) \cong \ker(1 \otimes \partial'')_n / \text{image}(1 \otimes \partial'')_{n+1} = (B' \otimes_R \overline{Z})_n / (B' \otimes \overline{B})_n.$$

Since tensoring with B' is exact, the exactness of $0 \to \overline{B} \to \overline{Z} \to H(D) \to 0$ implies the exactness of

$$0 \to B' \otimes_R \overline{B} \to B' \otimes_R \overline{Z} \to B' \otimes_R H(D) \to 0$$

in each degree. Thus $B' \otimes_R H(D) = (B' \otimes_R \overline{Z})/(B' \otimes_R \overline{B})$, and $H_n(B' \otimes_R D) \cong (B' \otimes H(D))_n = (B \otimes_R H(D)_{n-1}$.

Part (d) is handled in a fashion similar to (c).

30. For (a), $\operatorname{Tor}_1^R(Z, H(D)) = 0$ because Z is flat.

In (b), comparison of the exact sequence with $\ker \omega_{n-1}$ with the exact sequence displayed before part (a) (but with n replaced by $n-1$) shows that $\ker \omega_{n-1}$ is isomorphic to $\operatorname{Tor}_1^R(H(C), H(D))_{n-1}$. Substituting for $\ker \omega_{n-1}$ and incorporating the isomorphism into the mapping into $H_n(B' \otimes_R D)$ leads to β'_{n-1} as the one-one mapping.

In (c), we have

$$\begin{aligned}\operatorname{coker}(\iota \otimes 1) &= H_n(C \otimes_R D)/\operatorname{image}(\iota_n \otimes 1) = H_n(C \otimes_R D)/\ker(\partial'_n \otimes 1)\\ &\cong \operatorname{image}(\partial'_n \otimes 1) = \ker \omega_{n-1} \cong \operatorname{Tor}_1^R(H(C), H(D))_{n-1}.\end{aligned}$$

The composition of maps leading from $H_n(C \otimes_R D)$ to $H_n(B' \otimes_R D)$ has to be $\partial'_n \otimes 1$, and thus $\beta'_{n-1}\beta_{n-1} = \partial'_n \otimes 1$. The map β_{n-1}, apart from isomorphisms, is onto because q was constructed as onto.

Part (d) is completely analogous, and the resulting map α_n is one-one.

For (e), we know that α is one-one and that β is onto. Also, we have $\beta'_{n-1}\beta_{n-1}\alpha_n\alpha'_n = (\partial'_n \otimes 1)(\iota_n \otimes 1) = 0$. Since β'_{n-1} is one-one and α'_n is onto, $\beta_{n-1}\alpha_n = 0$. Finally suppose that x is in $\ker \beta_{n-1}$. Then x is in $\ker(\beta'_{n-1}\beta_{n-1}) = \ker(\partial'_n \otimes 1) = \operatorname{image}(\iota_n \otimes 1) = \operatorname{image}(\alpha_n\alpha'_n) = \operatorname{image} \alpha_n$. This completes the proof of exactness.

31. This is immediate.

32. Let $X = \{X_n\}$ and $Y = \{Y_n\}$. Then $\operatorname{Morph}(X, Y)$ is the subgroup of $\prod_{n=-\infty}^{\infty} \operatorname{Hom}(X_n, Y_n)$ consisting of those elements in the product satisfying the chain map conditions. A zero object is any tuple of 0's, and certainly product and coproduct make sense. One readily verifies that the tuple of kernels of a chain map furnishes a kernel for a chain map and that the tuple of cokernels furnishes a cokernel.

33. The additional objects and morphisms at the top of the extended diagram are $C_0 = 2\mathbb{Z}/8\mathbb{Z}$, $B_0 = \mathbb{Z}$, k given by 2 mod 8 $\mapsto$ 2 mod 8, $\widetilde{k}$ given by $\times 2$, $\widetilde{\psi}$ given by $1 \mapsto 2$ mod 8, and $\widetilde{\varphi}$ given by $\times 4$. Since the composition of $\widetilde{k}$ followed by $\beta = \times 2$ is not 0, $(B_0, \widetilde{k})$ cannot be the kernel of β.

The additional objects and morphisms at the bottom of the extended diagram are $A'_0 = \mathbb{Z}/4\mathbb{Z}$, $B'_0 = \mathbb{Z}/16\mathbb{Z}$, p given by $1 \mapsto 1$ mod 4, $\widetilde{p}$ given by $1 \mapsto 1$ mod 16, $\widetilde{\varphi}'$ given by 1 mod 4 $\mapsto$ 4 mod 16, and $\widetilde{\psi}'$ given by 1 mod 16 $\mapsto$ 1 mod 4.

34. We give the argument only for $\operatorname{Hom}(M, \cdot)$. Let $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ be a given exact sequence, and form the sequence

$$0 \longrightarrow \operatorname{Hom}(M, A) \xrightarrow{\operatorname{Hom}(1,\varphi)} \operatorname{Hom}(M, B) \xrightarrow{\operatorname{Hom}(1,\psi)} \operatorname{Hom}(M, C).$$

We are to show that $\operatorname{Hom}(1, \varphi)$ is one-one and that exactness holds at $\operatorname{Hom}(M, B)$.

If σ is in $\operatorname{Hom}(M, A)$ with $\operatorname{Hom}(1, \varphi)(\sigma) = 0$, then $\varphi\sigma = 0$, and it follows that $\sigma = 0$ because φ is a monomorphism.

For the exactness at $\operatorname{Hom}(M, B)$, we use Theorem 4.42e. We know immediately that $\operatorname{Hom}(1, \psi)\operatorname{Hom}(1, \varphi) = \operatorname{Hom}(1, \psi\varphi) = \operatorname{Hom}(1, 0) = 0$. Thus suppose that

$\tau \in_m \mathrm{Hom}(M, B)$ has $\mathrm{Hom}(1, \psi)\tau \equiv 0$. This condition means that $\psi\tau \equiv 0$. Since the given sequence is exact, Theorem 4.42e produces some $\tau' \in_m A$ with $\varphi\tau' \equiv \tau$. In turn, this says that $\mathrm{Hom}(1, \varphi)\tau' \equiv \tau$. By Theorem 4.42, we have exactness at $\mathrm{Hom}(M, B)$.

35. We give the proof only that the splitting of exact sequences as indicated implies that P is projective. Thus suppose that a morphism $\tau \in \mathrm{Hom}(P, B)$ and an epimorphism $\psi \in \mathrm{Hom}(C, B)$ are given. We are to produce $\sigma \in \mathrm{Hom}(P, C)$ with $\tau = \psi\sigma$. Let $(W, \widetilde{\psi}, \widetilde{\tau})$ be a pullback of (ψ, τ). Then $\tau\widetilde{\psi} = \psi\widetilde{\tau}$, and Proposition 4.40 shows that $\widetilde{\psi}$ is an epimorphism. Then it follows that

$$0 \to \mathrm{domain}(\ker\widetilde{\psi}) \xrightarrow{\ker\widetilde{\psi}} W \xrightarrow{\widetilde{\psi}} P \to 0$$

is exact, and it must split by assumption. Thus there exists $\rho \in \mathrm{Hom}(P, W)$ with $\widetilde{\psi}\rho = 1_P$. Put $\sigma = \widetilde{\tau}\rho$. Then $\psi\sigma = \psi\widetilde{\tau}\rho = \tau\widetilde{\psi}\rho = \tau 1_P = \tau$, as required.

Chapter V

1. If ξ is a root of $F(X)$, then the given formula shows that $D(\xi)$ is -23 and -31 in the two cases. These contain no square factor and therefore equal $D_{\mathbb{K}}$ in the two cases.

2. For (a), let $G(X) = F(X + \frac{2}{3}) = X^3 - \frac{4}{3}X + \frac{22}{27}$. Then $F(X)$ and $G(X)$ have the same discriminant, and the discriminant for $G(X)$ is given by the formula of Problem 1. It is -44.

For (b), let $x = a + b\xi + c\xi^2$ be given with a, b, c all in $\{0, 1\}$. The matrix of left-by-x in the ordered basis $(1, \xi, \xi^2)$ works out to be

$$\begin{pmatrix} a & -2c & -2b-4c \\ b & a & -2c \\ c & b+2c & a+2b+4c \end{pmatrix},$$

and the determinant of it is

$$a^3 + 2a^2(b + 4c) + 4c^3 - 2b(b + 2c)^2 + 4ac(b + 2c) + 2bc(a + 2b + 4c).$$

For x to be twice an algebraic integer, this determinant, which is the norm of x, has to be $\equiv 0 \bmod 8$. All the terms are even except possibly the first, and thus a has to be even. That is, $a = 0$. The determinant then reduces to $4c^3 - 2b(b+2c)^2 + 4bc(b+2c)$. All terms here are divisible by 4 except possibly $-2b^2$. Thus b must be even. That is, $b = 0$. The determinant reduces in this case to $4c^3$. For this to be divisible by 8, c must be even. That is, $c = 0$. Proposition 5.2 consequently says that a further factor of 2^2 cannot be eliminated from the discriminant.

3. For (a), Theorem 5.21 and the remarks after it show that every equivalence class contains an ideal whose norm is $< (0.283)D_{\mathbb{K}}^{1/2}$. Proposition 5.8 shows that $D_{\mathbb{K}} = 3^5 = 243$. Thus every equivalence class contains an ideal with norm ≤ 4.

Conclusion (b) is immediate from Theorem 5.6 with $F(X) = X^3 - 3$. Conclusion (c) follows because $(\sqrt[3]{3}-1)(\sqrt[3]{9}+\sqrt[3]{3}+1) = (\sqrt[3]{3})^3 - 1 = 3-1 = 2$. Conclusion (d) is immediate from Proposition 5.10d.

For (e), any nonzero ideal is the product of powers of prime ideals associated with the various prime numbers. The ones corresponding to the prime numbers 2 and 3 are principal ideals by (b), (c), and (d). These are the only ones that need to be checked, according to (a). Thus every nonzero ideal is principal.

4. Conclusion (a) is immediate from Theorem 5.6, since $X^3 - 7$ factors modulo 2 as $(X + 1)(X^2 + X + 1)$. For (b), we show that no element $x = a + b\sqrt[3]{7} + c\sqrt[3]{49}$ has norm ± 2. Left multiplication by x carries 1 to $a + b\sqrt[3]{7} + c\sqrt[3]{49}$, carries $\sqrt[3]{7}$ to $7c + a\sqrt[3]{7} + b\sqrt[3]{49}$, and carries $\sqrt[3]{49}$ to $7b + 7c\sqrt[3]{7} + a\sqrt[3]{49}$. Thus its matrix is

$$\begin{pmatrix} a & 7c & 7b \\ b & a & 7c \\ c & b & a \end{pmatrix}.$$

The determinant is $a^3 + 49c^3 + 7b^3 - 21abc$, which is congruent modulo 7 to a^3. Modulo 7, the cubes are 0 and ± 1, and thus the congruence $a^3 \equiv \pm 2 \bmod 7$ has no solution.

5. Since the element $\sqrt{-1} + \sqrt{-5}$ has degree 4 over $\mathbb{Q}$, the minimal polynomial has degree 4. The product of $(X - (+\sqrt{-1} + \sqrt{-5}))$ and the Galois transforms $(X - (+\sqrt{-1} - \sqrt{-5}))$, $(X - (-\sqrt{-1} + \sqrt{-5}))$, and $(X - (-\sqrt{-1} - \sqrt{-5}))$ is $X^4 + 12X^2 + 16$, which is in $\mathbb{Z}[X]$.

6. The minimal polynomial of $\xi = \frac{1}{2}(\sqrt{-1}+\sqrt{-5})$ is $H(X) = X^4 + 2^{-2}12X^2 + 2^{-4}16 = X^4 + 3X^2 + 1$ with $|D(\xi)| = |N_{\mathbb{K}/\mathbb{Q}}(H'(\xi))|$. Here $H'(X) = 4X^3 + 6X = 2(2X^2 + 3)$. Since $\xi^4 + 3\xi^2 + 1 = 0$, we have $\xi^2 = -\frac{3}{2} \pm \frac{1}{2}\sqrt{5}$; thus $2\xi^2 + 3 = \pm\sqrt{5}$. So $|D(\xi)| = |N_{\mathbb{L}/\mathbb{Q}}(\pm 2\sqrt{5})|$. The four conjugates of $\sqrt{5}$ are $+\sqrt{5}$ twice and $-\sqrt{5}$ twice, and the norm is the product of the four conjugates. Thus $|D(\xi)| = |N_{\mathbb{L}/\mathbb{Q}}(\pm 2\sqrt{5})| = 2^4 5^2$.

7. These follow immediately by applying Theorem 5.6 to the indicated prime, 2 or 5, and the respective polynomials: $X^2 + 5$, $X^2 + X - 1$, and $X^2 + 1$.

8. With $\mathbb{Q} \subseteq \mathbb{K}' \subseteq \mathbb{L}$, the (e, f, g) for $\mathbb{L}/\mathbb{Q}$ has to be entry by entry $\ge$ the triple for $\mathbb{K}'/\mathbb{Q}$. The triple for $\mathbb{K}'/\mathbb{Q}$ is given in Problem 7b as (1, 2, 1) for $p = 2$. Similarly from $\mathbb{Q} \subseteq \mathbb{K}'' \subseteq \mathbb{L}$, the (e, f, g) for $\mathbb{L}/\mathbb{Q}$ has to be $\ge (2, 1, 1)$. Thus $e \ge 2$, $f \ge 2$, and $g \ge 1$. Since $efg = 4$, equality must hold throughout: $(e, f, g) = (2, 2, 1)$.

This proves (a). Similarly for (b), we must have $(e, f, g) \ge (2, 1, 1)$ and $(e, f, g) \ge (1, 1, 2)$. Thus $(e, f, g) \ge (2, 1, 2)$. Since $efg = 4$, $(e, f, g) = (2, 1, 2)$.

9. In (a), Problem 8a shows that $(2)T = P^2$, and we know that $(2)R = \wp_2^2$. Then $P^2 = (2)T = (2)RT = \wp_2^2 T = (\wp_2 T)(\wp_2 T)$. Since P is prime, P divides $\wp_2 T$. For the equality $P^2 = (\wp_2 T)^2$ to hold, we must have $P = \wp_2 T$.

Similarly $(5)T = P_1^2P_2^2$ and $(5)R = \wp_5^2$. Then $P_1^2P_2^2 = (5)T = (5)RT = \wp_5^2T = (\wp_5T)^2$. Since P_1 and P_2 are prime, P_1 and P_2 must divide $\wp_5T$. Therefore $P_1P_2 = \wp_5T$.

In (b), conclusion (a) shows that no prime ideal of R that divides $(2)R$ or $(5)R$ ramifies in T. Since $D(\xi)$ is divisible by no prime numbers other than 2 and 5, Theorem 5.6 shows that no prime ideal (p) of $\mathbb{Z}$ ramifies in T. Hence no prime ideal of R containing such a prime (p) of $\mathbb{Z}$ ramifies in T.

10. Roots of unity must map to roots of unity under the embedding, and there are only two roots of unity within $\mathbb{R}$. Hence there are no real-valued embeddings when $p > 2$. Thus the embeddings come in complex-conjugate pairs. The product $\sigma(x)\overline{\sigma}(x)$ is positive for $x > 0$, and $N_{\mathbb{K}/\mathbb{Q}}(x)$ is the product of these expressions over all such pairs.

11. For (a), $F(X)$ is the minimal polynomial of ζ^k when $\mathrm{GCD}(k, p) = 1$. Then $\zeta^k - 1$ is a root of $G(X) = F(X + 1)$ of the correct degree, and therefore $G(X)$ is the minimal polynomial of $\zeta^k - 1$. If $H(X)$ is the field polynomial of an element η, then $N_{\mathbb{K}/\mathbb{Q}}(\eta) = (-1)^{[\mathbb{K}:\mathbb{Q}]}H(0)$. In this instance $[\mathbb{K} : \mathbb{Q}] = p - 1$ is even. Taking $\eta = \zeta^k - 1$, we obtain $N_{\mathbb{K}/\mathbb{Q}}(\zeta^k - 1) = G(0) = F(1) = p$.

For (b), $\zeta - 1$ divides $\zeta^k - 1$, and hence the quotient is in R. If l is chosen with $lk \equiv 1 \bmod p$, then $\zeta - 1 = \zeta^{lk} - 1$, and $\zeta^k - 1$ divides $\zeta^{lk} - 1$. Therefore the reciprocal of $(\zeta^k - 1)/(\zeta - 1)$ is in R.

12. With $F(X)$ and $G(X)$ as in the previous problem, $F'(\zeta^k) = G'(\zeta^k - 1)$. Here $F(X) = (X^p - 1)/(X - 1)$ makes $G(X) = X^{-1}[(X + 1)^p - 1]$ and $G'(X) = X^{-2}[pX(X + 1)^{p-1} - (X + 1)^p + 1]$. Since $\zeta^{kp} = 1$,

$$F'(\zeta^k) = G'(\zeta^k - 1) = (\zeta^k - 1)^{-2}[p(\zeta^k - 1)\zeta^{k(p-1)} - \zeta^{kp} + 1] = (\zeta^k - 1)^{-1}p\zeta^{k(p-1)}.$$

The result now follows from the formula $\mathcal{D}(\zeta^k) = F'(\zeta^k)$.

13. Continuing from the previous problem gives

$$N_{\mathbb{K}/\mathbb{Q}}(F'(\zeta^k)) = N_{\mathbb{K}/\mathbb{Q}}(\zeta^k - 1)^{-1}p^{p-1}N_{\mathbb{K}/\mathbb{Q}}(\zeta^{k(p-1)}) = p^{p-2}.$$

The result follows from the computation $(-1)^{(p-1)(p-2)/2}D(\zeta^k) = N_{\mathbb{K}/\mathbb{Q}}(\mathcal{D}(\zeta^k)) = N_{\mathbb{K}/\mathbb{Q}}(F'(\zeta^k)) = p^{p-2}$.

