Chapter 2

1. (a) Show every number field of degree 2 over $\mathbb{Q}$ is one of the quadratic fields.

   Let K be a number field of degree 2, and $f(x) = x^2 + px + q$ be its minimum polynomial over $\mathbb{Q}$. Since $p, q \in \mathbb{Q}$ we can multiply through to clear the denominators and give us a polynomial $g(x) = ax^2 + bx + c$ over $\mathbb{Z}$ with the same roots as $f(x)$. Therefore $K = \mathbb{Q}[\sqrt{b^2 - 4ac}]$ is a quadratic field for $m = b^2 - 4ac$.

1. (b) Suppose $K = \mathbb{Q}[\sqrt{m}]$ contains $\sqrt{n}$ for n a squarefree integer. Since K has the basis $\{1, \sqrt{m}\}$, so $\sqrt{n} = p + q\sqrt{m}$ for $p, q \in \mathbb{Q}$. Therefore $n = p^2 + 2pq\sqrt{m} + q^2 m$, so either $p = 0$ or $q = 0$.

   If $p = 0$, then $\sqrt{n} = q\sqrt{m}$ and so $\sqrt{n}/\sqrt{m} = q$. This can only happen if $q = 1$, meaning $m = n$.

   If $q = 0$, then $\sqrt{n} = p$, which can only happen if p is also an integer, contradicting n squarefree.

   Therefore the quadratic fields are each distinct.

2. Let I be the ideal generated by 2 and $1 + \sqrt{-3}$ in the ring $\mathbb{Z}[\sqrt{-3}]$.

   We have $I \neq (2)$ because $1 + \sqrt{-3}$ $(\in I)$ does not have the form $2a + b\sqrt{-3}$ for $a, b \in \mathbb{Z}$. The ideal I^2 is generated by $(4, 2 + 2\sqrt{-3}, -2 + 2\sqrt{-3})$. The number $-2 + 2\sqrt{-3} = 2 + 2\sqrt{-3} - 4$ and so is redundant as a generator; therefore $I^2 = (4, 2 + 2\sqrt{-3}) = 2I$.

   Since $I^2 = 2I$, prime factorization of ideals in $\mathbb{Z}[\sqrt{-3}]$ must not hold; if we did then I would be invertible, meaning it could be cancelled from the right-hand-side of each equality, giving us $I = (2)$ which is not true (from above).

   Suppose P is a prime ideal of $\mathbb{Z}[\sqrt{-3}]$ containing 2. Then $4 \in P$ also. Since $(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4$ and P is a prime ideal, one of $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are also in P. However, if $1 - \sqrt{-3} \in P$ then $1 + \sqrt{-3} \in P$ since $-1 \cdot (1 - \sqrt{-3}) + 2 = 1 + \sqrt{-3}$. Therefore any prime ideal containing (2) also contains I and I is the unique prime ideal that contains (2). Since I cannot be expressed as a product of prime ideals, neither can (2).

   (We should expect this; $\mathbb{Z}[\sqrt{-3}]$ is an order of conductor 2 in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and I is not prime to the conductor, meaning it is not invertible.)

3. Complete the proof of Corollary 2, Theorem 1.

   The statement of the text leaves off with α being an algebraic integer if and only if $2r$ and $r^2 - ms^2$ are both integers, where $r, s \in \mathbb{Q}$.

   $2r$ being an integer requires that $r = \frac{a}{2}$, where a is an integer. Substituting $r = \frac{a}{2}$ into the second equation, we see that $a^2 - 4ms^2$ is an integer divisible by 4. In order for the quantity to be an integer, $s = \frac{b}{2}$, where b is an integer. Therefore α is an algebraic integer of the form $\frac{a+b\sqrt{m}}{2}$ if and only if $a^2 - mb^2 = 0 \mod 4$.

We finish by considering $m \mod 4$ and seeing under which statements the given equation is solvable. The key is that integer squares are either equivalent to 0 or 1 modulo 4.

- $m \equiv 1$ (4): Let a be even - then $a^2 \equiv 0 \mod 4$, and to satisfy the equality, $b^2 \equiv 0 \mod 4$ and so b must also be even. Similarly, if a is odd, then $a^2 \equiv 1 \mod 4$ - to satisfy the equality, b must also be odd. Therefore $\alpha = \frac{a+b\sqrt{m}}{2}$ for all $a \equiv b$ (2) as required.
- $m \equiv 2, 3 \mod 4$: For the equation to be solvable, both a and b must be equivalent to 0 or 2 modulo 4 (and so even), meaning $\alpha = c + d\sqrt{m}$ for $c, d \in \mathbb{Z}$ as required.

4. Suppose $a_0, \ldots, a_{n_1}$ are algebraic integers and α is a complex number satisfiying $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Show the ring $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$ has a finitely generated additive group.

   For each a_i let k_i be the degree of the algebraic integer a_i over $\mathbb{Q}$: therefore for any power $k >= k_i$, it can be written as a linear combination of powers of a_i less than k_i. Additionally any power of α^k where $k \geq n$ can be written as a linear combination of powers of α multiplied by each of the a_i. Therefore only a finite number of powers of $a_0^{m_0} \cdots a_n^{m_n} \alpha^m$ are needed; the a_i terms are capped to be lower than k_i and the α term is capped to be lower than n.

   Since α is a member of a subring of $\mathbb{C}$ that is finitely generated, α is therefore an algebraic integer.

5. Let f be a polynomial over $\mathbb{Z}_p$ where p is a prime. We prove $f(x^p) = (f(x))^p$ by induction on number of terms.

   If $f(x) = kx^b$ where $k \in \mathbb{Z}_p$, then $f(x^p) = kx^{pb} = k^p x^{bp} = (kx^b)^p$ (since $k^p = k$ for all $k \in \mathbb{Z}_p$).

   Next, let $f(x) = g(x) + h(x)$ where $g(x)$ and $h(x)$ have fewer terms than $f(x)$.

$$\begin{aligned} f(x)^p &= (g(x) + h(x))^p \\ &= g(x)^p + h(x)^p + \sum_{k=1} \binom{p}{k} g(x)^k h(x)^{p-k} \\ &= g(x)^p + h(x)^p \\ &= g(x^p) + h(x^p) \text{ (using the inductive hypothesis)} \\ &= f(x^p) \end{aligned}$$

   This is the required result.