14. For (a), we have $\lambda^k = (1 - \zeta)^k = \sum_{j=0}^k (-1)^j \binom{k}{j} \zeta^j$ and $\zeta^k = (1 - \lambda)^k = \sum_{j=0}^k (-1)^j \binom{k}{j} \lambda^j$. Conclusion (b) is a version of Problem 11b because the conjugates of ζ are the powers ζ^j for $1 \le j \le p - 1$. For (c), we have $p = \prod_{k=1}^{p-1}(1 - \zeta^k) = \prod_{k=1}^{p-1}(1-\zeta)u_k = (1-\zeta)^{p-1}\prod_{k=1}^{p-1}u_k$, where $u_k = (1-\zeta^k)/(1-\zeta)$. Each element u_k is a unit by Problem 11c, and (c) follows.

15. The identity $(p)R = (1 - \zeta)^{p-1}$ is immediate from Problem 14c. The extension $\mathbb{K}/\mathbb{Q}$ being Galois, we know that the prime decomposition of the ideal

$(p)R$ is of the form $(p)R = P_1^e \cdots P_g^e$, where $p - 1 = efg$ and f is the common value of all $\dim_{\mathbb{F}_p}(R/P_j)$. This latter fact says that no factorization of $(p)R$ into proper ideals can have more than $p - 1$ factors, and $p - 1$ factors occur only if all factors are prime. In this case, $(1 - \zeta)$ is a proper ideal because $N_{\mathbb{K}/\mathbb{Q}}(1 - \zeta) = p$. Thus each factor $(1 - \zeta)$ is prime.

16. Following Proposition 5.2, suppose that a_j is an integer for each j with $s \le j \le k$ such that $0 \le a_j \le p - 1$, $a_s \ne 0$, $a_k = 1$, and

$$a_s\lambda^s + a_1\lambda^{s+1} + a_2\lambda^{s+2} + \cdots + a_{k-1}\lambda^{k-1} + a_k\lambda^k = pr$$

with r in R. Subtracting all terms from the left side but the first and applying Problem 15 shows that $a_s\lambda^s$ lies in $(\lambda)^{s+1}$. Thus $(a_s)(\lambda)^s \subseteq (\lambda)^{s+1}$. Canceling gives $(a_s) \subseteq (\lambda)$, and this inclusion is a contradiction because $\mathrm{GCD}(N((a_s)), N((\lambda))) = 1$.

17. Each step toward a $\mathbb{Z}$ basis multiplies a discriminant by a square, and it is enough to prove that a primitive element ξ for $\mathbb{K}/\mathbb{Q}$ lying in R has $\operatorname{sgn} D(\xi) = (-1)^{r_2}$. We are thus to compute the sign of $\prod_{i<j}(\sigma_i(\xi) - \sigma_j(\xi))^2$. For a given pair (i, j), the factor $(\sigma_i(\xi) - \sigma_j(\xi))^2$ is matched by its complex conjugate elsewhere in the product unless σ_i and σ_j are both real or are complex conjugates of one another. The factor and its mate have a positive product, and pair with σ_i and σ_j both real contributes a positive square. If $\sigma_j = \overline{\sigma}_i$, then $\sigma_i(\xi) - \sigma_j(\xi)$ is purely imaginary, and its square is negative. Hence the sign is $(-1)^{r_2}$.

18. Let g be in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$. Replacing each σ_j by $g\sigma_j$ has the effect of permuting the columns of $[\sigma_j(\alpha_i)]$. If the permutation is even, then the terms contributing to P are the same before and after the permutation; otherwise they are interchanged. In either case, $P + N$ and PN are fixed. Since $P + N$ and PN are fixed by the Galois group, they are in $\mathbb{Q}$. The entries $\sigma_j(\alpha_i)$ of the matrix are in R, and thus P and N are in R. Consequently $P + N$ and PN are in $\mathbb{Z}$. The formula $D(\Gamma) = (P + N)^2 - 4PN$ shows that $D(\Gamma) \equiv (P + N)^2 \bmod 4$. Any square of a member of $\mathbb{Z}$ is congruent to 0 or 1 modulo 4, and the result follows.

19. Let J be an ideal of $S^{-1}R$. Proposition 8.47 of *Basic Algebra* shows that $I = R \cap J$ is an ideal in R and that $J = S^{-1}I$. Since $I_1, \ldots, I_h$ is a complete set of representatives for the equivalence classes, $aI = bI_j$ for some j with $1 \le j \le h$. Let $(a)_S$ and $(b)_S$ be the principal ideals of $S^{-1}R$ generated by a and b. The fact that u is in $I_j \cap S$ means that $S^{-1}I_j = S^{-1}R$, and thus

$$\begin{aligned}(a)_S J &= S^{-1}(a)S^{-1}I = S^{-1}(a)I = S^{-1}(b)I_j \\ &= S^{-1}(b)S^{-1}I_j = S^{-1}(b)S^{-1}R = (b)_S.\end{aligned} \tag{$*$}$$

Hence J is principal. (In fact, the equality shows that $aj = b$ for some $j \in J$. Hence $ba^{-1} = j$ is an element of $J \subseteq S^{-1}R$, the principal ideal $(ba^{-1})_S$ of $S^{-1}R$ is meaningful, and $(ba^{-1})_S \subseteq J$. For the reverse inclusion let $j \in J$ be given, and use $(*)$ to write $aj = bx$ with $x \in S^{-1}R$. Then $j = (ba^{-1})x$ shows that j is in $(ba^{-1})_S$, and $J \subseteq (ba^{-1})_S$.)

20. For (a), write $ab = u^k$. Then $a^{-1} = u^{-k}b$ exhibits a^{-1} as in $S^{-1}R$. For (b), if $u^{-m}a$ is a unit in $S^{-1}R$, then $u^{-m}a^{-1} = u^{-l}c$ for some $c \in R$. Hence $ac = u^{l-m}$. Since ac is in R and u is not, $l - m = k$ with $k \geq 0$. Then a divides u^k.

21. For (a), write $(u) = P_1^{e_1} \cdots P_l^{e_l}$. Then $(u^h) = (P_1^h)^{e_1} \cdots (P_l^h)^{e_l} = (b_1^{e_1} \cdots b_l^{e_l})$. Thus $u^h = b_1^{e_1} \cdots b_l^{e_l}\varepsilon$ for some unit ε in R, each b_j divides u^h, and the conclusion follows from Problem 20a.

For (b), we have $(a)(b) = (u)^k = P_1^{ke_1} \cdots P_l^{ke_l}$. Since a and b are in R, this equality implies that $(a) = P_1^{r_1} \cdots P_l^{r_l}$. For each j, use the division algorithm to write $r_j = n_j h + t_j$ with $0 \leq t_j < h$. Then $P_j^{r_j} = (P_j^h)^{n_j} P_j^{t_j} = (b_j)^{n_j} P_j^{t_j}$, and consequently $(a) = (d)P_1^{t_1} \cdots P_l^{t_l}$ as required, where $d = \prod_{j=1}^{l} b_j^{n_j}$.

The argument for (c) was given in parentheses at the end of the solution of Problem 19.

22. Because of Problem 21d, we now have $(a) = (d)(c_i)$. Thus $a = dc_i\varepsilon$ for some unit ε in R. Since $u^k = ab = c_i db\varepsilon$, c_i divides u^k and is a unit in $S^{-1}R$ by Problem 20a.

23. Problem 22 shows that any unit of $S^{-1}R$ is a product of a power of u by a product $\prod_{j=1}^{l} b_j^{n_j}$, an element c_i, and a unit ε of R. Problem 21a shows that each b_j is a unit in $S^{-1}R$, and Problem 22 shows that each c_i is a unit in $S^{-1}R$. Thus $(S^{-1}R)^\times$ is generated by u, the finitely many elements b_j and c_i, and a finite set of generators of $R^\times$. (The group $R^\times$ is finitely generated by the Dirichlet Unit Theorem.)

24. $G(4/\xi) = (64\xi^{-3} - 16\xi^{-2} + 8\xi^{-1} + 8) = 8\xi^{-3}(\xi^3 + \xi^{-2} - 2\xi + 8) = 8\xi^{-3}F(\xi) = 0$. The element η is in $\mathbb{K}$, and it is exhibited as the root of a monic polynomial in $\mathbb{Z}[X]$; therefore it is in R.

25. For (a), $0 = F(\xi)/\xi = \xi^2 + \xi - 2 + 8\xi^{-1} = \xi^2 + \xi - 2 + 2\eta$. For (b), $0 = G(\eta)/\eta = \eta^2 - \eta + 2 + 8/\eta = \eta^2 - \eta + 2 + 2\xi$. Solving the first equation for ξ^2 gives the first formula in the table, and solving the second equation for η^2 gives the second formula in the table. The formula $\xi\eta = 4$ is immediate from the definition $\eta = 4/\xi$. The formulas in the table together show that any integer polynomial in ξ and η reduces to a $\mathbb{Z}$ combination of 1, ξ, and η.

Conclusion (c) is clear. For (d), we have $\eta = 1 - \frac{1}{2}(\xi^2 + \xi)$, and this is not in $\mathbb{Z}(\{1, \xi, \xi^2\})$. For (e), we have $D((1, \xi, \xi^2)) = -2^2 \cdot 503$. Since the only square factor is 2^2, it follows that $\mathbb{Z}(\{1, \xi, \xi^2\})$ has index 2 in $\mathbb{Z}(\{1, \xi, \eta\})$ and that $D((1, \xi, \eta)) = -503$. This latter discriminant is square free and thus cannot be reduced further. Therefore $D_{\mathbb{K}} = -503$, and $\{1, \xi, \eta\}$ is a $\mathbb{Z}$ basis of R. Finally the formula $\eta = 1 - \frac{1}{2}(\xi^2 + \xi)$ shows that $\mathbb{Z}(\{1, \xi, \eta\}) = \mathbb{Z}(\{1, \xi, \frac{1}{2}(\xi^2 + \xi)\})$.

26. Application of φ to $\xi^2 = \xi + 2 - 2\eta$ gives $\overline{\xi}^2 = \overline{\xi}$. Similarly $\overline{\eta}^2 = \overline{\eta}$. The elements of a finite field of characteristic 2 fixed by the squaring map are 0 and 1. Hence $\overline{\xi}$ and $\overline{\eta}$ are in $\{0, 1\}$. Since $\mathbb{F} = \varphi(R)$ is generated by the values of φ on 1, ξ, and η, $\mathbb{F}$ has two elements. From $\xi\eta = 4$, it follows that $\overline{\xi}\,\overline{\eta} = 0$. Thus $\overline{\xi}$ and $\overline{\eta}$ cannot both be 1, and the only possibilities are the ones in the table.

27. Define $\varphi : R \to \mathbb{F}_2$ on ξ and η by one of the lines of the table of Problem 26, and set $\varphi(1) = 1$. Then φ extends to a well-defined additive homomorphism on $\mathbb{Z}(\{1, \xi, \eta\})$. We have to check that φ respects multiplication. It is enough to do so on additive generators. Thus we have to check that $\varphi(\xi^2) = (\varphi(\xi))^2$, that $\varphi(\eta^2) = (\varphi(\eta))^2$, and that $\varphi(\xi\eta) = (\varphi(\xi))(\varphi(\eta))$. Thus, for example, in the first one we want $-\varphi(\xi) + 2\varphi(1) - 2\varphi(\eta) = (\varphi(\xi))^2$. If we write the values of φ as triples corresponding to the three possible φ's, the left side is $-(0, 1, 0) + 2(1, 1, 1) - 2(0, 0, 1) \equiv (0, 1, 0) \bmod 2$, while the right side is $(0, 1, 0)^2 \equiv (0, 1, 0) \bmod 2$. These match, and this relation is verified. The other two relations are verified in similar fashion.

28. The norm of a kernel equals the number of elements in the image of the homomorphism, which is 2 in each case. Since each ideal has prime norm, the ideal is prime. Moreover, these ideals contain $(2)R$ and hence all figure into the prime factorization of $(2)R$. On the other hand, we must have $\sum e_i f_i = 3$ for the decomposition, and we have seen that there are at least three terms. So there are exactly three terms, and we must have $e_i = f_i = 1$ in each case. Therefore $(2)R = P_{0,0}P_{1,0}P_{0,1}$.

29. For (a), the elements listed are additive generators of the ideal in each case, and hence they are also ideal generators. For (b), $\eta = \eta(\xi + 1) - 2 \cdot 2$ shows that η is in the ideal $(2, \xi + 1)$. Thus $(2, \xi + 1, \eta) \subseteq (2, \xi + 1)$. The reverse inclusion is clear. In (c), the argument for $(2, \eta + 1)$ is completely symmetric. Let us see that $(2, \xi, \eta) = (2, \xi - \eta)$. The inclusion $\supseteq$ is clear. For the inclusion $\subseteq$, we use the two formulas

$$(-1 - \eta)2 + (-\xi)(\xi - \eta) = -2 - 2\eta - (-\xi + 2 - 2\eta) + 4 = \xi,$$
$$(3 + \xi)2 + (-\eta)(\xi - \eta) = 6 + 2\xi - 4 + (-2\xi - 2 + \eta) = \eta.$$

30. For (a), the field polynomial of $\theta - q$ is $H(X + q)$, and so the norm of $\theta - q$ is $-H(0+q)$, as required. In (b), the first two formulas come from the field polynomials $F(X)$ and $G(X)$ of ξ and η, and the other formulas follow from (a).

In (c), the fact that $N((\xi)) = |N_{\mathbb{L}/\mathbb{Q}}(\xi)| = 8$ shows that the prime factorization of (ξ) is into prime ideals whose norms are powers of two. Problem 28 shows that all such ideals have been identified, and thus $(\xi) = P_{0,0}^a P_{1,0}^b P_{0,1}^c$ for some exponents ≥ 0. Comparing norms shows that $a + b + c = 3$. Similar remarks apply to (η).

In (d), use of Problem 28 shows that $P_{0,0}^2 P_{1,0}^2 P_{0,1}^2 = ((2)R)^2 = (4)R = (\xi)(\eta) = P_{0,0}^{a+\alpha} P_{1,0}^{b+\beta} P_{0,1}^{c+\gamma}$. Then $a+\alpha = 2$, $b+\beta = 2$, and $c+\gamma = 2$ by unique factorization.

For (e), we observe from the kernels, or else we see from Problem 29a, that ξ is not in $P_{1,0}$ and that η is not in $P_{0,1}$. Hence $P_{1,0}$ does not appear in the prime factorization of (ξ), and $P_{0,1}$ does not appear in the prime factorization of (η). Therefore $b = \gamma = 0$.

For (f), the results of (e) and (d) combine to show that $a + \alpha = 2$, $\beta = 2$, and $c = 2$. Since $a + c = 3$ and $\alpha + \beta = 3$, $a = \alpha = 1$.

31. For (a), we see immediately from Problem 29a that $\xi + l$ lies in $P_{1,0}$ but not in $P_{0,0}$ and not in $P_{0,1}$. For (b), the formula $|N_{\mathbb{K}/\mathbb{Q}}(\xi + 3)| = 2^2$ shows that

$(\xi + 3)$ is the product of exactly two of the prime ideals of norm 2; thus (a) implies that $(\xi + 3) = P_{1,0}^2$. Similarly $|N_{\mathbb{K}/\mathbb{Q}}(\xi - 1)| = 2^3$, and (a) gives $(\xi - 1) = P_{1,0}^3$. Conclusion (c) is immediate from Problem 29a.

For (d), we have $(2)R \subseteq (2, \xi)$; thus $(2, \xi)$ is of the form $P_{0,0}^a P_{1,0}^b P_{0,1}^c$ with $a + b + c \leq 3$. Since ξ is not in $P_{1,0}$, $b = 0$. Since ξ is in $P_{0,0}$ and $P_{0,1}$, we must have $a > 0$ and $c > 0$. Since the inclusion $(2)R \subseteq (2, \xi)$ is proper $\big($because ξ is not in $(2)R = 2\mathbb{Z}(\{1, \xi, \eta\})\big)$, $N((2, \xi)) \leq 4$. Thus $a = c = 1$, and $(2, \xi) = P_{0,0}P_{0,1}$.

For (e), Problem 29a shows that $P_{0,1} = (2, \xi, \eta + 1)$. Thus $P_{0,1}^2$ contains 4 and $\xi(\eta + 1) = 4 + \xi$, hence ξ. If $P_{0,1}^2$ contains also $\xi + l$ with $l \equiv 2 \bmod 4$, then it contains $\xi + 2$, hence 2. This would mean that $P_{0,1}^2 \supseteq (2, \xi) = P_{0,0}P_{0,1}$. Since $P_{0,1}^2$ and $P_{0,0}P_{0,1}$ both have norm 4, they would have to be equal, and we would obtain $P_{0,1} = P_{0,0}$, contradiction.

For (f), Problem 30b gives $N((\xi + 2)) = 8$. In view of (c), $(\xi + 2) = P_{0,0}^a P_{0,1}^c$ with $a + c = 3$ and $c \geq 1$. Part (d) shows that $c \leq 1$. Thus $(\xi + 2) = P_{0,0}^2 P_{0,1}$. The argument for $(\xi - 2)$ is similar.

32. For (a), this kind of argument is done in a parenthetical remark at the end of the solution of Problem 19. For (b), we have $(\xi + 2) = r_{0,0}^2 P_{0,1}$ and $(\xi - 1) = P_{1,0}^3 = (\xi + 3)P_{1,0}$. Thus the same kind of argument shows that $P_{0,1}$ and $P_{1,0}$ are principal.

For (c), we factor $X^3 + X^2 - 2X + 8$ modulo 3; there is no root in $\mathbb{F}_3$, and hence the reduced polynomial is irreducible. By Theorem 5.6 the only prime ideal whose norm is a power of 3 has norm 3^3.

For (d), we factor $X^3 + X^2 - 2X + 8$ modulo 5 as $(X + 1)(X^2 - 2)$, and Theorem 5.6 gives us one prime ideal of norm 5 and one of norm 5^2. The one of norm 5, according to the theorem, is $(2, 1 + \xi)$. For (e), the technique of Problem 30a shows that $N((1 + \xi)) = 10$. Thus the only possibility for the prime factorization of $(1 + \xi)$ is as $(2, 1 + \xi)P$, where P is one of the three ideals of norm 2. For (f), since $(1 + \xi)$ and P are principal, $(2, 1 + \xi)$ is principal, by the same technique as in earlier parts.

For (g), the prime factorization of nonzero ideals allows us to conclude that every nonzero ideal of norm ≤ 6 is principal. Application of the technique after Theorem 5.21 shows that every ideal class has a representative with norm < 6.35, hence norm ≤ 6. All such ideals are principal, and therefore R is a principal ideal domain.

Chapter VI

1. Apply the Cauchy criterion. Since $|a_n + a_{n+1} + \cdots + a_m|_p \leq \max_{n \leq k \leq m} |a_k|_p$, the series is Cauchy, hence convergent, if and only if the terms tend to 0.

2. In (a), the equality $\mathrm{GCD}(3, 2^n) = 1$ implies that there exist integers x_n and y_n such that $3x_n - 2^n y_n = 1$. Then $x_n - \frac{1}{3} = 2^n 3^{-1} y_n$. Applying the 2-adic absolute value gives $|x_n - \frac{1}{3}|_2 = 2^{-n}|y_n|_2 \leq 2^{-n}$, and this tends to 0. For example take $x_n = \frac{1}{3}(2^{2n-1} + 1)$. In (b), the argument with $\frac{a}{b}$ replacing $\frac{1}{3}$ is similar: to get

$|x - \frac{a}{b}|_2 \le 2^{-n}$, start by finding x and y with $bx - 2^n y = a$.

3. Write ideles as tuples indexed by $\infty, 2, 3, 5, \dots$. If q is in $\mathbb{Q}$, then $\iota(q) = (q, q, q, q, \dots)$. If this is to be in $\mathbb{R}^\times \times \prod_p \mathbb{Z}_p^\times$, then the only restriction on the first coordinate is that $q \ne 0$, but the other coordinates are restricted by $|q|_p = 1$ for all primes p. This means that q in lowest terms has no p in either the numerator or the denominator. So $q = \pm 1$. This proves (a).

In (b), let $(x_\infty, x_2, x_3, \dots)$ be in $\mathbb{I}$. Since $|x_p|_p \ne 1$ for only finitely many p, there exists a unique positive rational q such that $|q|_p = |x_p|_p$ for all p. Define $z_p = x_p q^{-1}$ as a member of $\mathbb{Q}_p^\times$. Then $|z_p|_p = |x_p|_p |q|_p^{-1} = 1$ shows that $|z_p|_p = 1$ for all p. Finally define $r = x_\infty q^{-1}$ as a member of $\mathbb{R}^\times$. Then $(r, z_2, z_3, \dots)$ is in $\mathbb{I}(S_\infty)$, and $(x_\infty, x_2, x_3, \dots) = (q, q, q, \dots)(r, z_2, z_3, \dots)$.

4. In (a), the norm of the ideal divides the norm of any element, and if the norm of the ideal is prime, then the ideal is prime. With $K = \mathbb{Q}(\sqrt{-5})$, we have $N_{K/\mathbb{Q}}(1 \pm \sqrt{-5}) = 6$, $N_{K/\mathbb{Q}}(3) = 9$, and $N_{K/\mathbb{Q}}(2) = 4$. Therefore $N((1 \pm \sqrt{-5}, 3))$ divides $\mathrm{GCD}(6, 9) = 3$, and $N((1 \pm \sqrt{-5}, 2))$ divides $\mathrm{GCD}(6, 4) = 2$. One checks that these ideals are not all of R, and then the respective norms are 3 and 2. So the ideals are prime. In (b), $(1 + \sqrt{-5}) = (1 + \sqrt{-5}, 2)(1 + \sqrt{-5}, 3)$, and $(3) = (1 + \sqrt{-5}, 3)(1 - \sqrt{-5}, 3)$.

In (c), $\frac{1}{3}(1+\sqrt{-5})R = (1+\sqrt{-5}, 2)(1+\sqrt{-5}, 3)(1+\sqrt{-5}, 3)^{-1}(1-\sqrt{-5}, 3)^{-1}$ $= (1 + \sqrt{-5}, 2)(1 - \sqrt{-5}, 3)^{-1}$, and $(1 + \sqrt{-5}, 3)$ does not appear.

In (d), $\frac{1+\sqrt{-5}}{3} = \frac{2(1+\sqrt{-5})}{2 \cdot 3} = \frac{2(1+\sqrt{-5})}{(1+\sqrt{-5})(1-\sqrt{-5})} = \frac{2}{1-\sqrt{-5}}$.

5. The mapping $\varphi : 1 + P_v^n \to P_v^n / P_v^{n+1}$ induced by $1 + x \mapsto x + P_v^{n+1}$ is a homomorphism from $1 + P_v^n$ under multiplication into P_v^n / P_v^{n+1} under addition because the equalities $\varphi(1 + x) = x + P_v^{n+1}$, $\varphi(1 + y) = y + P_v^{n+1}$, and

$$\begin{aligned} \varphi\big((1 + x)(1 + y)\big) &= \varphi(1 + x + y + xy) \\ &= x + y + xy + P_v^{n+1} = x + y + P_v^{n+1} \end{aligned}$$

show that $\varphi\big((1 + x)(1 + y)\big) = \varphi(1 + x) + \varphi(1 + y)$. The kernel of φ is the set of all $1 + x$ with $x \in P_v^{n+1}$, i.e., $1 + P_v^{n+1}$, and the image is certainly all of P_v^n / P_v^{n+1}.

6. The composition $\mathbb{I}^1 / \iota(K^\times) \to \mathbb{I} / \iota(K^\times) \to \mathcal{I} / \mathcal{P}$ induced by the inclusion $\mathbb{I}^1 \to \mathbb{I}$ and the passage from $\mathbb{I}$ to $\mathcal{I}$ discussed in Section 10 is onto $\mathcal{I}/\mathcal{P}$ because the composition is affected by only the nonarchimedean places and because any member of $\mathbb{I}$ can be adjusted at the archimedean places so as to be in $\mathbb{I}^1$. In addition, the composition is continuous if $\mathcal{I}/\mathcal{P}$ is given the discrete topology. Since $\mathbb{I}^1 / \iota(K^\times)$ is compact, the discrete space $\mathcal{I}/\mathcal{P}$ has to be compact and must be finite.

7. Fix a finite subset S of places containing S_∞. Then the projection of $\prod_{w \in S} K_w^\times$ to $K_v^\times$ is continuous for each $v \in S$. Since also the inclusion $K_v^\times \to K_v$ is continuous, the composition $\prod_{w \in S} K_w^\times \to K_v$ is continuous. Thus the corresponding mapping $\prod_{w \in S} K_w^\times \to \prod_{w \in S} K_w$ is continuous. In similar fashion $\prod_{w \notin S} \mathbb{Z}_w^\times \to \mathbb{Z}_v$ is a

continuous function as a composition of continuous functions. Thus $\prod_{w\notin S}\mathbb{Z}_w^\times \to \prod_{w\notin S}\mathbb{Z}_w$ is continuous. Putting these two compositions together shows that $\mathbb{I}_K(S) \to \mathbb{A}_K(S)$ is continuous, and therefore $\mathbb{I}_K(S) \to \mathbb{A}_K$ is continuous. Since this is true for each S, it follows that $\mathbb{I}_K \to \mathbb{A}_K$ is continuous.

8. Each x_n lies in $\mathbb{A}_{\mathbb{Q}}(S_\infty)$, which is an open set in $\mathbb{A}_{\mathbb{Q}}$. For each prime p, $x_{n,p} = 1$ if n is large enough, and also $x_{n,\infty} = 1$ for all n. Since $\mathbb{A}_{\mathbb{Q}}(S_\infty)$ has the product topology, $\{x_n\}$ converges to (1). On the other hand, if $\{x_n\}$ were to converge to some limit x in $\mathbb{I}_{\mathbb{Q}}$, then x would have to lie in some $\mathbb{I}(S)$, and the ideles x_n would have to be in $\mathbb{I}(S)$ for large n. But $(x_{n,v})$ is not in $\mathbb{I}(S)$ as soon as v is outside S.

9. For fixed g in G, we have $d(\Phi(gx)) = d(\Phi(g)\Phi(x)) = d(\Phi(x))$, and hence $d(\Phi(\,\cdot\,))$ and $d(\,\cdot\,)$ are Haar measures on G. Any two Haar measures are proportional, and the result follows.

10. In (a) the equality is trivial if $c_1c_2 = 0$. When $c_1c_2 \neq 0$, we have $d(c_1c_2x) = |c_1c_2|_F\,dx$ and also $d(c_1c_2x) = |c_1|_F d(c_2x) = |c_1|_F|c_2|_F\,dx$, and it follows that $|c_1c_2|_F = |c_1|_F|c_2|_F$ in this case as well.

The proof of continuity is harder (but is essential to make sense out of (b)). We first check continuity at each $c_0 \neq 0$. Let f be a continuous real-valued function vanishing off a compact set S, and let N be a compact neighborhood of c_0 not containing 0. If c is in N, then $f(c^{-1}x)$ is nonzero only for x in the compact set NS. Let $\epsilon > 0$ be given. Continuity of $(c, x) \mapsto f(c^{-1}x)$ allows us to find, for each x in NS, an open subneighborhood N_x of c_0 and an open neighborhood U_x of x such that $|f(c^{-1}y) - f(c_0^{-1}x)| < \epsilon$ for $c \in N_x$ and $y \in U_x$. Then $|f(c^{-1}y) - f(c_0^{-1}y)| < 2\epsilon$ for $c \in N_x$ and $y \in U_x$. The open sets U_x cover NS. Forming a finite subcover and intersecting the corresponding finitely many sets N_x, we obtain an open neighborhood N' of c_0 such that $|f(c^{-1}y) - f(c_0^{-1}y)| < 2\epsilon$ for $c \in N'$ whenever y is in NS. As a result, $c \mapsto \int_V f(c^{-1}x)\,dx$ is continuous at $c = c_0$. Therefore $c \mapsto |c|_V \int_V f(x)\,dx$ is continuous at c_0, and so is $c \mapsto |c|_V$.

To prove continuity at $c = 0$, we are to show that $\lim_{c\to 0}\int_V f(c^{-1}x)\,dx = 0$ for f as above. Let U be any compact neighborhood of 0 in V. Find a sufficiently small neighborhood N of 0 in V such that $c \in V$ implies that cS does not meet U^c. Then $c^{-1}U^c \cap S = \varnothing$. For such c's, we have $\left|\int_V f(c^{-1}x)\,dx\right| = \left|\int_U f(c^{-1}x)\,dx\right| \leq \|f\|_{\sup}(dx(U))$, and the desired limit relation follows.

For (b), we have $d(cx)/|cx|_F = (|c|_F\,dx)/(|c|_F|x|_F) = dx/|x|_F$. For (c), $|x|_F = |x|$ if $F = \mathbb{R}$, and $|x|_F = |x|^2$ if $F = \mathbb{C}$. For (d), $|x|_F = |x|_p$ if $F = \mathbb{Q}_p$. For (e), we have $I = p\mathbb{Z}_p$, and therefore the Haar measure of I is the product of $|p|_p = p^{-1}$ times the Haar measure of $\mathbb{Z}_p$. Hence the Haar measure of I is p^{-1}.

11. If F has characteristic $p' \neq 0$, then the sum $1 + \cdots + 1$ with p' terms is 0 in R, and it must be 0 in $R/\mathfrak{p}$. So $R/\mathfrak{p}$ must have characteristic p'. Thus any such $p' \neq 0$ must be p.

12. In (a), apply Corollary 6.29 with $f(X) = X^{q-1} - 1$ in $R[X]$. Every nonzero $\bar{a}$ is a simple root of the reduced polynomial $\overline{f}(X) = X^{q-1} - 1$ in $\mathbb{F}_q[X]$, simple

because $(q-1)(\bar{a})^{q-1} \neq 0$. The corollary produces a root a of $f(X)$ whose image in $R/\mathfrak{p}$ is $\bar{a}$. In this way we obtain $q-1$ distinct roots of 1 in R, each corresponding to a different coset in $R/\mathfrak{p}$. Together with 0, these exhaust the cosets of $R/\mathfrak{p}$.

In (b), if F has characteristic p, then raising to the p^{th} power is a field mapping of F into itself. Since $q = p^m$, raising to the q^{th} power is the m-fold iterate of a field map and is a field map. If a and b are two $(q-1)^{\text{st}}$ roots of 1 in R, then $(a \pm b)^q = a^q + (\pm b)^q = a + (\pm b)$, and so $a \pm b$ is a $(q-1)^{\text{st}}$ root of 1. Since the nonzero elements of E are closed under inverses, E is a subfield.

13. In (a) let x be in R. Problem 12 produces a unique $a_0 \in E$ with $x - a_0$ in $\mathfrak{p}$, i.e., with $v(x-a_0) \geq 1$. Then $v\big(t^{-1}(x-a_0)\big) \geq 0$, and Problem 12 produces a unique a_1 in E with $t^{-1}(x-a_0) - a_1$ in $\mathfrak{p}$. Continuing in this way, we obtain $a_0, \ldots, a_N$ in E with

$$t^{-1}(t^{-1}(\cdots(t^{-1}(x-a_0)-a_1)-\cdots)-a_{N-1})-a_N$$

in $\mathfrak{p}$. Thus $v\big(x - \sum_{k=0}^{N} a_k t^k\big) \geq N+1$. Since F is complete, $\sum_{k=0}^{\infty} a_k t^k$ converges with sum x. The statement about the value of v is clear.

In (b), the part about the series giving an element in R is immediate from Problem 1, since t^k has limit 0. The operations on R now match those on $\mathbb{F}_q[[t]]$, and the isomorphism follows. For (c), let x be given with $x \notin R$. Set $v(x) = -N$. Then $v(t^N x) = 0$, and we can apply (a) to write $t^N x = \sum_{k=0}^{\infty} a_k t^k$. Then $x = \sum_{k=0}^{\infty} a_k t^{k-N}$, as required.

14. In (a), the inclusion of the integers into R, followed by passage to the quotient $R/\mathfrak{p}$, is an additive homomorphism. Since $R/\mathfrak{p}$ has order q, q must map to the 0 coset, namely $\mathfrak{p}$.

Part (a) shows that $v(q) \geq 1$. Since $v(q) = v(p^m) = mv(p)$, $v(p)$ is positive, and (b) is proved. The same argument as in the proof of Ostrowski's Theorem shows that $v(p') = 0$ for all prime numbers other than p, and then (c) is immediate. For (d), it is enough to check equality of the absolute values in question on the element p, and for that we have $|p|_F^{1/(mv_0)} = q^{-v(p)/(mv_0)} = q^{-1/m} = p^{-1}$.

For (e), the map of $\mathbb{Q}'$ to $\mathbb{Q}$, when composed with the completion $\mathbb{Q} \to \mathbb{Q}_p$, is a homomorphism of valued fields into a complete field. It therefore extends uniquely as a homomorphism of the closure $\overline{\mathbb{Q}'}$ into $\mathbb{Q}_p$. The dense set $\mathbb{Q}'$ maps to the dense set $\mathbb{Q}$, and hence the extended map is an isomorphism.

Part (f) is just a repetition of the argument in Problems 13a and 13c. In (g), let $x = \sum_{k=0}^{\infty} a_k t^k$ be the expansion of f, and put $c_{j_0} = \sum_{k=0}^{v_0-1} a_k t_k$. Since $v(t) = 1$, we obtain $v(x - c_{j_0}) \geq v(t^{v_0}) = v_0 v(t) = v_0$. Therefore $v(p^{-1}(x - c_{j_0})) \geq 0$. Iterating this procedure as in Problem 13a, we obtain a convergent expansion $x = \sum_{k=0}^{\infty} c_{j_k} p^k$. For (h), we then have $x = \sum_{k=0}^{\infty} c_{j_k} p^k = \sum_{j=1}^{l} c_j \sum_{\{k \mid j_k = j\}} p^k$, and we see that x lies in $\sum_{j=1}^{l} \overline{\mathbb{Q}'} c_j$. Therefore $\dim[F : \overline{\mathbb{Q}'}] \leq l$.

15. Part (a) is immediate, and (b) follows from Theorem 6.33. For (c), $R/\mathfrak{p}$ corresponds to extracting the constant term from a power series in t, and thus $L/\wp \cong \mathbb{F}_{q^f}$ is of dimension f over $R/\mathfrak{p} \cong \mathbb{F}_q$. The computation $\wp T = tUT = tT = tRT = \mathfrak{p}T = P^e$ shows that K/L has ramification index e. For (d), each index

(residue class degree and ramification index) for K/F is the product of that index for K/L and that index for L/F. So e for L/F is 1, and f for K/L is 1.

16. For (a), the irreducible polynomial $\overline{g}(X)$ has to be separable, and therefore all of its roots in $\Bbbk_K$ are simple. Application of Hensel's Lemma in the form of Corollary 6.29 produces α. For (b), the polynomial $g(X)$ is monic with coefficients in R, and its root α is therefore a member of L integral over R. Thus α lies in U. The natural field map $U/\wp \to T/P$ takes $u+\wp$ to $u+P$, hence takes $\alpha+\wp$ to $\alpha+P=\overline{\alpha}$. Thus we can regard $\overline{\alpha}$ as a member of $\Bbbk_L$. Since $\Bbbk_F$ and $\overline{\alpha}$ generate $\Bbbk_K$ by construction of $\overline{\alpha}$, $\Bbbk_L = \Bbbk_F$.

For (d), let us use subscripts on the indices e and f to indicate the field extension in question. Then we have $e_{L/F} f_{L/F} = [L : F] = \deg g(X) = \deg \overline{g}(X) = [\Bbbk_K : \Bbbk_F] = f_{K/F}$ on the one hand and $f_{K/F} = [\Bbbk_K : \Bbbk_F] = [\Bbbk_L : \Bbbk_F] = f_{L/F}$ on the other hand. The two chains of equalities together show that $e_{L/F} = 1$, and the second one in combination with $f_{K/F} = f_{K/L} f_{L/F}$ shows that $f_{K/L} = 1$.

17. In (a), the element y_j exists and is unique because of the nondegeneracy of the trace form, which holds because K/F is separable (Theorem 8.54 and Section IX.15 of *Basic Algebra*).