6. If f and g are polynomials over a field K and $f^2 \mid g$, then $g = f^2 h$. Therefore $g' = f^2 h' + 2hff'$, so $f \mid g'$.

7. Complete the proof of Corollary 2, Theorem 3.

   Let ϕ_k be the automorphism of $\mathbb{Q}[\omega]$ sending ω to ω^k. Then $(\phi_a \circ \phi_b)(\omega) = (\omega^a)^b = \omega^{ab} = \phi_{ab}$, giving the required result that composition of automorphisms corresponds to multiplication modulo m.

8. (a) Let $\omega = e^{2\pi i/p}$ where p is an odd prime. Then

$$\text{disc}(\omega) = \prod_{1 \le r < s \le n} (\alpha_r - \alpha_s)^2 = \pm p^{p-2}$$

   Therefore

$$\Bigg| \prod_{1 \le r < s \le n} (\alpha_r - \alpha_s) \Bigg| = \sqrt{\pm p^{p-2}} = p^{(p-3)/2}\sqrt{\pm p}$$

   Let $\zeta = e^{2\pi i/3}$. Using the above we have the identity $(\zeta - \zeta^2) = \sqrt{-3}$.

   Let $\zeta = e^{2\pi i/5}$. Note $\zeta^4 = -(\zeta^3 + \zeta^2 + \zeta + 1)$.

   We expand the product:

$$(\zeta - \zeta^2)(\zeta - \zeta^3)(\zeta - z^4)(\zeta^2 - \zeta^3)(\zeta^2 - \zeta^4)(\zeta^3 - \zeta_4) = 10\zeta^3 + 10\zeta^2 + 1$$

   Observing that this product is negative we flip the signs and divide by $5^{(5-3)/2} = 5$ to get the identity $\sqrt{5} = -2\zeta^3 - 2\zeta^2 - 1$.

8. (b) The 8th cyclotomic polynomial is x^4+1, so the 8th cyclotomic field contains all the roots of this equation, which includes $\sqrt{i} = (1/\sqrt{2})(1+i)$ and its complex conjugate $(1/\sqrt{2})(1-i)$. Thus the 8th cyclotomic field also contains their sum $2/\sqrt{2} = \sqrt{2}$.

8. (c) Let m be a squarefree number. Then m can be written as $2^i q$ where $2 \nmid q$, and $i \in \{0,1\}$. We proceed by case analysis, showing for each that $\sqrt{m}$ is contained in the dth cyclotomic field, where $d = \text{disc}(\mathbb{A} \cap \mathbb{Q}[\sqrt{m}])$.

   $m = -1$: $\sqrt{-1}$ is contained in the 4th cyclotomic field which contains the complex unit i ($d = -4$).

   $m = 2$: $\sqrt{2}$ is contained in the 8th cyclotomic field by part (b) ($d = 4 \cdot 2 = 8$).

   $m = -2$: The 8th cyclotomic field contains i (since it contains the 4th cyclotomic field as a subfield) so it contains $\sqrt{-2} = i\sqrt{2}$ ($d = 4 \cdot -2 = -8$).

   $m = q$ where $q \equiv 1 \mod 4$: Because $q \equiv 1 \mod 4$, q has an even number of prime factors $\equiv 3 \mod 4$, meaning that $\sqrt{q}$ must be contained in the q-th cyclotomic field ($d = q$ since $q \equiv 1 \mod 4$).

   $m = q$ where $q \equiv 3 \mod 4$: The $4q$-th cyclotomic field contains the q-th cyclotomic field (containing $\sqrt{-q}$) and the 4th cyclotomic field (containing $\sqrt{-1}$) ($d = 4q$ since $q \equiv 3 \mod 4$), and so contains $\sqrt{q}$.

   $m = 2q$ where q is a product of odd primes: Here $d = 8q$. By the above, $\sqrt{q}$ is contained in either the q-th or $4q$-th cyclotomic field, depending on its residue mod 4. Thus $\sqrt{2q}$ is contained in the $8q$-th cyclotomic field.

   This shows every quadratic field $\mathbb{Q}[\sqrt{m}]$ is contained within the d-th cyclotomic field.

9. Let θ be a primitive k-th root of unity, i.e. $\theta = e^{2\pi i/k}$. Let $\gcd(k,m) = d$. Using Euclid's extended algorithm we can find u, v such that $uk + vm = d$. Then we have

$$\omega^u \theta^v = e^{(2\pi i u)/m} e^{(2\pi i v)/k} = e^{2\pi i (uk+vm)/km} = e^{2\pi i d/km} = e^{2\pi i/r}$$

where $r = \mathrm{lcm}(k,m)$ ($\mathrm{lcm}(k,m) = km/\gcd(k,m)$).

10. Show if m is even, $m \mid r$, and $\phi(r) \le \phi(m)$ then $r = m$.

If $m \mid r$ there is some k such that $mk = r$. Let $d = \gcd(k,m)$, so $r = mdj$ with j satisfiying $\gcd(j,m) = 1$. Therefore $\phi(r) = \phi(md)\phi(j)$. Since $d \mid m$, $\phi(md) = d \cdot \phi(m)$, so

$$\phi(r) = d \cdot \phi(m)\phi(j) \le \phi(m)$$

The inequality forces $d = 1$ and $\phi(j) = 1$. Because $2 \mid m \mid r$, $\phi(j) = 1$ implies $j = 1$. Therefore $m = r$.

11. (a) Suppose all the roots to a monic polynomial f have absolute value 1. Show that the coefficient of x^r has absolute value $\le \binom{n}{r}$, where n is the degree of f and $\binom{n}{r}$ is the binomial coefficient.

Factor f as $f = (x - \alpha_0) \cdots (x - \alpha_n)$. Re-expanding f we see that the coefficient of x^r is equal to $\sum_{S \subseteq \{0,\dots,n\}, |S| = r} x^r \prod_{i \in S} \alpha_i$. By assumption $|\alpha_i| = 1$ for all i, so $|\prod_{i \in S} \alpha_i| = 1$. There are $\binom{n}{r}$ of these subsets of S.