In (b), the expression for the z_k's in terms of the y_j's shows that $\sum_{k=1}^n Rz_k \subseteq \sum_{j=1}^n Ry_j$. The assumption $\det A = \pm 1$ implies that $B = A^{-1}$ lies in $M_n(R)$. Since $y_j = \sum_k B_{kj} z_k$, we obtain $\sum_{j=1}^n Ry_j \subseteq \sum_{k=1}^n Rz_k$.

For (c), it is evident that the degree is at most $n-1$. Write $g(X) = \prod_j (X - \xi_j)$. The opening computations of Section V.4 show that $g'(\xi_i) = \prod_{j \neq i} (\xi_i - \xi_j)$. Therefore the value of the left side at ξ_k for the identity in question is

$$\sum_{i=1}^n \frac{\prod_{j\neq i}(\xi_k - \xi_j)}{\prod_{j\neq i}(\xi_i - \xi_j)}.$$

The numerator is 0 unless $i = k$. Thus only the i^{th} term makes a contribution, and its value, namely 1, matches the value of the right side. Then (d) is a routine computation.

For (e), the rational expression $(1 + c_1 X + \cdots + c_n X^n)^{-1}$ on the left side is expanded in series using $(1+Z)^{-1} = 1 - Z + Z^2 - Z^3 + \cdots$. Thus the left side is the sum of X^n and a series beginning with a multiple of X^{n+1}. The right side is $\sum_{k=0}^\infty \operatorname{Tr}_{K/F}\left(g'(\xi)^{-1}\xi^k X^{k+1}\right)$, and the conclusion of the problem results by equating the indicated coefficients.

For (f), the result of (e) handles the entries with $i + j \leq n+1$. For those with $n+2 \leq i+j \leq 2n$, we write $\xi^{i+j-2} g'(\xi)^{-1}$ as $\xi^n \xi^{i+j-n-2} g'(\xi)^{-1}$, substitute for ξ^n recursively from the field polynomial, and check that the traces are in R by applying (e). Thus all A_{ij} are in R.

For (g), conclusion (f) shows that A is triangular with 1's on the off diagonal, and hence the determinant of A is ± 1. Put $z_k = \sum_j A_{jk} y_j$. Since $x_i = \xi^{i-1}$,

$$\begin{aligned}\operatorname{Tr}_{K/F}(z_k x_i) &= \textstyle\sum_j A_{jk} \operatorname{Tr}_{K/F}(y_j x_i) = A_{ik} \\ &= \operatorname{Tr}_{K/F}((g'(\xi)^{-1}\xi^{k-1})\xi^{i-1}) = \operatorname{Tr}_{K/F}((g'(\xi)^{-1}\xi^{k-1})x_i).\end{aligned}$$

Therefore $z_k = g'(\xi)^{-1}\xi^{k-1}$. Combining this equality with (b) shows that $\widehat{N} = \sum_j Ry_j = \sum_k Rz_k = \sum_k Rg'(\xi)^{-1}\xi^{k-1} = g'(\xi)^{-1}N$.

18. For (a), the assumption $f = n$ makes $\dim_{\Bbbk_F}(\Bbbk_K) = n$. Thus $\deg g(X) = \deg \overline{g}(X) = n$. Since $\overline{g}(X)$ is irreducible, so is $g(X)$. The root α of $g(X)$ in K is such that $F(\alpha)$ is an n-dimensional subspace of K, hence equals K.

For (b), the conclusion $\widehat{N} \supseteq \widehat{T}$ follows from the definition. Since $\widehat{T} = \mathcal{D}(K/F)^{-1}$, we obtain $\mathcal{D}(K/F)^{-1} \subseteq \widehat{N} = g'(\alpha)^{-1}N \subseteq g'(\alpha)^{-1}T$.

For (c), the polynomial $\overline{g}(X)$ was constructed as irreducible, and $g(X)$ was constructed to reduce to $\overline{g}(X)$. Then $\overline{g}'(\overline{\alpha}) \neq 0$, and it follows that $g'(\alpha)$ is in T but not P. Thus $g'(\alpha)$ is a unit in T, and $g'(\alpha)^{-1}T = T$. Then $\mathcal{D}(K/F)^{-1} \subseteq T$. Since $\mathcal{D}(K/F)^{-1} \supseteq T$ also, $\mathcal{D}(K/F)^{-1} = T$, and $\mathcal{D}(K/F) = T$.

19. For (a), we may assume that $v(x_1) \leq v(x_j)$ for $j > 1$. If $v(x_1) < v(x_j)$ for all $j > 1$, then induction and use of property (vi) of discrete valuations shows inductively that $v(0) = v(x_1 + \cdots + x_m) = v(x_1)$, contradiction.

For (b), the element π is in T, and its minimal polynomial has coefficients in R because T is integral over R; in turn, the field polynomial is a power of the minimal polynomial. Since c_j is in R, we have $v_K(c_j) = nv_F(c_j)$, and therefore $v_K(c_j)$ is divisible by n.

For (c), apply (a) to the equality $c_0\pi^n + c_1\pi^{n-1} + \cdots + c_n = 0$ to produce indices $i < j$ with $v(c_i\pi^{n-i}) = v(c_j\pi^{n-j})$ and with $v(c_k\pi^{n-k}) \geq v(c_i\pi^{n-i})$ for all k. The equality involving i and j implies that $j - i = v_K(c_j) - v_K(c_i)$. From $i < j \leq n$, we have $n - i > 0$. Thus $v(c_i\pi^{n-i}) \geq v(c_i\pi) > 0$. By (b), $v(c_i\pi^{n-i}) \geq n$. So $v(c_k\pi^{n-k}) \geq n$.

In (d), the right side of the equality $j - i = v_K(c_j) - v_K(c_i)$ is divisible by n, by (b), and the left side is between 1 and n. Hence the two sides equal n, and we conclude that $i = 0$ and $j = n$. Thus the equality says that $n = v_K(c_n)$. Since c_n is in F and since $v_K = nv_F$, $v_F(c_n) = 1$. Therefore c_n is in $\mathfrak{p}$ but not $\mathfrak{p}^2$. The inequality $v_K(c_k\pi^{n-k}) \geq n$ implies that $v_K(c_k) \geq k$. For $1 \leq k \leq n$, this conclusion implies that $v_K(c_k) \geq 1$. Since c_K is in F and since $v_K = nv_F$, $v_F(c_k) > 0$ for $k \geq 1$. Thus c_k is in $\mathfrak{p}$ for $k \geq 1$.

In (e), the irreducibility is immediate from the Eisenstein irreducibility criterion, R being a principal ideal domain. Since the field polynomial is a power of the minimal polynomial, the field polynomial equals the minimal polynomial. Then the degree of $F(\pi)$ is n. Since $F(\pi)$ is an n-dimensional subfield of the n-dimensional field K, $K = F(\pi)$.

Part (f) is proved in the same way as Problem 14g. For (g), the expansion can be rewritten as $\sum_{k=0}^{\infty} a_k y_k = \sum_{i=0}^{\infty} \sum_{0 \leq j < e} a_{ei+j} y_{ei+j} = \sum_{0 \leq j < e} \pi^j \big(\sum_{i=0}^{\infty} a_{ei+j} \lambda^i \big)$. The term in parentheses is the most general member of R, and the left side is the most general member of T. Thus (g) follows.

In (h), conclusion (g) shows that $N = \sum_{k=0}^{n-1} R\pi^k$ equals T, and Problem 17 with $\xi = \pi$ shows that $\widehat{N} = g'(\pi)^{-1}N$. Thus $\mathcal{D}(K/F)^{-1} = \widehat{T} = g'(\pi)^{-1}T$. Multiplying by $(g'(\pi))\mathcal{D}(K/F)$, we obtain $\mathcal{D}(K/F) = (g'(\pi))$.

For (i), $g'(\pi) = e\pi^{e-1} + \sum_{k=1}^{n-1} c_{n-k} k \pi^{k-1} = e\pi^{e-1} + b$. In each term of b, $v_K(kc_{n-k}) \ge e v_F(c_{n-k}) \ge e$, and $v_K(\pi^{k-1}) = k-1$. Thus $v_K(b) \ge e$. Meanwhile, $v_K(e\pi^{e-1}) = (e-1) + v_K(e)$. Thus $v_K(g'(\pi)) \ge \min\big((e-1) + v_K(e),\ v_K(b)\big)$, and property (vi) of discrete valuations shows that equality holds if the two members $(e-1) + v_K(e)$ and $v_K(b)$ of the minimum are unequal. If $v_K(e) = 0$, then the members are unequal, and we obtain $v_K(g'(\pi)) = e - 1$. Otherwise, we obtain $v_K(g'(\pi)) \ge e$. We know that $\mathcal{D}(K/F) = (g'(\pi)) = P^{v_k(g'(\pi))}$, and Lemma 6.47 follows.

Chapter VII

1. If x and y are members of L purely inseparable over K, then x^{p^e} and $y^{p^{e'}}$ are in K for suitable e and e'. Without loss of generality, let $e' \le e$. Then x^{p^e} and y^{p^e} are in K, and hence $(x \pm y)^{p^e} = x^{p^e} \pm y^{p^e}$ are in K and so are $(xy)^{p^e} = x^{p^e} y^{p^e}$ and $(xy^{-1})^{p^e} = x^{p^e} y^{-p^e}$ if $y \ne 0$. So $x \pm y$, xy, and xy^{-1} are purely inseparable over K, the last of these if $y \ne 0$.

2. In view of Proposition 7.10, the given conditions imply that $[K(\alpha) : K] = p^e[K(\alpha^{p^e}) : K]$ and that $X^{p^\mu} - \alpha^{p^e}$ is irreducible over $K(\alpha^{p^e})$ for every $\mu \ge 0$. Since $\alpha^{p^{e-\mu}}$ is a root of this polynomial within $K(\alpha)$ for each $\mu \le e$, $K(\alpha)$ has a chain of subfields

$$K(\alpha^{p^e}) \subsetneqq K(\alpha^{p^{e-1}}) \subsetneqq \cdots \subsetneqq K(\alpha^p) \subsetneqq K(\alpha)$$

in which the consecutive degrees of the extensions are all p. Let β be separable over K, and let $K(\alpha^{p^r})$ be the first of these fields to contain β. Arguing by contradiction, suppose that $r < e$. Then β and $\alpha^{p^{r+1}}$ generate $K(\alpha^{p^r})$ because $[K(\alpha^{p^r}) : K(\alpha^{p^{r+1}})]$ is prime. The separability of β over K implies that β is separable over $K(\alpha^{p^{r+1}})$, hence that $K(\alpha^{p^r})$ is separable over $K(\alpha^{p^{r+1}})$, hence that α^{p^r} is separable over $K(\alpha^{p^{r+1}})$. Since $(\alpha^{p^r})^p$ lies in $K(\alpha^{p^{r+1}})$, α^{p^r} is also purely inseparable over $K(\alpha^{p^{r+1}})$. By Corollary 7.12, α^{p^r} lies in $K(\alpha^{p^{r+1}})$. This contradicts the fact that the above chain of subfields is strictly increasing. We conclude that $r = e$. Hence all elements β separable over K lie in $K(\alpha^{p^e})$.

3. For suitable integers R_a, we form the tuple $z = (R_a + a\mathbb{Z})_{a \ge 1}$, using the realization of the inverse limit in Proposition 7.27. We have to specify the integers R_a. The condition for z to lie in $\widehat{\mathbb{Z}}$, coming from the condition $f_{ab} \circ f_b = f_a$ when a divides b, works out to be that $R_b - R_a$ is divisible by a whenever a divides b. After the integers R_a have been defined for all a, it is enough to check that $R_{pa} - R_a$ is divisible by a whenever p is prime.

For n odd, define $R_{2^c n} = nk + 1$, where k is the unique integer from 0 to $2^c - 1$ such that $nk + 1$ is divisible by 2^c. This k exists and is unique because $-n$ has an inverse modulo 2^c. One checks that $R_{2^{c+1}n} - R_{2^c n}$ is divisible by 2^c and by n, and that $R_{2^c pn} - R_{2^c n}$ is divisible by 2^c and by n if p is an odd prime. The definition makes $R_2 = 0$ and $R_q = 1$ for every odd prime q, and therefore z is not of the form z_c for any integer c.

4. The first part is immediate from Theorem 7.34. For the second part the group $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$ is trivial. In fact, any member of $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$ must fix $\mathbb{Q}$ and map squares in $\mathbb{R}$ to squares. It therefore respects the ordering. For any $r \in \mathbb{R}$, it fixes each rational less than r, and hence it fixes r.

5. Use $K_n = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$, where p_n is the n^{th} prime, and Proposition 7.30 to see that $\mathrm{Gal}(K/\mathbb{Q})$ is an infinite product of groups of order 2. (A problem at the end of Chapter IX of *Basic Algebra* can help with this step.) The open subgroups of index 2 correspond to quadratic extensions of $\mathbb{Q}$, of which there are countably many. Since $\mathrm{Gal}(K/\mathbb{Q})$ has uncountably many subgroups of index 2, such a subgroup H exists that is not open. The field extension $K/\mathbb{Q}$ is normal, and thus $\mathrm{Gal}(K/\mathbb{Q})$ is a homomorphic image of $\mathrm{Gal}(\mathbb{Q}_{\text{alg}}/\mathbb{Q})$, say by a homomorphism φ. Then $\varphi^{-1}(H)$ is the required subgroup of $\mathrm{Gal}(\mathbb{Q}_{\text{alg}}/\mathbb{Q})$.

6. Suppose I is primary. If $b + I$ is a zero divisor in R/I, then ab is in I for some a not in I. Since I is primary, b^m is in I for some m. Thus $(b + I)^m = b^m + I = I$, and $b + I$ is nilpotent in R/I.

If every zero divisor in R/I is nilpotent, then the ideal 0 in R/I is primary because whenever $(a + I)(b + I) = I$ and $a + I \neq I$, then the nilpotence of $b + I$ implies that $b^m + I = I$ for some m. This says that the 0 ideal $0 + I$ in R/I is primary.

If the 0 ideal in R/I is primary and if ab is in I with a not in I, then $(a+I)(b+I) = I$ with $a + I \neq I$, and hence $(b + I)^m = I$ for some m, 0 being primary in R/I. This means that b^m is in I, and I is primary.

7. In (a), if xy is in $\sqrt{I}$, then $(xy)^m$ is in I for some m, and therefore either x^m is in I or y^{mn} is in I for some n, i.e., either x is in $\sqrt{I}$ or y is in $\sqrt{I}$.

In (b), let x be in $\sqrt{I}$, and choose n such that x^n is in I. Then x^n is in J because $I \subseteq J$. Since J is prime, some factor of x^n is in J, i.e., x is in J.

8. In (b), $R/I \cong \mathbb{C}[y]/(y^2)$. The zero divisors of R/I are cy with $c \in \mathbb{C}$, and $(cy)^2 = 0$ in R shows that cy is nilpotent in R. By Problem 6, I is primary. The radical $P = \sqrt{I}$ is (x, y) by inspection, and this is prime. Since $P^2 = (x^2, xy, y^2)$, we have $P^2 \subsetneqq I \subsetneqq P$. If $I = Q^n$ for some prime ideal Q, then $I \subseteq Q$, and Problem 7b shows that $\sqrt{I} \subseteq Q$. Since $\sqrt{I}$ is maximal in this case, Q has to be P.

In (c), $R/P \cong K[X, Y, Z]/(XY - Z^2, X, Z) \cong K[Y]$, and this is an integral domain. Hence P is prime. Next, $P^2 = (x^2, xz, z^2)$. Thus $xy = z^2$ lies in P^2. However, x is not in P^2, and y^m is not in P^2 for any $m > 0$. So P^2 is not primary.

9. Let a and b be in R with ab in I and a not in I. To show that I is primary, we are to show that b is in $\sqrt{I}$. We do this by showing that $(b) + I \subseteq \sqrt{I}$. The ideal $(b) + I$ is proper, since otherwise $1 = cb + x$ with $x \in I$, which implies that $a = cba + xa$ is in I, contradiction. Let J be a maximal ideal with $(b) + I \subseteq J$. It is enough to show that $\sqrt{I} \subseteq J$; in fact, then $\sqrt{I} = J$ because $\sqrt{I}$ is assumed maximal, and $(b) + I \subseteq \sqrt{I}$ as asserted. So let u be in $\sqrt{I}$. Then u^m is in $I \subseteq J$ for some m, and u is in J because J is prime.

This proves the first part. The second part follows from the observation that if J

is maximal, then $\sqrt{J^n} = J$. In fact, J^n contains all elements a^n for $a \in J$. So $\sqrt{J^n}$ has to contain all elements $a \in J$. Since J is maximal and $\sqrt{J^n}$ has to be proper, $\sqrt{J^n} = J$.

10. In (a), let P be a prime ideal, and suppose that $P = I \cap J$ nontrivially. If i is in I but not J and if j is in J but not I, then ij is in P, but i is not in P because i is not in J and similarly j is not in P because j is not in I.

In (b), $I^2 = (x^2, xy, y^2)$ is primary by Problem 9. The equality of I^2 with $(Rx + I^2) \cap (Ry + I^2)$ holds by inspection.

11. Arguing by contradiction, we can use the Noetherian property to obtain an ideal I maximal with respect to the property of not being a finite intersection of proper irreducible ideals. Since I is not irreducible, $I = A \cap B$ nontrivially. By maximality, A and B are intersections, and then so is I, contradiction.

12. Let Q be a proper irreducible ideal in R. Then 0 is a proper irreducible ideal in R/Q. We show that 0 is primary in R/Q, and then Problem 6 shows that Q is primary. Thus let $xy = 0$ in R/Q with $y \neq 0$ in R/Q. We want to see that some power of x is 0 in R/Q. In R/Q, we form the sequence of annihilators $\mathrm{Ann}(x) \subseteq \mathrm{Ann}(x^2) \subseteq \cdots$ and use the Noetherian property of R and its quotient R/Q to obtain $\mathrm{Ann}(x^l) = \mathrm{Ann}(x^{l+1})$ for some l. Let us see that the intersection $(x^l) \cap (y)$ is 0 in R/Q. In fact, if a is in (y), then $xy = 0$ implies $ax = 0$, and if a is in (x^l), then $a = bx^l$ and $0 = ax = bx^{l+1}$, from which we see that b is in $\mathrm{Ann}(x^{l+1}) = \mathrm{Ann}(x^l)$. Therefore $a = bx^l = 0$ in R/Q. Thus indeed $(x^l) \cap (y) = 0$. Since 0 is irreducible in R/Q and $(y) \neq 0$, we conclude that $(x^l) = 0$ and $x^l = 0$ in R/Q. This is what we were to show.

13. If ab is in Q and a is not in Q, then ab is in Q_i for all i and a is not in Q_{i_0} for some i_0. Since Q_{i_0} is primary, b^m is in Q_{i_0} for some m, i.e., b is in $\sqrt{Q_{i_0}} = P$. Since $\sqrt{Q_i} = P$ for all i, b^{k_i} is in Q_i for some k_i depending on i. Taking N to be the maximum of the integers k_i, we see that b^N is in each Q_i and hence is in their intersection Q. Thus Q is primary.

Problem 7b shows that $\sqrt{Q} \subseteq P$. On the other hand, if b is in P, we have just seen that some power b^N lies in Q. So b lies in $\sqrt{Q}$. Therefore $\sqrt{Q} = P$.

14. Problem 11 shows that every ideal is the finite intersection of proper irreducible ideals, and Problem 12 shows that these are primary. Thus if I is given, we have $I = \bigcap Q_i$ with each Q_i primary. Group all Q_i's whose associated prime ideal is the same P_j, and denote the intersection of these by Q'_j. The ideal Q'_j is primary by Problem 13. Then $I = \bigcap Q'_j$, and the Q'_j have distinct associated prime ideals. So condition (ii) is satisfied. Finally among all expressions for I as intersections satisfying (ii), choose one that involves the smallest number of primary ideals. This minimality forces (i) to hold.

Chapter VIII

1. $(q^{n+1} - 1)/(q - 1) = 1 + q + q^2 + \cdots + q^n$.

3. It is enough to consider a monomial $F(X_1, \ldots, X_n) = X^{\alpha_1} \cdots X^{\alpha_n}$ with $\sum_{j=1}^{n} \alpha_j = d$. Then $X_j \frac{\partial}{\partial X_j}(X^{\alpha_1} \cdots X^{\alpha_n}) = \alpha_j X^{\alpha_1} \cdots X^{\alpha_n}$, and the sum on j equals $dX^{\alpha_1} \cdots X^{\alpha_n}$.

4. If f^ι and g^ι have a nontrivial common factor in $B[X]$, then $0 = R(f^\iota, g^\iota) = \iota(R(f, g))$. Since ι is one-one, $R(f, g) = 0$. Therefore f and g have a nontrivial common factor in $A[X]$.

5. Let us show that if $g_n \neq 0$ and $f_m = 0$, then Theorem 8.1 for indices $(m-1, n)$ implies the theorem for indices (m, n), and vice versa. Assume for the moment that $m \geq 2$. Let $\mathcal{R}(f, g)$ be the resultant matrix of size $m + n$ that takes into account all coefficients $f_0, \ldots, f_m$ of f, and let $R(f, g)$ be its determinant. With $f_m = 0$, let $\mathcal{R}'(f, g)$ be the resultant matrix of size $m+n-1$, and let $R'(f, g)$ be its determinant. The matrix $\mathcal{R}'(f, g)$ is obtained by erasing the m^{th} row and last column of $\mathcal{R}(f, g)$. On the other hand, the only nonzero entry in the last column of $\mathcal{R}(f, g)$ is g_n. Expansion in cofactors therefore gives $R'(f, g) = g_n R(f, g)$. The hypotheses of Theorem 8.1 apply to f and g for either of these resultants, and we have just seen that the two conditions (c) are equivalent. Certainly the two conditions (a) are equivalent. For the two conditions (b), the resultant of size $m + n - 1$ tells us that $a'f + b'g = R'(f, g)$ with $\deg a' < n$ and $\deg b' < m - 1$. Certainly this implies that $af + bg = R(f, g)$ with $a = a'g_n$ and $b = b'g_n$. Conversely if $af + bg = R(f, g)$ with $\deg a < n$ and $\deg b < m$, we define $a' = ag_n^{-1}$ and $b' = bg_n^{-1}$. Then $a'f + b'g = R'(f, g)$ with $\deg a' < n$, and we need to see that $\deg b' = \deg b < m - 1$. Since $f_m = 0$, all the powers of X in af are $\leq (n-1) + (m-1)$, and the same must be true in bg. Since g has degree n, we must have $\deg b \leq m - 2 < m - 1$, as required.

Next we check what happens when $m = 1$ and we are comparing the resultant of size $n + 1$ and a degenerate resultant whose matrix is of size n and contains only the entries of g. The determinant formula is still valid, and we see that $R'(f, g) = g_0^n$, which is nonzero. Thus (a) and (c) are false for both sizes. For (b), we cannot have $af + bg = 0$ with $\deg b < 0$ and $b \neq 0$. We need to check that $af + bg = 0$ cannot happen with $\deg a < n$ and $\deg b < 1$; in fact, then $\deg bg = \deg g = n$, while $f_1 = 0$ implies that $\deg af < n + \deg f = n$. So we cannot have $af + bg = 0$ in this case either.

The result of these calculations is that Theorem 8.1 for (m, n) is equivalent to the theorem for $(m-1, n)$ if $g_n \neq 0$ and $f_m = 0$. Using induction, we see that the theorem for (m, n) is equivalent to the theorem for (k, n) if $g_n \neq 0$ and $f_{k+1} = \cdots = f_m = 0$. Taking $k = \deg f$ gives the desired result.

6. Proof via Nullstellensatz: Since f is irreducible and $K[X_1, \ldots, X_n]$ is a unique factorization domain, the principal ideal (f) is prime. Corollary 7.2 shows that g lies in (f): hence $g = hf$ for some h.

Proof via resultants: The idea is to arrange to have

$$af + bg = R(f, g), \tag{$*$}$$

with the resultant taken with respect to X_n. Proposition 8.1 shows that this happens if f and g are of positive degree in X_n, and we shall show that either this is the case

or else f divides g for easy reasons. Since f is nonconstant, it depends nontrivially on some X_j, and renumbering the variables allows us to assume that f depends nontrivially on X_n. Then f is of the form

$$f(X_1, \ldots, X_n) \\ = c_0(X_1, \ldots, X_{n-1}) + c_1(X_1, \ldots, X_{n-1})X_n + \cdots + c_r(X_1, \ldots, X_{n-1})X_n^r$$

with $r > 0$ and with c_r nonzero in $K[X_1, \ldots, X_{n-1}]$. If $g = 0$, then certainly f divides g. So we may assume that $g \neq 0$. Choose $a_1, \ldots, a_{n-1}$ in K such that

$$g(a_1, \ldots, a_{n-1}, X_n)c_r(a_1, \ldots, a_{n-1}) \neq 0. \qquad (**)$$

Then $f(a_1, \ldots, a_{n-1}, X_n)$ is a polynomial in X_n whose coefficient of X_n^r is nonzero. Since K is algebraically closed, this polynomial in X_n has a root, say a_n. Since $f(a_1, \ldots, a_n) = 0$, the hypothesis shows that $g(a_1, \ldots, a_{n-1}, a_n) = 0$, and $(**)$ allows us to conclude that $g = g(X_1, \ldots, X_n)$ depends nontrivially on X_n. This proves $(*)$.

To complete the proof, we show that $c_r R$ is 0 at every point $(b_1, \ldots, b_{r-1})$. Since K is infinite, it will follow that the polynomial $c_r R$ is 0; thus $R = 0$ because c_r is not the 0 polynomial. Then f and g will have a nontrivial common factor by Proposition 8.1, and f will have to divide g because f is prime. Thus suppose that $c_r(b_1, \ldots, b_{r-1}) \neq 0$. Then $f(b_1, \ldots, b_{r-1}, X_n)$ is a nonconstant polynomial in X_n and must have a root b_r, since K is algebraically closed. Hence $f(b_1, \ldots, b_r) = 0$, and the hypothesis on g shows that $g(b_1, \ldots, b_r) = 0$. By $(*)$, $R(b_1, \ldots, b_{r-1}) = 0$. This completes the proof.

7. $Y^3 - 2XY^2 + 2X^2Y - 4X^3 = (Y - 2X)(Y + i\sqrt{2}\,X)(Y - i\sqrt{2}\,X)$.

8. The resultant matrix in the W variable is

$$\begin{pmatrix} XY^4 - Y^5 & -2X^2Y^2 & X^3 & 0 \\ 0 & XY^4 - Y^5 & -2X^2Y^2 & X^3 \\ Y^4 & Y^3 & -X^2 & 0 \\ 0 & Y^4 & Y^3 & -X^2 \end{pmatrix},$$

and its determinant is $-X^3Y^9(Y - 2X)^2$. Substituting into either of the equations $F = 0$ and $G = 0$ gives the projective solutions (x, y, w) equal to $(1, 0, 0)$, $(0, 0, 1)$, and $(1, 2, 4 \pm 4\sqrt{2})$, up to nonzero scalar factors. (One has to check that both the equations $F = 0$ and $G = 0$ are satisfied.)

9. Introduce a new indeterminate $T = Y_i - Z_j$, and remove Y_i. Then $R(F, G) = R(Y_1, \ldots, T + Z_j, \ldots, Y_m, Z_1, \ldots, Z_n)$ is a polynomial in T, the Z_j's, and all the Y's except for Y_i. Also, $R(F, G) = 0$ when T is set equal to 0. Hence $R(F, G)$ is divisible by T. Then (a) and (b) follow. For (c), the polynomials $Y_i - Z_j$ are distinct primes. Since each divides $R(F, G)$, their product must divide. Their product has the same degree as $R(F, G)$, and the result follows.

10. We may assume that K is algebraically closed and that f is monic, say with $f(X) = \prod_{i=1}^{m} (X - \xi_i)$ and $f'(X) = m \prod_{j=1}^{m-1} (X - \eta_j)$. Then the previous problem gives $f'(\xi_i) = m \prod_{j=1}^{m-1} (\xi_i - \eta_j)$, and

$$R(f, f') = m^m c_{m,m-1} \prod_{i,j} (\xi_i - \eta_j) = m^m c_{m,m-1} \prod_{i=1}^{m} f'(\xi_i)$$

with $c_{m,m-1}$ equal to the constant c from Problem 9c when $n = m - 1$. According to Section V.4, the product is $(-1)^{n(n-1)/2}$ times the discriminant $D(f)$ of f. So the result follows.

11. Replace G by $G(X, Y, W) - (X^2 + Y^2)F(X, Y, W)$ to get $YWH(X, Y, W)$, where $H(X, Y, W) = (X^2 + Y^2)(X^2 - 3Y^2) - 4X^2YW$. Then

$$I(P, F \cap G) = I(P, F \cap YWH) = I(P, F \cap Y) + I(P, F \cap W) + I(P, F \cap H).$$

For $I(P, F \cap Y)$, we use the method of Section 4, looking at $F(t, 0, 1)$, which is t^4; thus $I(P, F \cap Y) = 4$. Since P is not on W, $I(P, F \cap W) = 0$.

For $I(P, F \cap H)$, replace H by $H(X, Y, W) - F(X, Y, W)$ to get $YJ(X, Y, W)$, where $J(X, Y, W) = -4X^2Y - 4Y^3 - 7X^2W + Y^2W$. Then

$$I(P, F \cap H) = I(P, F \cap YJ) = I(P, F \cap Y) + I(P, F \cap J),$$

and again $I(P, F \cap Y) = 4$. If the local expressions of F and J are denoted by f and j, then their lowest-order terms $f_3(x, y)$ and $j_2(x, y)$ are given by

$$f_3(x, y) = 3x^2y - y^3 = y(\sqrt{3}\,x + y)(\sqrt{3}\,x - y),$$
$$j_2(x, y) = -7x^2 + y^2 = -(\sqrt{7}\,x + y)(\sqrt{7}\,x - y).$$

Thus F and J have no tangent lines in common at P, and $I(P, F \cap J) = 3 \cdot 2 = 6$. Collecting the results, we find that $I(P, F \cap G) = 4 + 4 + 6 = 14$.

12. Let $P = [x_0, y_0, w_0]$, and choose $\Phi \in \mathrm{GL}(3, K)$ with $\Phi(x_0, y_0, w_0) = (0, 0, 1)$. The local versions of G and L are $g(X, Y) = G(\Phi^{-1}(X, Y, 1))$ and $l(X, Y) = L(\Phi^{-1}(X, Y, 1))$. The expansion of g as a sum of homogeneous polynomials is $g = g_m + \cdots + g_d$ because $m = m_P(G) > 0$, and l is of the form $l(X, Y) = aX + bY$ because P lies on L. We can parametrize l by $\varphi(t) = (bt, -at)$, and then the definition of intersection multiplicity is that $I(P, L \cap G)$ is the least integer k such that the expression $g_k(\varphi(t)) = t^k g_k(b, -a)$ is nonzero. The definition of tangent line is any projective line L_i whose local version l_i is one of the factors of $g_m(X, Y) = c \prod_i (\alpha_i X + \beta_i Y)^{m_i}$. Then $g_m(\varphi(t)) = t^m g_m(b, -a) = c \prod_i (\alpha_i b - \beta_i a)^{m_i}$. If (a, b) is a multiple of some (α_i, β_i), then $g_m(\varphi(t)) = 0$; hence $I(P, L \cap G) \geq m + 1$. Otherwise $g_m(\varphi(t)) \neq 0$, and $I(P, L \cap G) = m$.

13. The linear span $\mathrm{LT}(I)$ of the members $\mathrm{LT}(f)$ for f in I is a monomial ideal and is of the form $(M_1, \ldots, M_k)$ for suitable monomials M_j each of the form $\mathrm{LM}(f_j)$ for some f_j in I. Then $\{f_1, \ldots, f_k\}$ is a subset of I such that $\big(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_k)\big) = \mathrm{LT}(I)$, and $\{f_1, \ldots, f_k\}$ is a Gröbner basis of I by definition.

14. If α, β, γ are vectors of exponents in monomials such that the first i with $w^{(i)} \cdot \alpha \neq w^{(i)} \cdot \beta$ has $w^{(i)} \cdot \alpha > w^{(i)} \cdot \beta$, then it equally true that the first i with $w^{(i)} \cdot (\alpha + \gamma) \neq w^{(i)} \cdot (\beta + \gamma)$ has $w^{(i)} \cdot (\alpha + \gamma) > w^{(i)} \cdot (\beta + \gamma)$. This proves that property (i) of monomial orderings holds with no further conditions on the weights. Property (ii) says for each vector α of nonnegative exponents not all 0 that the first i with $w^{(i)} \cdot \alpha \neq 0$ has $w^{(i)} \cdot \alpha > 0$. Applying this condition as a necessary condition to the j^{th} standard basis vector $\alpha = e_j$, we see that the first i such that $w_j^{(i)} \neq 0$ must have $w_j^{(i)} > 0$ for (ii) to hold. On the other hand, if this condition holds for all j, then a suitable positive linear combination of these conditions gives (ii) for any α.

15. In (a), $a > a'$ implies that $X^{a-a'} \geq X > Y^{b'}$ for all $b' \geq 0$. Multiplying by $X^{a'}$ gives $X^a > X^{a'}Y^{b'}$. Since $Y^b \geq 1$ implies $X^aY^b \geq X^a$, we conclude that $X^aY^b > X^{a'}Y^{b'}$ for all b and b'. For $a = a'$, we observe that $b > b'$ implies that $Y^{b-b'} > 1$ and hence that $Y^b > Y^{b'}$. Multiplying by X^a gives $X^aY^b > X^aY^{b'}$. Hence the ordering is lexicographic.

In (b), we observe that an inequality between X^a and Y^b implies the same inequality between X^{na} and Y^{nb}. Consequently the particular inequality for X^a and Y^b depends only on the rational number a/b. The assumption for (b) is that $X < Y^q$, hence that $X^a \leq Y^{qa} \leq Y^b$ if $qa \leq b$, thus if $a/b \leq q^{-1}$. Thus the set S of rationals a/b such that $X^a > Y^b$ is bounded below by q^{-1}. Let r^{-1} be the greatest lower bound of S. We know then that $q^{-1} \leq r^{-1}$, hence that $r \leq q$. So $0 \leq r < \infty$, and r is a well-defined real number.

Suppose that $u/v < r^{-1}$. Then u/v is not in S, and so $X^u \leq Y^v$. In the reverse direction, suppose that $u/v > r^{-1}$. Then there is some rational c/d in S with $u/v > c/d \geq r^{-1}$; this has $X^c > Y^d$. Then $X^{ud} > X^{vc} > Y^{vd}$. Since $d > 0$, $X^u < Y^v$ would imply $X^{ud} < Y^{vd}$, which is false. Thus we must have $X^u > Y^v$. This proves (b).

For (c), the only rational u/v for which the inequality between X^u and Y^d is not decided is $u/v = r^{-1}$, and that only if r is rational. In this case a single weight vector will decide the correct inequality. All other inequalities between monomials follow from these. In fact, what needs deciding is the inequality between X^aY^b and $X^{a'}Y^{b'}$ when $a > a'$ and $b < b'$, and this is the same as the inequality between $X^{a-a'}$ and $Y^{b'-b}$.

16. The formulas for f are a matter of computation. Both satisfy the conditions of Proposition 8.20 because $\mathrm{LM}(f) = X^2Y$ is $\geq$ each of $\mathrm{LM}((X+Y)f_1) = X^2Y$, $\mathrm{LM}(1f_2) = Y^2$, $\mathrm{LM}(Xf_1) = X^2Y$, and $\mathrm{LM}((X+1)f_2) = XY^2$ and because no term of r_1 or r_2 is divisible by $\mathrm{LM}(f_1) = XY$ or $\mathrm{LM}(f_2) = Y^2$.

17. In (a), we check that $\{X^2 + cXY, XY\}$ is a Gröbner basis using Theorem 8.23. The leading monomials of the two generators are X^2 and XY, and neither divides the

other. Since the leading coefficients are 1, this Gröbner basis is minimal.