Using the identity $|a + b| \le |a| + |b|$ we have:

$$\begin{aligned} \left| \sum_{S \subseteq \{0,\dots,n\}, |S|=r} \prod_{i \in S} \alpha_i \right| &\le \sum_{S \subseteq \{0,\dots,n\}, |S|=r} |\prod_{i \in S} \alpha_i| \\ &\le \sum_{S \subseteq \{0,\dots,n\}, |S|=r} 1 \\ &\le \binom{n}{r} \end{aligned}$$

11. (b) We will consider all monic polynomials f of degree n and show that only a finite number of them can have a root α all of whose conjugates have absolute value 1.

By Theorem 1, if α is an algebraic integer, than the coefficients of f are integers. By (b), the absolute value of the coefficients of f are bounded above $\binom{n}{r}$, therefore there are at most $2\binom{n}{r}$ choices for each coefficient beyond the x^nth term. The constant term of the polynomial must be 1 (since α has absolute value 1) and the first term of the polynomial must also be 1 (since f is monic). This gives an upper bound of $\sum_{r=1}^{n-1} 2\binom{n}{r} = 2(2^n - 2) = 4(2^{n-1} - 1)$ on the number of algebraic integers satisfying the given condition.

11. (c) (TODO)

12. (a) Let u be a unit in $\mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/p}$. Show $u/\overline{u}$ is a root of 1.

The field $\mathbb{Q}[\omega]$ has Galois group $\simeq \mathbb{Z}_p^\times$, which has cardinality $p-1$ and so has an element of order 2 (complex conjugation). Therefore u has $p-1$ conjugates, which consist of $(p-1)/2$ elements along with their complex conjugates. Enumerate the conjugates of u as $a_1, \ldots, a_n, \overline{a_1}, \ldots, \overline{a_n}$.

Therefore, the conjugates of $u/\overline{u}$ have the form $a_i/\overline{a_i}$ or $\overline{a_i}/a_i$. Multiplying over all conjugates of $u/\overline{u}$, we have $\prod_{i=0}^n a_i/\overline{a_i} \cdot \prod_{i=0}^n \overline{a_i}/a_i = 1$, and so $u/\overline{u}$ and all its conjugates have absolute value 1. By 11 (c), $u/\overline{u}$ is then a root of 1, and so has form $\pm\omega^k$.

12. (b) Suppose $u/\overline{u} = -\omega^k$. We derive a contradiction. Raising both sides to the p-th power we have $u^p/\overline{u^p} = -(\omega^k)^p = -(\omega^p)^k = -1$, and so $u^p = -\overline{u^p}$. By exercise 1.25, $u^p \equiv a\ (p)$ for some $a \in \mathbb{Z}$. Applying exercise 1.23, we see $\overline{u^p} \equiv \overline{a} = a\ (p)$, and so $a \equiv -a\ (p)$. There a must be 0, and $u^p \equiv 0\ (p)$, so p divides u^p. This contradicts u^p being a unit, since if p divided u^p, p would also divide the absolute value of u^p, which is 1. Therefore $u/\overline{u} = \omega^k$.

13. Show that 1 and -1 are the only units in the ring $A \cap \mathbb{Q}[\sqrt{m}]$, m squarefree and $m < 0, m \neq -1, -3$. What if $m = -1, -3$?

Let u be a unit in $A \cap \mathbb{Q}[\sqrt{m}]$. Then $u = a + b\sqrt{m}$ where $p, q \in A \cap \mathbb{Q}[sqrtm]$. Since $N(u) = 1$, then $(a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - b^2m = 1$. We proceed by cases on whether $m \equiv 1\ (4)$.

If $m \not\equiv 1 \mod 4$, then a and b must be integers and so $a^2 - b^2m = 1$ can only be satisfied if one of the terms is 1 and the other is 0. If $a^2 = 1$, then $b^2m = 0$. This corresponds to the units 1 and -1 in $A \cap \mathbb{Q}[\sqrt{m}]$. If $-b^2m = 1$, then $b^2m = -1$ and so $m = -1$. This corresponds to the units i and $-i$ in $A \cap \mathbb{Q}[\sqrt{-1}]$.

If $m \equiv 1\ (4)$ then let $a = r/2$ and $b = s/2$. Therefore $r^2 - s^2m = 4$. Since m is negative, both r^2 and $-s^2m$ must be positive. r^2 must be either 0, 1, or 4.

If r^2 is 0 then $-s^2m = 4$, so $s^2m = -4$, forcing $m = -1$ which is not $\equiv$ mod 4. (We have considered this case already.)

If r^2 is 1 then $-s^2m = 3$ so $s^2m = -3$ and $m = -3$, $s = \pm 1$. This corresponds to the unit $\pm\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$ in the ring $A \cap \mathbb{Q}[\sqrt{-3}]$.

If r^2 is 4 then $-s^2m = 0$, which corresponds to the unit ± 1 in the ring $A \cap \mathbb{Q}[\sqrt{m}]$.

14. Show that $1 + \sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$, but not a root of 1.

$1 + \sqrt{2}$ is a unit, as $-(1 - \sqrt{2})$ is its inverse:

$$-(1 + \sqrt{2})(1 - \sqrt{2}) = -1 + (\sqrt{2})^2 = 1$$

If $1 + \sqrt{2}$ were a root of 1, we would have $(1 + \sqrt{2})^k = 1$ for some k. However by the Binomial Theorem, $(1 + \sqrt{2})^k = \sum_{i=0}^k \binom{k}{i} (\sqrt{2})^i$, which will always contains a term $\sqrt{2}$ multiplied by a positive number. Therefore $1+\sqrt{2}$ is not a root of 1.

Let $(1+\sqrt{2})^k = a + b\sqrt{2}$. The inverse of this term is

$$((1+\sqrt{2})^k)^{-1} = ((1+\sqrt{2})^{-1})^k = (-1)^k(1-\sqrt{2})^k = (-1)^k(a-b\sqrt{2})^k$$

Therefore, $(a+b\sqrt{2})^k \cdot (a-b\sqrt{2})^k = \pm 1$ and so the powers of $1+\sqrt{2}$ give an infinite number of a, b such that $a^2 - 2b^2 = \pm 1$.

15. (a) Let $a+b\sqrt{-5}$ be an element of $\mathbb{Z}[\sqrt{-5}]$. Then the norm of $a+b\sqrt{-5}$ is $(a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2$, where $a, b \in \mathbb{Z}$. Since there are no integer solutions a, b such that $a^2+5b^2 = 2$ or $a^2+5b^2 = 3$, there can be no element of $\mathbb{Z}[\sqrt{-5}]$ with a norm of 2 or 3.

15. (b) In $\mathbb{Z}[\sqrt{-5}]$, $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. If unique factorization held in $\mathbb{Z}[\sqrt{-5}]$, there would be elements $a, b, c, d \in \mathbb{Z}[\sqrt{-5}]$ such that $a\cdot b = 2$, $c\cdot d = 3$, $a\cdot d = 1+\sqrt{-5}$, $b\cdot c = 1-\sqrt{-5}$. However by (a), 2 and 3 are irreducible in $\mathbb{Z}[\sqrt{-5}]$, meaning they are irreducible elements, and so no a, b, c, d can exist.

16. We argue in the style of K. Conrad: Trace and Norm, Section 4. Suppose $\sqrt{3} \in \mathbb{Q}[\alpha]$ where $\alpha = \sqrt[4]{2}$; therefore $\sqrt{3} = a + b\alpha + c\alpha^2 + d\alpha^3$. We have the following traces:

$$\begin{aligned}
\mathrm{Tr}(\sqrt{3}) &= \sqrt{3} - \sqrt{3} = 0 \\
\mathrm{Tr}(\alpha) &= \alpha - \alpha + i\alpha - i\alpha = 0 \\
\mathrm{Tr}(\alpha^2) &= \alpha^2 - \alpha^2 + i\alpha^2 - i\alpha^2 = 0 \\
\mathrm{Tr}(\alpha^3) &= \alpha^3 - \alpha^3 + i\alpha^3 - i\alpha^3 = 0
\end{aligned}$$

Since $\sqrt{3} = a + b\alpha + c\alpha^2 + d\alpha^3$,

$$\begin{aligned}
\mathrm{Tr}(\sqrt{3}) &= \mathrm{Tr}(a + b\alpha + c\alpha^2 + d\alpha^3) \\
0 &= a\mathrm{Tr}(1) + b\mathrm{Tr}(\alpha) + c\mathrm{Tr}(\alpha^2) + d\mathrm{Tr}(\alpha^3) \\
0 &= 4a
\end{aligned}$$

Therefore $a = 0$, and we have $\sqrt{3} = b\alpha + c\alpha^2 + d\alpha^3$. We have $\mathrm{Tr}(\sqrt{3}\alpha) = \mathrm{Tr}(\sqrt[4]{9/2}) = \sqrt[4]{9/2} - \sqrt[4]{9/2} + i\sqrt[4]{9/2} - i\sqrt[4]{9/2} = 0$, so $0 = b\mathrm{Tr}(1) + c\mathrm{Tr}(\alpha) + d\mathrm{Tr}(\alpha)^2 = 4b$ and so $b = 0$.

Similarly $\mathrm{Tr}(\sqrt{3}/\alpha^2) = \mathrm{Tr}(\sqrt{3/2}) = 0$, and so $c = 0$.

From eliminating the coefficients a, b, c, we have $d\sqrt[4]{8} = \sqrt{3}$ and so $3 = d^2\sqrt{8} = 2d^2\sqrt{2}$. Therefore $\sqrt{2}$ is expressible as a rational number $3/d^2$, a contradiction. Therefore $\sqrt{3} \notin \mathbb{Q}[\alpha]$.

(Where would this argument break down for $\sqrt{2}$? $\sqrt{2} = \alpha^2$ so $\sqrt{2}/\alpha^2 = 1$ and so we would conclude that $c = 1$ rather than $c = 0$.)

17 - TODO

18 - TODO

19 - TODO

20. Write $f(x) = (x - \alpha)g(x)$. By the chain rule $f'(x) = (x - \alpha)g'(x) + g(x)$, so $f'(\alpha) = g(\alpha) = \prod_{\beta \neq \alpha}(\alpha - \beta)$.

21. Let $f(x) = g(x)h(x)$, where $g(x)$ is the minimum polynomial of α over $\mathbb{Z}$. Then $f'(x) = g'(x)h(x) + g(x)h'(x)$ and $f'(\alpha) = g'(\alpha)h(\alpha)$. We have

$$\mathrm{N}(f'(\alpha)) = \mathrm{N}(g'(\alpha))\mathrm{N}(h(\alpha))$$

. By Theorem 8, $\mathrm{N}(g'(\alpha)) = \pm\mathrm{disc}(\alpha)$, so

$$\mathrm{N}(f'(\alpha)) = \pm\mathrm{disc}(\alpha)\mathrm{N}(h(\alpha))$$

Therefore $\mathrm{disc}(\alpha)$ divides $\mathrm{N}(f'(\alpha))$ as required.

23. (c) Let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis for K ($n = [K : \mathbb{Q})$ and let $\{\beta_1, \ldots, \beta_m\}$ be an integral basis for L ($m = [L : \mathbb{Q}]$). Therefore

$$\{\alpha_i\beta_j \mid 1 \leq i \leq n, 1 \leq j \leq m$$

is an integral basis for KL.

We have the tower of field extensions $KL : K : \mathbb{Q}$ where $[KL : K] = m$, $[K : \mathbb{Q}] = n$. By the formula established in (b),

$$\mathrm{disc}(\alpha_i\beta_j) = (\mathrm{disc}(\alpha_i))^m N_{\mathbb{Q}}^K \mathrm{disc}(\beta_j) = (\mathrm{disc}\ R)^m(\mathrm{disc}\ S)^n$$

Because disc S is an integer, its norm is the degree of K over $\mathbb{Q}$.

24 Let G be a free abelian group of rank n and let H be a subgroup. Take $G = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. We show by induction that H is a free abelian group of rank $\leq n$.

First prove the result for $n = 1$.

If G is a free abelian group of rank 1, $G = \mathbb{Z}$. If H is a subgroup of G then H must have a least non-negative element, call it m. Then H is generated by m (all subgroups of $\mathbb{Z}$ are generated by a single element).

Next, we assume the result holds for $n - 1$, and define $\pi : G \to \mathbb{Z}$ the projection of G onto the first factor. Let K denote the kernel of π.