In (b) when $c \neq 0$, $X^2 + cXY$ has a nonzero term whose monomial is divisible by the leading monomial of another generator; specifically the term cXY in $X^2 + cXY$ is divisible by the XY from the other generator. Following the procedure in Theorem 8.28, we find that $\{X^2, XY\}$ is the reduced Gröbner basis.

18. If $(c_1, \ldots, c_n)$ lies in $V_K(I)$, then c_j is one of finitely many roots of $P_j(X)$, for each j. Hence $|V_K(I)| \leq \prod_{j=1}^n \deg P_j$.

19. Fix j, and choose a polynomial Q_j in X that vanishes at the j^{th} coordinate of every member of $V_K(I)$. Then $P_j(X_1, \ldots, X_n) = Q_j(X_j)$ is a polynomial vanishing on $V_K(I)$, and the Nullstellensatz shows that some power of it is in I. The result is a polynomial in X_j alone, as required.

20. If $V_K(I)$ is a finite set, then Problem 19 shows that I contains a nonconstant polynomial in X_j for each j. The leading monomial for the j^{th} such polynomial has to be a power of X_j, and it lies in $\text{LT}(I)$. Conversely suppose that a power $X_j^{l_j}$ lies in $\text{LT}(I)$ for each j. Form a reduced Gröbner basis of I. Since the only monomials dividing $X_j^{l_j}$ are powers of X_j, there exist members g_j of the Gröbner basis for $1 \leq j \leq n$ such that

$$g_j(X_1, \ldots, X_n) = X_j^{m_j} + X_j^{m_j - 1} a_{j,m_j-1} + \cdots + X_j a_{j,1} + a_{j,0}$$

for suitable polynomials $a_{j,m_j-1}, \ldots, a_{j,0}$ in $X_{j+1}, \ldots, X_n$. Then $V_K(I)$ is contained in $V_K((g_1, \ldots, g_n))$, and any member $(c_1, \ldots, c_n)$ of the latter has the property for each j that c_j is a root of a polynomial of degree m_j in one variable, once $(c_{j+1}, \ldots, c_n)$ is fixed. Thus $V_K(I)$ is contained in a finite set and has to be finite.

21. For (a), the coefficients $a_{i_1,\ldots,i_n}$ are given as in $K(X)$, and we look for solutions of $F(T_1, \ldots, T_n) = 0$. Clearing fractions in the coefficients, we see that it is enough to find a solution when each $a_{i_1,\ldots,i_n}$ has denominator 1.

For (b), substitution of $T_i = \sum_{j=1}^N b_{ij} X^j$, where each b_{ij} is an unknown in K, into the equation $F(T_1, \ldots, T_n) = 0$ gives

$$\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} \Big(\sum_{j=1}^N b_{ij} X^j \Big)^{i_1} \cdots \Big(\sum_{j=1}^N b_{ij} X^j \Big)^{i_n} = 0.$$

We expand this out and set the coefficient of each power of X equal to 0. The largest possible power of X that can appear is the sum of the largest power of X in any $a_{i_1,\ldots,i_n}$, namely δ, and $\sum_{k=1}^n N i_k$. Since F is homogeneous of degree d, $\sum_{k=1}^n i_k = d$. Thus the largest possible power of X is $Nd + \delta$. We get one equation for each power of X that appears, and the unknowns are the various b_{ij}'s.

22. The number of equations is $\leq Nd + \delta + 1$, since the powers of X go from 0 to at most $Nd + \delta$. The number of unknowns is one for each index i with $1 \leq i \leq n$ and each possible power of X from 0 to N, hence exactly $(N + 1)n$. For N sufficiently large we want to see that $Nd + \delta + 1 \leq (N + 1)n$. Since $d < n$, the inequality in question is $\delta + 1 - n \leq N(n - d)$, and this is satisfied by taking N large enough.

23. In the context of Problem 22, we have a homogeneous system with more unknowns than equations (for large N). If the number of unknowns is $n+1$ and the number of equations is m, then we are looking for solutions in $\mathbb{P}^n_K$. Since the inequality $m \leq n$ is satisfied, the quoted theorem applies and produces a nonzero solution for the b_{ij}'s.

Chapter IX

1. For (a), we argue by contradiction. Suppose that $c_1(x), \ldots, c_n(x)$ are members of $\Bbbk(x)$, not all 0, such that $\sum_j c_j(x)t_j = 0$. Clearing fractions, we may assume that each $c_j(x)$ lies in $\Bbbk[x]$. If necessary, we can divide through by a power of x and arrange that some $c_j(x)$, say $c_{j_0}(x)$, has a nonzero constant term. The element x is by assumption transcendental over $\Bbbk$. Applying the substitution homomorphism of $\Bbbk[x]$ into $\Bbbk$ given by evaluation at 0 yields $\sum_j c_j(0)t_j = 0$. By the assumed linear independence of $t_1, \ldots, t_n$ over $\Bbbk$, $c_j(0) = 0$ for all j. This contradicts the fact that $c_{j_0}(0) \neq 0$. Then (b) is immediate. For (c), we know that $[\mathbb{F} : \Bbbk(x)] < \infty$, and therefore $[\Bbbk'(x) : \Bbbk(x)] < \infty$. By (b), $[\Bbbk' : \Bbbk] < \infty$.

2. This is immediate from Proposition 7.15. Alternatively, here is a direct proof. We may assume that the characteristic is p. It is enough to prove that if K is perfect and L is a finite extension, then L is perfect. Arguing by contradiction, we may assume that $[L : K]$ is as small as possible among all counterexamples. The image M of L under $x \mapsto x^p$ is a subfield of L, and M contains K because K is perfect. We cannot have $M = L$, since L is assumed not to be perfect. By construction of L, M is perfect. Composing $x \mapsto x^p$ from L into M with $x \mapsto x^{1/p}$ from M into itself, we obtain a field map of L onto M that fixes M. The result is a one-one M linear transformation of the finite-dimensional M vector space L onto a proper vector subspace, contradiction.

3. Let $\mathbb{F}$ be a function field in one variable over $\Bbbk$. Since $\Bbbk$ is perfect, Theorem 7.20 shows that $\mathbb{F}$ is separably generated. Let us write $\mathbb{F} = \Bbbk(x_1, \ldots, x_n)$. Theorem 7.18 shows that there is some x_j such that $\mathbb{F}$ is a separable extension of $\Bbbk(x_j)$. If we write x for x_j, then the Theorem of the Primitive Element shows that $\mathbb{F} = \Bbbk(x)[y]$ for some y algebraic over $\Bbbk(x)$. Put $R = \Bbbk[x][y] = \Bbbk[x, y]$; the field of fractions of R is $\mathbb{F}$. Let $g(x, Y)$ be the minimal polynomial of y over $\Bbbk(x)$. If $d(x)$ is a common denominator for the coefficients of $g(x, Y)$, then $d(x) \neq 0$ because x is transcendental over $\Bbbk$. If we set $f(X, Y) = d(X)g(X, Y)$, then $f(x, y) = 0$. Hence the substitution homomorphism $\Bbbk[X, Y] \to R$ given by replacing X by x and Y by y factors through to a homomorphism φ carrying $\Bbbk[X, Y]/(f(X, Y))$ onto R. The ring R is an integral domain; hence the ideal $(f(X, Y))$ is prime, and $f(X, Y)$ is irreducible. We can find an ideal I in $\Bbbk[X, Y]$ containing $(f(X, Y))$ such that φ descends to an isomorphism of $\Bbbk[X, Y]/I$ onto R. This ideal I has to be prime, and we let J be a maximal ideal

of $\Bbbk[X, Y]$ containing it. Then we have a chain of inclusions of prime ideals

$$0 \subsetneqq (f(X, Y)) \subseteq I \subseteq J.$$

Theorem 7.22 shows that $\Bbbk[X, Y]$ has Krull dimension 2, and it follows that either $(f(X, Y)) = I$ in the above chain of inclusions, or $I = J$. The latter equality would mean that I is maximal and therefore that $R \cong \Bbbk[X, Y]/I$ is a field; this is not the case, and thus $(f(X, Y)) = I$. Hence $R \cong \Bbbk[X, Y]/(f(X, Y))$. Here $f(X, Y)$ is an affine plane curve irreducible over $\Bbbk$, and the field of fractions of R is by definition the function field of the curve; this field is $\mathbb{F}$, and the argument is complete.

4. The singular points are common zeros of f, $\frac{\partial f}{\partial X}$, and $\frac{\partial f}{\partial Y}$. If there are infinitely many, then Bezout's Theorem says that f and $\frac{\partial f}{\partial X}$ have a nontrivial common factor, and so do f and $\frac{\partial f}{\partial Y}$. Since f is irreducible and the partial derivatives reduce degrees in one or the other variable, we must have $\frac{\partial f}{\partial X} = \frac{\partial f}{\partial Y} = 0$ as polynomials. This is impossible in characteristic 0. In characteristic p, the first condition says that the only powers of X that appear in f are powers of X^p, and the second condition says that the only powers of Y that appear are powers of Y^p. The coefficients of f are powers of p because $\Bbbk$ is assumed perfect, and thus f is exhibited as a p^{th} power, in contradiction to its assumed irreducibility.

5. Differentiate $f(X, b) = (X - a)f_1(X)$ and evaluate at (a, b) to obtain $\frac{\partial f}{\partial X}(a, b) = f_1(a) + (a - a)f_1'(a) = f_1(a)$.

6. Multiply the equation $g(X, b) = (X-a)g_1(X)$ by $f_1(X)$ and substitute to obtain $g(X, b)f_1(X) = f(X, b)g_1(X)$. Then the function $g(X, \cdot)f_1(X) - f(X, \cdot)g_1(X)$ is 0 at b and is of the form $g(X, Y)f_1(X) - f(X, Y)g_1(X) = (Y - b)h_1(X, Y)$, where $h_1(X, Y)$ for each X is a polynomial in Y. Since $(Y - b)h_1(X, Y)$ is equal to a polynomial in (X, Y), $h_1(X, Y)$ is a polynomial in (X, Y). To complete the problem, evaluate both sides at (x, y), and use the facts that $f(x, y) = 0$ and that $f_1(x) \neq 0$.

7. Since $\mathbb{F} = \Bbbk(x, y)$ is a function field in one variable, it is enough to see that y is transcendental over $\Bbbk$. Arguing by contradiction, suppose that there is some nonzero polynomial $c(Y)$ in $\Bbbk[Y]$ having y as a root. As a polynomial in $\Bbbk[X, Y]$, $c(Y)$ maps to $c(y) = 0$ when we pass to the quotient in $\Bbbk[X, Y]/(f(X, Y))$, and therefore $c(Y)$ is the product of $f(X, Y)$ by a polynomial. On the other hand, $\frac{\partial f}{\partial X}$ is not 0, and thus $f(X, Y)$ depends nontrivially on X. Hence the product of $f(X, Y)$ and any nonzero polynomial in (X, Y) depends nontrivially on X, contradiction. The result now follows from the observation at the end of Section 1.

8. Substituting a for x in the formula for $g(x, y)$ gives

$$g(a, y) = (y - b)^k h_k(a, y)/f_1(a)^k.$$

In this formula, $h_k(a, y)$ is a polynomial expression in y, hence also in $y - b$. Thus v_1 is ≥ 0 on it. The expression $f_1(a)^k$ is a nonzero member of $\Bbbk$, on which v_1 takes the value 0. Therefore

$$v_1(g(a, y)) = kv_1(y - b) + v_1(h_k(a, y)) \geq kv_1(y - b).$$

The left side is independent of k, and the right side is unbounded in k. Therefore there is some upper bound to the values of k for which $g(x, y)$ has an expansion of the kind in question.

9. For (a), we cannot have $h_k(a, b) = 0$ in Problem 8 for arbitrarily large k because of the bound found in Problem 8. If $k = n$ is the smallest k for which $h_k(a, b) \neq 0$, then the displayed formula holds with $h = h_n$. For uniqueness we substitute a for x and see that $g(a, y) = p_n(y)(y-b)^n$ for a polynomial p_n with $p_n(b) \neq 0$. We cannot have two such expressions involving distinct powers n because y is transcendental over $\Bbbk$.

For (b), we see from (a) that every nonzero member of R is of the required form with $n \geq 0$. Since $\mathbb{F}$ is the field of fractions of R, the same thing is true for $\mathbb{F}$ as long as we allow n to be arbitrary in $\mathbb{Z}$.

For (c), if we have two such expressions, we set them equal, clear fractions, and write the result as $(y-b)^k p(x, y) = q(x, y)$ for some $k \geq 0$ and for some polynomials p and q with $p(a, b) \neq 0$ and $q(a, b) \neq 0$. Substituting (a, b) for (x, y), we obtain 0 from $(y - b)^k p(x, y)$ unless $k = 0$, and we obtain something nonzero from $q(x, y)$. Therefore $k = 0$, and the required uniqueness follows.

10. From the definition we immediately have $v(g) = +\infty$ if and only if $g = 0$, as well as $v(gg') = v(g) + v(g')$ for all g and g'. We are to show that $v(g + g') \geq \min(v(g), v(g'))$. Thus write $g(x, y) = (y - b)^n h_1(x, y)/h_2(x, y)$ and $g'(x, y) = (y - b)^m h_1'(x, y)/h_2'(x, y)$ with $n \leq m$. Then $\min(v(g), v(g')) = \min(n, m) = n$. Also,

$$g + g' = (y - b)^n \, \frac{h_1 h_2' + (y-b)^{m-n} h_2 h_1'}{h_2 h_2'}.$$

The numerator of the displayed fraction is a polynomial and can be written in the form of Problem 9a. Say that $(y - b)^k$ is the power of $(y - b)$ that appears in it, k being ≥ 0. Then $v(g + g') = n + k$, and this is $\geq n = \min(v(g), v(g'))$. The assertions about the valuation ring and the valuation ideal are clear.

11. Let v' be a second valuation having the stated properties. If $g(x, y)$ is given in $\mathbb{F}^\times$, decompose g as in Problem 9b, and apply v'. Then we obtain $v'(g(x, y)) = nv'(y - b) + v'(h_1(x, y)) - v'(h_2(x, y))$. The assumptions on v' show that $v'(h_1(x, y)) = v'(h_2(x, y)) = 0$. Therefore

$$v'(g(x, y)) = nv'(y - b) = v'(y - b)v(g(x, y)),$$

and $v' = v'(y - b)v$. By assumption, $v'(y - b)$ is positive. Since v' has to be onto $\mathbb{Z} \cup \{\infty\}$, we must have $v'(y - b) = 1$.

12. For (a), the argument is the same as with Problem 7 except that the roles of x and y are reversed. The partial derivative $\frac{\partial(y^2 - f(x))}{\partial y} = 2y$ is not the 0 element because the characteristic is not 2, and hence that earlier argument applies. Part (b) is elementary field theory, and (d) is a routine verification.

For (c), let $\Bbbk'$ be the subfield of elements of $\mathbb{F}$ algebraic over $\Bbbk$. Problem 1 shows that $[\Bbbk' : \Bbbk] \leq [\Bbbk'(x) : \Bbbk(x)] \leq [\mathbb{F} : \Bbbk] = 2$. Arguing by contradiction, suppose

that $\{1, t\}$ is a basis of $\Bbbk'$ over $\Bbbk$. let $X^2 + uX + v$ be the minimal polynomial of t over $\Bbbk$; t satisfies $t^2 + ut + v = 0$. Problem 1a shows that $t = a(x) + yb(x)$ with $b(x) \neq 0$, and then t satisfies $t^2 - 2a(x)t + (a(x)^2 - f(x)b(x)^2) = 0$. Hence $ut + v = -2a(x)t + (a(x)^2 - f(x)b(x)^2)$. If $u \neq -2a(x)$, then we can solve for t and obtain the contradiction that t is in $\Bbbk(x)$. Thus $u = -2a(x)$, and also $v = a(x)^2 - f(x)b(x)^2$. Since x is transcendental over $\Bbbk$, the first of these shows that $a(x)$ does not involve x, i.e., $a(x)$ lies in $\Bbbk$. Then the second shows that $f(x)b(x)^2$ lies in $\Bbbk$, and unique factorization leads to the conclusion that $f(x)$ and $b(x)$ do not depend on x. This contradicts the assumption that $f(X)$ is nonconstant.

13. Let $z = a(x) + yb(x)$ be in the integral closure. Then so is the image of z under the nontrivial Galois group element σ, and so are $z + \sigma(z)$ and $z\sigma(z)$. The latter elements are $2a(x)$ and $a(x)^2 - f(x)b(x)^2$. Thus $a(x)$ is in the intersection of the integral closure with $\Bbbk(x)$, which is $\Bbbk[x]$ because $\Bbbk[x]$ is a principal ideal domain and is integrally closed. Then $f(x)b(x)^2$ is in $\Bbbk[x]$ by the same argument. Since $f(x)$ is square free, it follows that $b(x)$ is in $\Bbbk[x]$.

14. Part (a) is immediate from Corollary 6.6. Discrete valuations of $\mathbb{F}$ that are not in $D_{\mathbb{F}}$ play no role because of the inclusion $\Bbbk \subseteq R$: any discrete valuation that is ≥ 0 on R has to be 0 on $\Bbbk^\times$, since the image of $\Bbbk^\times$ under the valuation is a subgroup of $\mathbb{Z}$.

For (b), the condition for $z \neq 0$ to be in $p(x)_\infty$ is that $v(z) \geq -p \operatorname{ord}_v(x)_\infty$ for all $v \in D_{\mathbb{F}}$. If a particular v has $v(x) \geq 0$, then v does not contribute to $(x)_\infty$, and this condition says that $v(z) \geq 0$. By (a), z is in R.