(a): Show that $H \cap K$ is a free abelian group of rank $\leq n - 1$.

Let ι be the map that drops the first factor from G; as K is a subgroup of G, then $\iota(H \cap K)$ must be a subgroup of $\iota(G)$. $\iota(G)$ is a free abelian group of rank $n - 1$, and so applying the inductive hypothesis, we see $\iota(H \cap K)$ $= 0 \oplus (H \cap K)$ is a free abelian group of order $n - 1$.

(b): The image $\pi(H) \subset \mathbb{Z}$ is either $\{0\}$ or infinite cyclic. If it is 0, then $H = H \cap K$. Otherwise let $h \in \pi(H)$ be a generator of $\pi(H)$. Show H is the direct sum of its subgroups $\mathbb{Z}h$ and $K \cap H$.

Let h be as in the problem statement. Let $a \in H$. We will show a is a member of $\mathbb{Z}h \oplus (K \cap H)$. If $\pi(a) = 0$, then $a \in H \cap K$ and so a is a member of the required group. Otherwise $\pi(a) = m\pi(h)$ for some integer m and so $mh - a \in K \cap H$ (a free abelian group of rank $\leq n-1$). Therefore a is the direct sum of $mh \in \mathbb{Z}h$ and the components of $mh - a$. Since a was chosen arbitrarily, $H = \mathbb{Z}h \oplus (K \cap H)$.

25. Let α be an algebraic number, so there is some $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. We convert this polynomial into a (non-monic) $g \in \mathbb{Z}[x]$ by through multiplying by the GCD m for all of the denominators in the coefficients of f. Then $g = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $g(\alpha) = 0$. Multiplying through by a_n^{n-1} gives the relationship $(a_n\alpha)^n + a_{n-1}a_n^{n-1}\alpha^{n-1} + \cdots + a_n^{n-1}a_0 = 0$. This is a monic polynomial with integer coefficients, so $ma_n^n\alpha$ is an algebraic integer.

    Given any finite set of algebraic numbers, $\{\alpha_0, \ldots \alpha_n\}$ let m_i be such that $m_i\alpha_i$ is an algebraic integer. Therefore taking M to be the least common multiple of each m_i gives us a number M such that each $M\alpha_i$ is an algebraic integer.

26. The proof that two sets that generate the same subgroup have the same discriminant is the same as that of Theorem 11: as $\{\beta_1, \ldots, \beta_n\}$ and $\gamma_1, \ldots, \gamma_n\}$ generate the same additive subgroup, we can write the γ_i in terms of the β_i through an matrix M with entries in $\mathbb{Z}$, and vice versa. This shows that the translate matrices must have determinant 1, so the discriminants are equal.

27. Let G and H be two free abelian subgroups of rank n in K, with $H \subset G$.

27. (a) Show G/H is a finite group.

    Since G and H are free abelian subgroups of rank n, $G \simeq \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ and since H is a subgroup of G, then $H \simeq I_1 \oplus \cdots \oplus I_n$, where each $I_i \subseteq \mathbb{Z}$ is an additive subgroup of $\mathbb{Z}$. Each $\mathbb{Z}/I_i$ is finite, having cardinality equal to the generating element of I_i. Therefore G/H is finite, having cardinality $\prod_{i=0}^n |\mathbb{Z}/I_i|$.

27. (b) The well-known finite structure theorem for abelian groups says G/H is a direct sum of at most n cyclic groups. Use this to show that G has a generating set $\beta_1, \ldots, \beta_n$ such that for appropriate integers d_i, $d_1\beta_1, \ldots, d_n\beta_n$ is a generating set for H.

    Let β_i be 1 projected to the ith-factor and 0 elsewhere. Then the set of $\{\beta_i\}$ generate G. Let d_i be the minimum element of I_i, an additive subgroup of $\mathbb{Z}$: we show $\{d_i\beta_i\}$ generates H. Take $a \in H$, and let $\iota_i(a)$ be the ith factor of a, so $\iota_i(a) \in I_i$. By choice of d_i, $\iota_i(a) = d_i m$ for some integer m, and $a = \iota_1(a) \oplus \cdots \oplus \iota_n(a) = d_1\beta_1 + \cdots + d_n\beta_n$. Since a was chosen arbitrarily, the $\{d_i\beta_i\}$ generates H.

27. (c) $\mathrm{disc}(H) = \mathrm{disc}(d_1\beta_1, \ldots, d_n\beta_n)$: by Exercise 3.18 (a),

$$\mathrm{disc}(H) = (d_1 \cdots d_n)^2 \mathrm{disc}(\beta_1, \ldots, \beta_n) = |G/H|^2 \mathrm{disc}(G)$$

27. (d) Show that if $\alpha_1, \ldots, \alpha_n \in R = \mathbb{A} \cap K$, then they form an integral basis iff $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(R)$.

Let H be the additive subgroup formed by $\alpha_1, \ldots, \alpha_n$. By (c), we have $\mathrm{disc}(H) = |R/H|^2 \mathrm{disc}(R)$. Therefore $\mathrm{disc}(R) = \mathrm{disc}(G)$ iff $|G/H|^2 = 1$, which is the same as saying that there is $b \in G$ such that $b \notin H$. Therefore $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(R)$ if and only if they form an integral basis for R.

27. (e) Show that if $\alpha_1, \ldots, \alpha_n \in R = \mathbb{A} \cap K$ and $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ is squarefree, then the α_i form an integral basis for R.

If $\mathrm{disc}(H)$ is squarefree then $|R/H| = 1$ which implies that $\mathrm{disc}(H) = \mathrm{disc}(R)$. By (d) the α_i form an integral basis for R.

28. (a) Taking the derivative of the polynomial, we have $f'(x) = 3x^2 + a$. We then have:

$$\begin{aligned}
f'(\alpha) &= 3\alpha^2 + a \\
\alpha f'(\alpha) &= 3\alpha^3 + a\alpha \\
\alpha f'(\alpha) &= -3(a\alpha + b) + a\alpha \\
\alpha f'(\alpha) &= -2a\alpha - 3b \\
f'(\alpha) &= -(2a\alpha + 3b)/\alpha
\end{aligned}$$

28. (b) It is straightforward that $2a\alpha + 3b$ is a root of the polynomial $g(x) = (\frac{x-3b}{2a})^3 + a(\frac{x-3b}{2a}) + b$. To calculate the norm of $2a\alpha + 3b$ over $\mathbb{Q}[\alpha]$, we thus divide the zero coefficient of $g(x)$ by negative the initial coefficient of $g(x)$ (negative since $n = 3$ is odd):

$$-(2a)^3 \left(\frac{(-3b)^3}{(2a)^3} - \frac{3b}{2} + b \right)$$

Reducing terms gives us

$$\mathrm{N}(2a\alpha + 3b) = (3b)^3 + (2^2)a^3 b = 27b^3 + 4a^3 b$$

28. (c) By Theorem 8, $\mathrm{disc}(a) = -\mathrm{N}(f'(\alpha))$ (the negative sign holds since $n = 3 \not\equiv 0, 1$ (4),).

Note that given the factoring of $f(x)$ into $(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, $(-1)\alpha_1\alpha_2\alpha_3 = -\mathrm{N}(\alpha) = b$, $\mathrm{N}(\alpha) = -b$.

We now compute the discriminant of α:

$$\begin{aligned} \mathrm{disc}(\alpha) &= -\mathrm{N}(f'(\alpha)) \\ &= -\mathrm{N}(-(2a\alpha + 3b)/\alpha) \\ &= \frac{27b^3 + 4a^3 b}{-b} \\ &= -(27b^2 + 4a^3) \end{aligned}$$

This is the required result.

28. (d) If $\alpha^3 = \alpha + 1$, then $a = -1$ and $b = -1$. By (c), $\mathrm{disc}(\alpha) = -27 - 4 = -31$, which is squarefree. By 27 (c) the powers of α thus form an integral basis for $\mathbb{A} \cap \mathbb{Q}[\alpha]$.

Similarly if $a = 1$ and $b = -1$, then $\mathrm{disc}(\alpha) = -27 + 4 = -23$ (squarefree) and so again by 27 (c) the powers of α form an integral basis for $\mathbb{A} \cap \mathbb{Q}[\alpha]$.

29. Let $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$, where $(m,n) = 1$. Find an integral basis and the discriminant of this basis for (a): the case where $m, n \equiv 1$ (4) and (b) where $m \equiv 1$ (4), $n \not\equiv 1$ (4).

For both given scenarios, the ring of integers is a linear combination of the ring of integers of $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$, and so Theorem 12, Corollary 1 applies, and an integral basis can be found as a combination of the bases of the individual rings.

29. (a) $m, n \equiv 1$ (4): The corresponding rings of integers for $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are $\mathbb{Z}[(1 + \sqrt{m})/2]$ and $\mathbb{Z}[(1 + \sqrt{n})/2)]$ with discriminants m and n. By assumption, these discriminants are relatively prime, so Theorem 12, Corollary 1 applies. The field $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$ thus has an integral basis $\{1, (\sqrt{m} + 1)/2, (\sqrt{n} + 1)/2, (1 + \sqrt{m} + \sqrt{n} + \sqrt{nm})/4\}$. By Exercise 23 (c), the discriminant for this basis is $m^2 n^2$.

29. (b) The rings of integers for $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are $\mathbb{Z}[(1 + \sqrt{m})/2]$ and $\mathbb{Z}[\sqrt{n}]$, with discriminants m and $4n$. Since m was assumed to be squarefree, $(m, 4n) = 1$, so Theorem 12, Corollary 1 applies again. The field $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$ thus has an integral basis $\{1, (\sqrt{m}+1)/2, \sqrt{n}, (\sqrt{mn}+\sqrt{n})/2\}$. By Exercise 23 (c), the discriminant for this basis is $m^2(4n)^2 = 16m^2n^2$.

30. Let f be the monic irreducible polynomial for α over $\mathbb{Z}$ and for each $g \in \mathbb{Z}[x]$, let $\overline{g}$ denote the polynomial in $\mathbb{Z}_3[x]$ obtained by reducing the coefficients mod 3.

30. (a) Show that $g(\alpha)$ is divisible by 3 in $\mathbb{Z}[\alpha]$ if and only if $\overline{g}$ is divisible by $\overline{f}$ in $\mathbb{Z}_3[x]$.

Suppose $g(\alpha)$ is divisible by 3. Then $g(\alpha) = 3m$ for some m and so $(g - 3m)(\alpha) = 0$. Since this is a polynomial in α and f is the minimum polynomial, $f \mid g - 3m$. Therefore $\overline{f} \mid \overline{g - 3m} = \overline{g}$.

If $\overline{g}$ is divisible by $\overline{f}$ in $\mathbb{Z}_3[x]$, then $\overline{g} = \overline{fh}$ for some $h \in \mathbb{Z}[x]$, and so $g = (f + 3j)h$ in $\mathbb{Z}[x]$ for some polynomial $j(x) \in \mathbb{Z}[x]$. So $g(\alpha) = 3j(\alpha)h(\alpha)$ and $g(\alpha)$ is divisible by 3.

30. (b) Consider the four algebraic integers:

$$\begin{aligned}
\alpha_1 &= (1+\sqrt{7})(1+\sqrt{10}) \\
\alpha_2 &= (1+\sqrt{7})(1-\sqrt{10}) \\
\alpha_3 &= (1-\sqrt{7})(1+\sqrt{10}) \\
\alpha_4 &= (1-\sqrt{7})(1-\sqrt{10})
\end{aligned}$$

The conjugates of each α_i are the other α_j, and each product $\alpha_i\alpha_j$ is divisible by 3: $\alpha_1\alpha_3$, $\alpha_2\alpha_3$, $\alpha_1\alpha_4$, and $\alpha_2\alpha_4$ are divisible by -6, and $\alpha_1\alpha_2$, $\alpha_1\alpha_4$, $\alpha_2\alpha_3$, and $\alpha_3\alpha_4$ are divisible by -9.

We show that $\alpha_i^n/3$ is not an algebraic integer by considering its trace: $\mathrm{Tr}(\alpha_i^n/3) = \mathrm{Tr}(\alpha_i^n)/3$, so we compute $\mathrm{Tr}(\alpha_i^n)$. The conjugates of α_i^n are each of the other α_j^n, so $\mathrm{Tr}(\alpha_i^n) = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n$. Modulo 3, $(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n \equiv \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n$ because any of the monomials with any nonzero powers is divisible by 3 and so cancel out mod 3. However $(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n = 1^n = 1$. Since each α_i is conjugate to each of the α_j, their traces must be identical.