15. For (a), let $c(x) = c_n x^n + \cdots + c_0 = x^n(c_n + c_{n-1}x^{-1} + \cdots + c_0 x^{-n})$ with $c_n \neq 0$. Then $v(c_n) = 0$, and $v(c_j x^{j-n}) > 0$ for $j < n$. Hence

$$\begin{aligned} v\big(x^n(c_n + c_{n-1}x^{-1} + \cdots + c_0x^{-n})\big) &= nv(x) + v(c_n + c_{n-1}x^{-1} + \cdots + c_0x^{-n}) \\ &= nv(x) + v(c_n) = nv(x). \end{aligned}$$

For (b), $2v(y) = v(y^2) = v(f(x)) = (\deg f)v(x)$, the latter equality holding by (a). In (c), we have

$$\begin{aligned} v(a(x) + yb(x)) &\geq \min\big(v(a(x)), v(yb(x))\big) \\ &= \min\big(v(a(x)), v(y) + v(b(x))\big) \\ &= \min\big((\deg a)v(x), (\tfrac{1}{2}\deg f + \deg b)v(x)\big) \\ &= v(x)\max\big(\deg a, \tfrac{1}{2}\deg f + \deg b\big) \geq pv(x). \end{aligned}$$

16. Any $v \in D_{\mathbb{F}}$ with $v(x) \geq 0$ has $v(z) \geq 0 = -\operatorname{ord}_v(x)_\infty$ on all elements $z = a(x) + yb(x)$ with $a(x)$ and $b(x)$ in $\Bbbk[x]$, by Problems 13 and 14a. Suppose that $v(x) < 0$. Then Problem 15c and the assumptions on the degrees of $a(x)$ and $b(x)$ shows that $v(z) \geq pv(x) = -p \operatorname{ord}_v(x)_\infty$. Hence $(z) \geq -p(x)_\infty$, and z lies in $L(p(x)_\infty)$.

18. For (a), let σ be the nontrivial element of the Galois group. Problem 17c shows that if $z = a(x) + yb(x)$ is in $L(p(x)_\infty)$, then so is $\sigma(z) = a(x) - yb(x)$. Hence any $v \in D_{\mathbb{F}}$ with $v(x) < 0$ has $v(a(x) + yb(x)) \geq -p \operatorname{ord}_v(x)_\infty = pv(x)$ and $v(a(x) - yb(x)) \geq -p \operatorname{ord}_v(x)_\infty = pv(x)$. Consequently

$$\begin{aligned} v(a(x)) = v(2a(x)) &\geq \min\big(v(a(x) + yb(x)),\, v(a(x) - yb(x))\big) \\ &\geq \min\big(pv(x),\, pv(x)\big) = pv(x) \end{aligned}$$

and

$$v\big(a(x)^2 - f(x)b(x)^2\big) = v(a(x) + yb(x)) + v(a(x) - yb(x)) \geq pv(x) + pv(x).$$

Using Problem 15a and the fact that $v(x) < 0$, we see from these two inequalities that $\deg a \leq p$ and $\deg(a^2 - fb^2) \leq 2p$.

For (b), Problem 14b shows that $L(p(x)_\infty) \subseteq R$, and Problem 13 shows that R consists of all $a(x) + yb(x)$ with $a(x)$ and $b(x)$ in $\Bbbk[x]$. Part (a) thus shows that $\deg a \leq p$ and $\deg(a^2 - fb^2) \leq 2p$. Since $\deg a \leq p$, the second of these inequalities shows that $\deg fb^2 \leq 2p$. Thus $\deg b + \frac{1}{2}\deg f \leq p$. In the reverse direction, if $a(x)$ and $b(x)$ are polynomials satisfying the degree relations, then Problem 16 shows that $a(x) + yb(x)$ is in $L(p(x)_\infty)$.

19. The polynomials $a(x)$ and $b(x)$ are limited only by the restrictions on their degrees. From $\deg a \leq p$, we get a space of dimension $p+1$. From $\deg b + \frac{1}{2}\deg f \leq p$, we have $\deg b \leq \big[p - \frac{1}{2}\deg f\big]$, and we get a space of dimension $\big[p - \frac{1}{2}\deg f\big] + 1$ if $\big[p - \frac{1}{2}\deg f\big] \geq 0$. Thus

$$\begin{aligned} \ell(p(x)_\infty) &= (p+1) + \big[p - \tfrac{1}{2}\deg f\big] + 1 \\ &= 2p + 2 + \big[-\tfrac{1}{2}\deg f\big] = 2p + 2 - \big[\tfrac{1}{2}(1 + \deg f)\big] \end{aligned}$$

if $p \geq -\big[-\frac{1}{2}\deg f\big] = +\big[\frac{1}{2}(1 + \deg f\big]$.

20. Part (a) is immediate from Theorem 9.3, since $[\mathbb{F} : \Bbbk(x)] = 2$. For (b), Theorem 9.9 and Problem 19, in combination with the result of (a), show for sufficiently large positive p that

$$1 - g = \ell\big(p(x)_\infty\big) - p\deg(x)_\infty = 2p + 2 - \big[\tfrac{1}{2}(1 + \deg f\big] - 2p.$$

Hence $g = \big[\frac{1}{2}(1 + \deg f\big] - 1$.

21. Let $\Phi : \Bbbk(X)[Y] \to \Bbbk(X)[Z]$ be the substitution homomorphism that fixes $\Bbbk(X)$ and has $\Phi(Y) = g(X)Z$, and follow it with the quotient homomorphism to $\Bbbk(X)[Z]/(Z^2 - h(X))$. Then

$$\Phi(Y^2 - f(X)) = g(X)^2Z^2 - f(X) = g(X)^2(Z^2 - h(X)),$$

which goes to 0 in the quotient. Thus the composition of Φ followed by the quotient map descends to a field map $\varphi : \Bbbk(X)[Y]/(Y^2 - f(X)) \to \Bbbk(X)[Z]/(Z^2 - h(X))$. The inverse is constructed in the same way, starting from the formula $\Psi(Z) = g(X)^{-1}Y$.

22. For (a), the conclusion genus 1 when there are no repeated roots is immediate from Problem 20b with $\deg f = 3$. If there are repeated roots, then we can write $f(X) = g(X)^2 h(X)$ with $\deg g = \deg h = 1$. Applying Problem 21, we see that the genus is the same as for Problem 20b with $\deg f = 1$, i.e., the genus is 0.

For (b), a singularity occurs only at points (x, y) of the zero locus in $\mathbb{k}_{\text{alg}}^2$ at which both first partials are 0. Then $2Y = 0$, which says that $y = 0$ because the characteristic is not 2, and $f'(X) = 0$, which says that x is a root in $\mathbb{k}_{\text{alg}}$ of both $f(X)$ and $f'(X)$. This means that x is at least a double root in $\mathbb{k}_{\text{alg}}$ of $f(X)$.

23. The residue class degree f_v is 1, since $\mathbb{k}$ is algebraically closed. Thus $\deg nv = n$. Corollary 9.4 gives $\ell(0v) = 1$, Corollaries 9.22 and 9.23 together give $\ell(1v) = 1$ if $g \geq 1$, and Corollary 9.19 gives $\ell((2g-1)v) = \deg((2g-1)v) + (1-g) = (2g-1) + (1-g) = g$ and $\ell(2gv) = \deg(2gv) + (1-g) = g+1$. The inequality $\ell(nv) \leq \ell((n+1)v) \leq \ell(nv) + 1$ follows by combining Theorem 9.6, the fact that $A \leq B$ implies $L(A) \subseteq L(B)$, and the fact that $f_v = 1$.

24. For each $n \geq 0$,

$$L(nv) = \{0\} \cup \{x \in \mathbb{F}^\times \mid -(x)_\infty \geq -nv\} = \{0\} \cup \{x \in \mathbb{F}^\times \mid (x)_\infty \leq nv\}.$$

Thus $n \geq 1$ is a gap if and only if $\ell(nv) = \ell((n-1)v)$, and otherwise $\ell(nv) = \ell((n-1)v) + 1$ by the last fact in Problem 23.

Suppose that there are m gaps in passing from $\ell(0v)$ to $\ell(2gv)$. In the process we take $2g$ steps from $(n-1)v$ to nv, of which m are gaps and $2g-m$ are nongaps. (The gaps are certain of these integers n, $1 \leq n \leq 2g$.) Since $\ell(0v) = 1$ and $\ell(2gv) = g+1$ by Problem 23, the total number of nongaps is $(g+1) - 1 = g$. Solving $2g - m = g$ gives $m = g$. The formulas $\ell((2g-1)v) = g$ and $\ell(2gv) = g+1$ from Problem 23 show that $2g$ is not a gap.

25. For (a), if the gap sequence is $(1, 2, \ldots, g)$, then $1 = \ell(0v) = \ell(1v) = \ell(2v) = \cdots = \ell(gv)$. Conversely if the gap sequence is something else, let n with $1 \leq n \leq g$ be the first nongap; then $1 = \ell(0v) = \cdots = \ell((n-1)v) < \ell(nv) \leq \ell(gv)$.

For (b), Problem 23 gives $\ell(0v) = \ell(1v) = 1$ if $g \geq 1$, and thus 1 is a gap.

For (c), there are no integers strictly between 0 and $2g$ if $g = 1$, and the only such integer for $g = 1$ is 1. Part (b) shows that the gap sequence is indeed (1) if $g = 1$, and thus the gap sequence is always the standard one.

For (d), we have some x and y in $\mathbb{F}^\times$ with $(x)_\infty = rv$ and $(y)_\infty = sv$. Thus $(x) = (x)_0 - rv$ and $(y) = (y)_0 - sv$, and $(xy) = (x)_0 + (y_0) - (r+s)v$. Since v does not contribute to $(x)_0$ and $(y)_0$, $(xy)_\infty = (r+s)v$, and thus $r+s$ is a nongap.

For (e), if 2 is a nongap, then iteration of (d) shows that $2, 4, 6, \ldots, 2g-2$ are nongaps. The only possible gaps are the remaining integers from 1 to $2g-1$, namely $1, 3, 5, \ldots, 2g-1$. There are g of these, and so all of them must be gaps.

Chapter X

1. If F is in $I(P)$, expand F as a sum of homogeneous terms $F = \sum_{d=0}^{\infty} F_d$. Then $0 = F(tx_0, \dots, tx_n) = \sum_{d=0}^{\infty} F_d(tx_0, \dots, tx_n) = \sum_{d=0}^{\infty} F_d(x_0, \dots, x_n)t^d$ for all $t \in \Bbbk^\times$. Since $\Bbbk$ is infinite, every coefficient of this polynomial in t is 0. Thus each F_d is in $I(P)$, and $I(P)$ is generated by homogeneous elements.

2. In each part we argue by contradiction. For (a), if $\{X_\alpha\}$ is a system of nonempty closed subsets of X with the finite intersection property such that $\bigcap_\alpha X_\alpha = \varnothing$, then we can inductively define a strictly decreasing sequence of finite intersections of the X_α's, in contradiction to the Noetherian property. In (b), if E is a closed irreducible subset that is not connected, then $E = U \cup V$ with U and V nonempty, disjoint, and relatively open. Then $E = U^c \cup V^c$ contradicts the irreducibility of E.

3. For (a), the continuous image of a connected set is connected. Continuity is by Proposition 10.32, and connectedness is by Problem 2b applied to the Noetherian topological space V. For (b), if f is any polynomial function on $\mathbb{A}^n$, then $f \circ \varphi$ is in $\mathcal{O}(V)$ because φ is a morphism, and $f \circ \varphi$ is constant by Corollary 10.31. Then φ cannot have two distinct points in its image, since any two points in $\mathbb{A}^n$ can be distinguished by some polynomial.

4. Certainly $\mathcal{O}(U) \supseteq \Bbbk[X, Y]$. Also, the function field $\Bbbk(U)$ consists of all quotients of polynomials a/b with a and b in $\Bbbk[X, Y]$ and $b \neq 0$. Thus suppose that $f = a/b$ lies in $\mathcal{O}(U)$. By unique factorization in $\Bbbk[X, Y]$, we may assume that a and b are relatively prime. In the expression $f = a/b$, regularity at P implies that $b(P) \neq 0$ because an equality $a/b = c/d$ of two such expressions implies that $a = kc$ and $b = kd$ for some nonzero scalar k. Since f is regular everywhere in $\mathbb{A}^2$ except possibly at the origin, $b(X, Y)$ is nonvanishing away from the origin. However, if b is nonconstant, then $V(b)$ is a curve and has dimension 1, whereas the origin has dimension 0. We conclude that b is constant, and $f = a/b$ is in $\Bbbk[X, Y]$.

5. Arguing by contradiction, let $\varphi : W \to U$ be an isomorphism from an affine variety onto U. Then the map $\widetilde{\varphi} : \mathcal{O}(U) \to \mathcal{O}(W) = A(W)$ given by $\widetilde{\varphi}(f) = f \circ \varphi$ is an isomorphism. Let $\iota : U \to \mathbb{A}^2$ be the inclusion. The corresponding map on regular functions is $\widetilde{\iota} : A(\mathbb{A}^2) \to \mathcal{O}(U)$ given by $\widetilde{\iota}(h)(x, y) = h(x, y)$ for $(x, y) \neq (0, 0)$, and it is an isomorphism by Problem 4. Then $(\varphi \circ \iota)^{\sim} = \widetilde{\iota} \circ \widetilde{\varphi}$ is an isomorphism of $A(\mathbb{A}^2)$ onto $A(W)$. Its inverse has to be of the form $\widetilde{\psi}$ with $\widetilde{\psi}(g) = g \circ \psi$ for some isomorphism $\psi : \mathbb{A}^2 \to W$, according to Theorem 10.38. Since $\widetilde{\psi} \circ \widetilde{\varphi} \circ \widetilde{\iota}$ is the identity map on $A(\mathbb{A}^2)$, $\iota \circ \varphi \circ \psi$ is the identity map on $\mathbb{A}^2$. Using the definition of ι shows that $\varphi \circ \psi(x, y) = (x, y)$ for $(x, y) \neq (0, 0)$. Thus $\varphi \circ \psi$ is an isomorphism of $\mathbb{A}^2$ onto U that is the identity on U. This is a contradiction, since there is no possible image for $(0, 0)$ under $\varphi \circ \psi$ that makes $\varphi \circ \psi$ one-one.

6. Let φ be the rational map of the irreducible curve C into the irreducible curve C', and let (E, φ_E) be a morphism in the class φ. If φ is not dominant, then $\overline{\varphi_E(E)}$ is a proper closed subset of C' and must be finite. Hence $\varphi_E(E)$ is finite. The set E is connected by Problem 2b, and morphisms are continuous by definition. Therefore

$\varphi_E(E)$ is connected. Being connected and finite, it is a singleton set $\{y\}$. If φ_C is defined as everywhere equal to y on C, then (C, φ_C) is in the equivalence class φ. So φ is constant.

7. Suppose that f is a member of $\mathcal{O}_{\varphi(P)}(V)$ with $\varphi_P^*(f) = 0$. Since the set on which $f \in \Bbbk(V)$ is regular is open, there exists an open neighborhood E of $\varphi(P)$ on which f is defined. The morphism φ is continuous, and thus $\varphi^{-1}(E)$ is open in U. Since φ is a morphism and f is regular on E, $f \circ \varphi$ is regular on $\varphi^{-1}(E)$. According to the proof of Proposition 10.42, $\varphi_P^*(f)$ is defined to be the unique member of $\Bbbk(V)$ that agrees with $f \circ \varphi$ on $\varphi^{-1}(E)$. We are assuming $\varphi_P^*(f)$ to be 0, and thus $f \circ \varphi$ equals 0 on $\varphi^{-1}(E)$. By dominance of φ, $\varphi(\varphi^{-1}(E))$ is a dense subset of E. Thus the continuous function f is 0 on a dense subset of its domain E and is 0.

8. The inclusion $(WX - YZ) \subseteq (X, Z)$ yields a homomorphism φ of $A(V)$ onto $\Bbbk[W, X, Y, Z]/(X, Z) \cong \Bbbk[W, Y]$. Let $b' = \varphi(\bar{b})$. Then $b'(w, y) = \bar{b}(w, 0, y, 0)$ is a polynomial in (w, y) nonzero in the complement of the origin. The solution of Problem 4 shows that $b'(0, 0) \neq 0$. Thus $\bar{b}(0, 0, 0, 0) \neq 0$, and f is defined at $(0, 0, 0, 0)$. In view of the discussion of this example in Section 4, f is everywhere defined. Therefore it is in $\mathcal{O}(V)$, which equals $A(V)$ because V is an affine variety. Thus there is a polynomial g in $\Bbbk[W, X, Y, Z]$ whose image $\bar{g}$ in $A(V)$ equals $\overline{X}/\overline{Y}$. Then $\overline{Y}\bar{g} = \overline{X}$, and $Yg = X + (WX - YZ)h$ for some polynomial h. So $Y(g + hZ) = X(1 + Wh)$. This implies that Y divides $1 + Wh$, which we see is impossible by evaluating at the origin.

9. The equivalence of continuity of φ and continuity of all φ_α will be taken as known. Suppose that $\varphi : U \to V$ is a morphism. Let an index α, an open set $E \subseteq V_\alpha$, and a member f of $\mathcal{O}(E)$ be given. We are to show that $f \circ \varphi_\alpha$ is in $\mathcal{O}(\varphi_\alpha^{-1}(E))$. Since φ is a morphism and E is open in V, we know that $f \circ \varphi$ is in $\mathcal{O}(\varphi^{-1}(E))$. By restriction, $f \circ \varphi_\alpha$ is in $\mathcal{O}(U_\alpha \cap \varphi^{-1}(E)) = \mathcal{O}(\varphi_\alpha^{-1}(E))$. Thus φ_α is a morphism.

In the reverse direction suppose that all $\varphi_\alpha : U_\alpha \to V_\alpha$ are morphisms. Let E be open in V, and let f be in $\mathcal{O}(E)$. We are to show that $f \circ \varphi$ is in $\mathcal{O}(\varphi^{-1}(E))$. Since $\varphi^{-1}(E) = \bigcup_\alpha (U_\alpha \cap \varphi^{-1}(E))$, it is enough to prove regularity of $f \circ \varphi$ on each $U_\alpha \cap \varphi^{-1}(E)$. On this open set, $f \circ \varphi$ equals $f \circ \varphi_\alpha$, which is regular because φ_α is a morphism. Thus φ is a morphism.