Therefore the trace of α_i^n is an integer $\equiv 1$ (3), and so $\mathrm{Tr}(\alpha_i^n/3)$ cannot be an integer, and so by Corollary 2 to Theorem 4, $\alpha_i^n/3$ must not be an algebraic integer.

30. (c) Let α_i from (b) be defined by $f_i(\alpha)$ (for any fixed α). Because $\alpha_i\alpha_j$ is divisible by 3, by (a), $\overline{f} \mid \overline{f_i f_j}$. However, $\overline{f} \nmid \overline{f_i}^n$ for any power of n (or else 3 would $\overline{f_i}^n$ which is not the case by (b)), so $\overline{f_i f_j} \neq \overline{f_i}^n$ for any n. Therefore, since $\mathbb{Z}_3[x]$ is a UFD, $\overline{f}$ has an irreducible factor that does not divide $\overline{f_i}$ but does divide $\overline{f_j}$ for all $j \neq i$.

30. (d) The result of (c) is that $\overline{f}$ has at least 4 irreducible factors in $\mathbb{Z}_3[x]$. However, $\overline{f}$ is of degree at most 4, since $\alpha \in \mathbb{Q}[\sqrt{7}, \sqrt{10}]$. For there to be at least 4 irreducible factors of $\overline{f}$ it would imply each are of degree 1, but there are only 3 monic polynomials of degree 1 in $\mathbb{Z}_3[x]$: x, $x-1$, $x-2$. Therefore $\mathbb{A} \cap \mathbb{Q}[\sqrt{7}, \sqrt{10}] \neq \mathbb{Z}[\alpha]$ for any α.

31. Show that $\frac{\sqrt{3}+\sqrt{7}}{2}$ is an algebraic integer.

$\frac{\sqrt{3}+\sqrt{7}}{2}$ is the root of the degree 4 polynomial $f(x) = x^4 - 5x^2 + 1$. This shows that the intersection of the ring of integers $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Z}[\sqrt{7}]$ is not $\mathbb{Z}[\sqrt{3}, \sqrt{7}]$; neither original ring contains fractional elements. (Their discriminants are 12 and 28 respectively, sharing a factor of 4.)

32. The fields $\mathbb{Q}[\sqrt[3]{2}]$ and $\mathbb{Q}[\omega\sqrt[3]{2}]$ where $\omega = e^{2\pi i/3}$ both have degree 3 over $\mathbb{Q}$, but their composition $\mathbb{Q}[\omega, \sqrt[3]{2}]$ has degree 6 over $\mathbb{Q}$.

33. Let $\omega = e^{2\pi i/m}$, where $m \geq 3$. We know that $N(\omega) = \pm 1$ because ω is a unit. Show the + sign holds.

    Write $e^{2\pi ik/m}$ as ω_k. The conjugates of ω have the form ω_k where $(k,m) = 1$. There are $\phi(m)$ of these, which is even for all $m \geq 3$. If ω_k is a conjugate, then ω_{m-k} is also a conjugate, since $(k,m) = 1$ implies there exist integers a, b such that $ak+bm = 1$, so $-a(m-k)+(b+a)m = 1$, and so $(m-k, m) = 1$.

    For each conjugate ω_k, $\omega_k \neq \omega_{m-k}$; if this were the case, $k = -k\ (m)$, so $2k = 0\ (m)$ and so k would divide m, contradicting $(k,m) = 1$. Therefore all the conjugates are distinct.

    Finally, for each conjugate ω_k, $\omega_k \cdot \omega_{m-k} = 1$, so in computing the norm of ω, all the conjugates cancel out and the norm of ω is seen to be 1.

34. (a) Show that $1 + \omega + \omega^2 + \ldots + \omega^{k-1}$ is a unit in $\mathbb{Z}[\omega]$ if k is relatively prime to ω.

$$(1 + \omega + w^2 + \ldots + \omega^{k-1})\left(\frac{1-w}{1-\omega^k}\right) = \frac{1-\omega^k}{1-\omega^k} = 1$$

    Therefore, if $\frac{1-w}{1-\omega^k} \in \mathbb{Z}[\omega]$ then $1 + \omega + \ldots + \omega^{k-1}$ is a unit. Since $(k,m) = 1$, then there exist $a, b \in \mathbb{Z}$ such that $ak + bm = 1$, and so $\omega = \omega^{ak+bm} = \omega^{ak}\omega^{bm} = \omega^{ak}$. Since $\omega^{ak} = \omega^{(m-a)k}$ for negative a, a can be assumed to be positive. We then have

$$\frac{1-\omega}{1-\omega^k} = \frac{1-\omega^{ak}}{1-\omega^k} = 1 + \omega^k + \omega^{2k} + \ldots + \omega^{(a-1)k} \in \mathbb{Z}[\omega]$$

    This implies $1 + \omega + \omega^2 + \ldots + \omega^{k-1}$ is a unit in $\mathbb{Z}[\omega]$.

34. (b) The conjugates of $1 - \omega$ are $\omega^{kp^{r-1}} - 1$ for $1 \leq k \leq p-1$. By (a), $1 - w^k = \frac{1-\omega}{1+\omega+\ldots+\omega^k}$, so

$$\mathrm{N}(1-w) = (1-\omega)^n \left(\prod_{(j,p^r)=1} \sum_{i=0}^{j} \omega^i \right)^{-1}$$

    By (a) the sum of the ω^i factors is a unit in $\mathbb{Z}[\omega]$, so the inverse of the product of each of these is also a unit, call it u. Therefore

$$\mathrm{N}(1-w) = u(1-w)^n$$

    However as $f(x) = 1 + x^{p^{r-1}} + \ldots + x^{(p-1)p^{r-1}}$ is the p^rth cyclotomic polynomial, the norm of $1 - w$ is the constant coefficient of the polynomial $1 + (1-x)^{p^{r-1}} + \ldots + (1-x)^{(p-1)p^{r-1}} = p$, and so $\mathrm{N}(1-w) = p$. Setting both sides equal to one another gives $p = u(1-\omega)^n$.