10. For (a), we use the equivalence of regularity with the condition in Proposition 10.28. Thus regularity at P in U means that there is a subneighborhood U_0 of U within V about P such that f equals a quotient $\bar{a}/\bar{b}$ on U_0 with $\bar{a}$ and $\bar{b}$ in $A(V)$ and with $\bar{b}$ nowhere vanishing on U_0. Choose polynomials a and b in $\Bbbk[X_1, \ldots, X_n]$ that restrict to $\bar{a}$ and $\bar{b}$ on V. Let U_0' be an open subset of $\mathbb{A}^n$ whose intersection with V is U_0. Since b is nowhere 0 on U_0 and is continuous on U_0', the subset $\widetilde{U}_0$ of U_1 on which b is nonvanishing is open and contains U_0. Then Proposition 10.28 shows that $F = a/b$ is a member of $\mathcal{O}(\widetilde{U}_0)$ whose restriction to U_0 equals f.

For (b), the result of (a) is local. Thus we can immediately allow V to be quasi-affine. Using Proposition 10.37, we can extend (a) to the case that V is quasiprojective.

11. Continuity is no problem. For the condition involving regularity, we use Problem 10. Let E be a relatively open set in V, and let f be in $\mathcal{O}(E)$. We are to show that $f \circ \varphi$ is in $\mathcal{O}(\varphi^{-1}(E))$. Thus let P be in $\varphi^{-1}(E) \subseteq U$; then $\varphi(P)$ is in $E \subseteq V$. Since f is in $\mathcal{O}(E)$, Problem 10 produces a relatively open neighborhood E_0 of $\varphi(P)$, an open subset $\widetilde{E}_0$ of Y with $\widetilde{E}_0 \cap V = E_0$, and a function F in $\mathcal{O}(\widetilde{E}_0)$ such that $F\big|_{E_0} = f\big|_{E_0}$. Since $\varphi : X \to Y$ is a morphism, $F \circ \varphi$ is in $\mathcal{O}(\varphi^{-1}(\widetilde{E}_0))$. Since $\varphi(\varphi^{-1}(\widetilde{E}_0) \cap U) \subseteq \widetilde{E}_0 \cap V = E_0$, $F \circ \varphi$ agrees with $f \circ \varphi$ on $\varphi^{-1}(\widetilde{E}_0) \cap U$. Thus $f \circ \varphi$ has an extension $F \circ \varphi$ from $\varphi^{-1}(\widetilde{E}_0) \cap U$ to $\varphi^{-1}(\widetilde{E}_0)$ that is in $\mathcal{O}(\widetilde{E}_0)$. The quotients that exhibit $F \circ \varphi$ as defined at points of $\varphi^{-1}(\widetilde{E}_0) \cap U$ exhibit $f \circ \varphi$ as defined there. The inclusion $\varphi^{-1}(E_0) = \varphi^{-1}(\widetilde{E}_0 \cap V) = \varphi^{-1}(\widetilde{E}_0) \cap \varphi^{-1}(V) \subseteq \varphi^{-1}(\widetilde{E}_0) \cap U$ shows that $f \circ \varphi$ is in $\mathcal{O}(\varphi^{-1}(E_0))$. This being true for all P in $\varphi^{-1}(E)$, $f \circ \varphi$ is in $\mathcal{O}(\varphi^{-1}(E))$.

12. Part (a) follows by applying instances of Problem 11 to φ and φ^{-1}. Then (b) follows by another application of Problem 11. Part (c) follows by inductive application of (b).

13. Let d_i be the degree of homogeneity of F_i. Then the i^{th} row of the right-hand matrix is $\lambda^{d_i - 1}$ times the i^{th} row of the left-hand matrix. Hence the dimension of the span of the rows is the same for the two matrices, and this number is the rank.

14. This comes down to the fact that differentiating with respect to X_j for $j > 0$ and then setting X_0 equal to 1 is the same as setting X_0 equal to 1 and then differentiating with respect to X_j.

15. For any of the functions F_i, the right side of the formula in Euler's Theorem is 0 at $(x_0, \dots, x_n)$ by assumption. Hence Euler's Theorem gives $x_0 \frac{\partial F_i}{\partial X_0}(x_0, \dots, x_n) = -\sum_{j=1}^n x_j \frac{\partial F_i}{\partial X_j}(x_0, \dots, x_n)$. This says that

$$x_0 \times 0^{\text{th}} \text{ column of } J(F)(x_0, \dots, x_n) = -\sum_{j=1}^{n} x_j \times j^{\text{th}} \text{ column of } J(F)(x_0, \dots, x_n).$$

Since $x_0 \neq 0$, this is a relation of the required type.

16. Problem 13 shows that the left side equals rank $J(F)(1, x_1/x_0, \dots, x_n/x_0)$, which Problem 15 shows to be equal to the rank of the matrix formed from the last n columns, which Problem 14 shows to be equal to the rank of $J(f)(x_1/x_0, \dots, x_n/x_0)$.

18. Regard the elements w_{ij} as the entries of a matrix. The given condition is that every 2-by-2 subdeterminant of this matrix equals 0. The matrix is not 0, and consequently its rank is 1. Every matrix over $\Bbbk$ of rank 1 is of the form xy^t for column vectors x and y, and then $[\{w_{ij}\}]$ is exhibited as $\sigma\big([\{x_i\}], [\{y_j\}]\big)$.

19. For (a), one suitable monomial ordering is the lexicographic ordering that takes the elements W_{ij} in the order $W_{00}, W_{01}, \dots, W_{mn}$ with W_{00} largest. Given a monomial M' of total degree d, choose among all monomials of total degree d the smallest one in the ordering that is congruent to M' modulo $\mathfrak{a}$. Write $M = \prod_{i,j} W_{ij}^{a_{ij}}$.

If $a_{ij} > 0$ and if there exists (k, l) with $l > j, k > i$, and $a_{kl} > 0$, then $W_{ij}W_{kl}$ divides M. Write $M_0 = M/W_{ij}W_{kl}$. Put $M'' = M_0W_{il}W_{kj}$. Since $W_{ij}W_{kl} - W_{il}W_{kj}$ is in $\mathfrak{a}$, M'' is congruent to M modulo $\mathfrak{a}$. In the monomial ordering, all of the elements W_{kl}, W_{il}, W_{kj} are smaller than W_{ij}. Therefore $M'' < M$, in contradiction to the minimality of M.

In (b), let the largest W_{ij} whose exponents in M and M' are unequal be $W_{i_0j_0}$. Let the products of the powers of the strictly larger monomials be N and N', respectively. It is enough to prove that $\varphi(M/N) \neq \varphi(M'/N')$. Then we have

$$M/N = \prod_{W_{ij} \le W_{i_0j_0}} W_{ij}^{a_{ij}} = W_{i_0j_0}^{a_{i_0j_0}} \prod_{\substack{(i,j) \text{ with} \\ i_0<i \text{ or} \\ (i_0=i \text{ and } j_0<j)}} W_{ij}^{a_{ij}}$$

and a similar expression for M'/N'. The minimality condition says that $a_{ij} = 0$ if $i_0 < i$ and $j_0 < j$. Thus

$$M/N = \Big(\prod_{i_0<i,\ j_0\ge j} W_{ij}^{a_{ij}}\Big)\Big(\prod_{i_0=i,\ j_0\le j} W_{ij}^{a_{ij}}\Big) = \Big(\prod_{k>i_0}\prod_{l\le j_0} W_{kl}^{a_{kl}}\Big)\Big(\prod_{l\ge j_0} W_{i_0l}^{a_{i_0l}}\Big),$$

and
$$\varphi(M/N) = \Big(\prod_{k>i_0}\prod_{l\le j_0} X_k^{a_{kl}}Y_l^{a_{kl}}\Big)\Big(\prod_{l\ge j_0} X_{i_0}^{a_{i_0l}}Y_l^{a_{i_0l}}\Big).$$

On the right side each pair of indices (k, l) occurs at most once. Thus an equality $\varphi(M/N) = \varphi(M'/N')$ would imply that $a_{kl} = b_{kl}$ for every (k, l). This proves (b).

In (c), we know that $\mathfrak{a} \subseteq \ker\varphi$. If equality fails, then there is a linear combination $\sum_r c_rM_r$ of monomials in $\ker\varphi$ that is not in $\mathfrak{a}$. Applying (a), we may assume that each M_r is reduced. Then $\sum_r c_r\varphi(M_r) = 0$. Each $\varphi(M_r)$ is a monomial, and (b) shows that the various monomials $\varphi(M_r)$ are distinct. Since the set of monomials is linearly independent, each c_r is 0. Therefore $\sum_r c_rM_r = 0$, contradiction.

20. For (a), compute the kernel of the natural substitution homomorphism of $\Bbbk[X_0, \ldots, X_m, Y_0, \ldots, Y_n]$ into $R[Y_0, \ldots, Y_n]$. For (b), let $P = [y_0, y_1, \ldots, y_n]$, $\mathfrak{p} = I(U) \subseteq \Bbbk[X_0, \ldots, X_m]$, and $\mathfrak{q} = I(\{P\} \subseteq \Bbbk[Y_0, \ldots, Y_n]$. The inside homomorphism has kernel $\mathfrak{a}$ by Problem 19. The outside homomorphism takes $X_0, \ldots, X_m$ into R and takes each Y_j to y_jZ, where Z is an indeterminate; its kernel is isomorphic to $\mathfrak{pq}$. The kernel of the composition is $I(\sigma(U \times \{P\}))$, which is prime because $R[Z]$ is an integral domain.

21. See Fulton's book, page 145.

22. See Fulton's book, page 146.

23. For (a), Proposition 10.9 shows that $I(V(I)) = (h(X, Y))$ for an irreducible polynomial h if $\dim V(I) = 1$. The containment $I \subseteq I(V(I))$ shows that each f_j has to be of the form $f_j = a_jh$ for some a_j in $\Bbbk[X, Y]$. Since f_j and h are irreducible, a_j has to be a scalar. Thus $I = (h(X, Y))$, and I is prime. For (b), one can take $I = (Y + X^2, Y - X^2)$, which has $V(I) = \{(0, 0)\}$ and which is not prime because it contains X^2 but not X.

24. Let $\{g_1, \ldots, g_s\}$ be a minimal Gröbner basis, and suppose that $g_j = ab$ is a nontrivial factorization of g_j in $\Bbbk[X_1, \ldots, X_n]$. Since I is prime, we may assume that a lies in I. Then $\mathrm{LM}(g_j) = \mathrm{LM}(a)\,\mathrm{LM}(b)$, and $\mathrm{LM}(a)$ lies in $\mathrm{LT}(I)$. Since $\{g_1, \ldots, g_s\}$ is a Gröbner basis, $\mathrm{LM}(a)$ lies in the monomial ideal $(\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s))$. By Lemma 8.17, $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(a)$ for some i. It follows that $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(g_j)$. Since the Gröbner basis is minimal, $i = j$. That is, $\mathrm{LM}(g_i) = \mathrm{LM}(a) = \mathrm{LM}(g_j)$. Thus $\mathrm{LM}(b) = 1$, in contradiction to the assumption that the factorization of g_j is nontrivial.

25. Identify $a_{11}X^2 + 2a_{12}XY + a_{22}Y^2 + 2a_{13}XZ + 2a_{23}YZ + a_{33}Z^2$ with the symmetric matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}.$$

By the Principal Axis Theorem choose an invertible matrix M such that $A' = M^t AM$ is diagonal. Put $\begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = M^{-1} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$ and substitute. Then the given quadratic polynomial equals $\alpha X'^2 + \beta Y'^2 + \gamma Z'^2$, where α, β, γ are the diagonal entries of A'. If $\alpha\beta\gamma = 0$, this is reducible; it is readily checked to be irreducible if $\alpha\beta\gamma \neq 0$. Since $\alpha\beta\gamma = \det A' = (\det M)^2 \det A$, the reducible polynomials correspond to the affine hypersurface on which $\det A = 0$.

26. The first conclusion is a special case of Corollary 9.19. Then take x to be a nonconstant member of $L(2v_O)$, and take y to be a member of $L(3v_O)$ not in the linear span of $\{1, x\}$. Corollary 9.22 shows that $(x)_\infty = 2$, and then the equality $(y)_\infty = 3$ follows from the definitions.

27. These are special cases of Theorem 9.3.

28. Since $2 = [\Bbbk(E) : \Bbbk(x)] = [\Bbbk(E) : \Bbbk(x, y)]\,[\Bbbk(x, y) : \Bbbk(x)]$, the integer $[\Bbbk(E) : \Bbbk(x, y)]$ divides 2. The corresponding equality with 3 and $\Bbbk(y)$ shows that $[\Bbbk(E) : \Bbbk(x, y)]$ divides 3. Therefore $[\Bbbk(E) : \Bbbk(x, y)] = 1$.

29. The values of v_O on the seven listed members of $\Bbbk(E)$ are 0, 2, 3, 4, 5, 6, 6, respectively. The members are all in $L(6v_O)$, which has dimension 6 by Problem 28, and thus the listed members are linearly dependent. If y^2 or x^3 does not contribute to this dependence, then v_O takes distinct values on the remaining six members of $L(6v_O)$, and Problem 19a at the end of Chapter VI gives a contradiction. Hence the coefficients b and c of y^2 and x^3, respectively, are nonzero. If x and y are replaced by $-bcx$ and bc^2y and if the linear combination of terms is then divided by b^3c^4, then the linear dependence takes the form $(y^2 + a_1xy + a_3x) - (x^3 + a_2x^2 + a_4x + a_6) = 0$, as required. Hence φ carries $E - \{0\}$ into $C \cap \mathbb{A}^2$.

30. Certainly $f(X, Y)$ is not divisible by any nonconstant polynomial in X. Thus the only possible reducibility is of the form $f(X, Y) = (Y + p(X))(Y + q(X))$. Expanding out the right side shows that

$$\begin{aligned} p(X) + q(X) &= a_1X + a_3, \\ p(X)q(X) &= -(X^3 + a_2X^2 + a_4X + a_6). \end{aligned}$$

The second equation shows that at least one of $p(X)$ and $q(X)$ has degree > 1, and then the first equation shows that $\deg p(X) = \deg q(X)$. But this equality would mean that $\deg p(X)q(X)$ is even, contradiction. Hence $f(X, Y)$ is irreducible.

31. The function φ is a morphism of $E - \{O\}$ into $C \cap \mathbb{A}^2$ by Lemma 10.39, and the composition with β_0 is a morphism into $\mathbb{P}^2$. Then φ is a morphism of $E - \{O\}$ into C by Problem 11. The class of $(E - \{O\}, \varphi)$ is therefore a rational map of E into C, and Corollary 10.54 shows that φ extends to a morphism $\Phi : E \to C$.

32. Let $\widetilde{\Phi} : \Bbbk(C) \to \Bbbk(E)$ be the field mapping that corresponds to Φ under Theorem 10.45. The field $\Bbbk(C)$ is generated by the functions x_0 and y_0 that pick out the coordinates of points of $C \cap \mathbb{A}^2$, and Theorem 10.45 shows that $\widetilde{\Phi}(x_0) =$ (class of $x_0 \circ \varphi$). For P in $E - \{O\}$, this has $\widetilde{\Phi}(x_0)(P) = x_0(\varphi(P)) = x(P)$, i.e., $\widetilde{\Phi}(x_0) = x$. Similarly $\widetilde{\Phi}(y_0) = y$. Therefore $\widetilde{\Phi}(\Bbbk(C)) = \Bbbk(x, y)$. By Problem 28, $\widetilde{\Phi}$ is onto $\Bbbk(E)$. By Corollary 10.46, Φ is birational.

33. The homogeneous polynomial of degree 3 from which $f(X, Y)$ arises is

$$F(X, Y, W) = (Y^2W + a_1XYW + a_3YW^2) - (X^3 + a_2X^2W + a_4XW^2 + a_6W^3).$$

The points of C on the line at infinity arise by setting $W = 0$ and $F(X, Y, W) = 0$ simultaneously, and the only such point is $[0, 1, 0]$. Computation shows that $\frac{\partial F}{\partial W}(0, 1, 0) = 1$. Consequently $[0, 1, 0]$ is a nonsingular point of C.

34. A point (x_0, y_0) in $\mathbb{A}^2$ is a singular point of C if and only if $f(x_0, y_0) = \frac{\partial f}{\partial X}(x_0, y_0) = \frac{\partial f}{\partial Y}(x_0, y_0) = 0$. At (x_0, y_0), computation shows that

$$\tfrac{\partial^2 f}{\partial X^2} = -6X - 2a_2, \quad \tfrac{\partial^2 f}{\partial X \partial Y} = a_1, \quad \tfrac{\partial^2 f}{\partial Y^2} = 2, \quad \tfrac{\partial^3}{\partial X^3} = -6.$$

All higher-order derivatives are 0. Application of Taylor's formula about (x_0, y_0) therefore gives

$$f(X, Y) = (-3x_0 - a_2)(X - x_0)^2 + a_1(X - x_0)(Y - y_0) + (Y - y_0)^2 - (X - x_0)^3.$$

We put $X = x$ and $Y = y$, taking into account that $f(x, y) = 0$. After division by $(x - x_0)^2$, the result is that

$$((y - y_0)(x - x_0)^{-1})^2 + a_1(y - y_0)(x - x_0)^{-1} = (3x_0 + a_2) + (x - x_0).$$

That is, $z^2 + a_1z = (3x_0 + a_2) + (x - x_0)$. Suppose that P is in $E - \{O\}$ and that $v_P(z) < 0$. Then we have $v_P(z + a_1) < 0$ and

$$0 \le v_P\big((3x_0 + a_2) + (x - x_0)\big) = v_P(z^2 + a_1z) = v_P(z) + v_P(z + a_1) < 0,$$

contradiction. Therefore $v_P(z) \ge 0$. Meanwhile, $v_O(x - x_0) = v_O(x) = -2$ and $v_O(y - y_0) = v_0(y) = -3$. Hence $v_O(z) = (-3) - (-2) = -1$.

35. Corollary 9.22 shows that no member of $\Bbbk(E)$ has the properties of z found in Problem 34. Thus C is nonsingular at every (x_0, y_0). In combination with Problem 33, this shows that C is everywhere nonsingular. By Corollary 10.55, Φ is an isomorphism.