35. (a) Let $\omega = e^{2\pi i/m}$ and $\theta = \omega + \omega^{-1}$. Then $\omega^2 - (\omega + \omega^{-1})(\omega) + 1 = 0$ and so ω is a root of the polynomial $x^2 + \theta x + 1$. $\omega \notin \mathbb{Q}[\theta]$, therefore $\mathbb{Q}[\omega] : \mathbb{Q}[\theta]$ has degree 2.

35. (b) Since $\theta = \omega + \omega^{-1} \in \mathbb{R}$, clearly $\mathbb{Q}[\theta] \subseteq \mathbb{Q}[\omega] \cap \mathbb{R}$. We therefore have the tower of field extensions $\mathbb{Q}[\theta] \subseteq \mathbb{Q}[\omega] \cap \mathbb{R} \subsetneq \mathbb{Q}[\omega]$. By (a), $[\mathbb{Q}[w] : \mathbb{Q}[\theta]] = 2$. By the Tower Law, $[\mathbb{R} \cap \mathbb{Q}[\omega] : \mathbb{Q}[\theta]]$ must be a divisor of 2 by distinct from 2 (since $w \notin \mathbb{R}$). Therefore the degree must be 1 and so $\mathbb{R} \cap \mathbb{Q}[\omega] = \mathbb{Q}[\theta]$.

35. (c) Let σ be the automorphism defined by $\sigma(\omega) = \omega^{-1}$. Then $\sigma(\theta) = \theta$, and so $\mathbb{Q}[\theta]$ is in the fixed field of the automorphism σ. As the degree of $\mathbb{Q}[\omega]$ over $\mathbb{Q}[\theta]$ is 2, there can be no distinct intermediate field between $\mathbb{Q}[\omega]$ and $\mathbb{Q}[\theta]$. $\mathbb{Q}[\omega]$ is not in the fixed field of σ and so $\mathbb{Q}[\theta]$ must be the fixed field of this automorphism.

35. (d) Show that $\mathbb{A} \cap \mathbb{Q}[\theta] = \mathbb{R} \cap \mathbb{Z}[\theta]$.

$$\begin{aligned}
\mathbb{A} \cap \mathbb{Q}[\theta] &= \mathbb{A} \cap (\mathbb{R} \cap \mathbb{Q}[\omega]) && \text{By 35 (b).} \\
&= (\mathbb{A} \cap \mathbb{Q}[\omega]) \cap \mathbb{R} && \text{By associativity of intersection} \\
&= \mathbb{Z}[\omega] \cap \mathbb{R} && \text{By Theorem 12, Corollary 2}
\end{aligned}$$

This is the required result.

35. (e) Let $n = \phi(m)/2$. The set $\{1, \omega, \omega^2, \ldots, \omega^{n-1}, \omega^n, \omega^{n+1}, \ldots, \omega^{m-1}\}$ is an integral basis for $\mathbb{Z}[\omega]$.

Since $w^{n-k} = \omega^{-k}$, we can write this basis as $\{1, \omega, \omega^{-1}, \omega^2, \omega^{-2}, \ldots, \omega^{-n}\}$ instead (note $\omega^n = \omega^{-n}$). We examine the set $\{1, \omega, \theta, \theta\omega, \theta^2, \theta^2\omega, \ldots, \theta^n\}$.

Now we pair up the expressions $\theta^k\omega$ with ω^{k+1} and θ^k with ω^{-k}:

$$\{1, \omega, \omega^{-1}, \omega^2, \omega^{-2}, \omega^3, \ldots, \omega^n\} \tag{1}$$

$$\{1, \omega, \theta, \theta\omega, \theta^2, \theta^2\omega, \ldots, \theta^{n-1}\omega\} \tag{2}$$

We evaluate the expression θ^k using the Binomial Theorem:

$$\theta^k = (\omega + \omega^{-1})^k = \sum_{i=0}^{k} \binom{k}{i} \omega^i \omega^{-(k-i)} = \sum_{i=0}^{k} \binom{k}{i} \omega^{2i-k}$$

Therefore

$$\theta^k \omega = \sum_{i=0}^{k} \binom{k}{i} \omega^{2i-k+1}$$

For θ^k, the power of ω ranges between $-k$ and k for θ^k, and it uses 1 term of the power ω^{-k} and no power of ω with absolute value greater than k.

For $\theta^k\omega$, the power of ranges between $-k+1$ and $k+1$ for $\theta^k\omega$. It uses 1 power of ω^k and no other power of ω with absolute value of greater than or equal to k.

Therefore, there is a lower triangular translation matrix A between the basis (1) and (2). A has all 1s in the diagonal, and so A has determinant 1 and is invertible over $\mathbb{Z}$. Since (1) is an integral basis of $\mathbb{Z}[\omega]$, so is (2).

$$A = \begin{array}{c} \\ 1 \\ \omega \\ \theta \\ \theta\omega \\ \theta^2 \\ \vdots \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & \omega & \omega^{-1} & \omega^2 & \omega^{-2} & \dots \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & 0 & \dots \\ 0 & 1 & 1 & 0 & 0 & \dots \\ 1 & 0 & 0 & 1 & 0 & \dots \\ 2 & 0 & 0 & 1 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \end{array}$$

35. (f) Show that $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ is an integral basis for $\mathbb{A} \cap \mathbb{Q}[\theta]$.

By (d), $\mathbb{A} \cap \mathbb{Q}[\theta] = \mathbb{R} \cap \mathbb{Z}[\theta]$, and by (e), any member α of $\mathbb{Z}[\theta]$ is expressible in terms of the basis vectors $\{1, \omega, \theta, \theta\omega, \theta^2, \dots\}$:

$$\beta = a_0 + a_1\omega + a_2\theta + a_3\theta\omega + \dots + a_{m-1}\theta^{n-1}$$

Since $\beta \in \mathbb{R}$, $\sigma(\beta) = \beta$ (where σ is complex conjugation). Therefore:

$$\begin{aligned} \beta &= \sigma(a_0 + a_1\omega + a_2\theta + a_3\theta\omega + \dots + a_{m-1}\theta^{n-1}) \\ &= \sigma(a_0) + \sigma(a_1\omega) + \sigma(a_2\theta) + \sigma(a_3\theta\omega) + \dots + \sigma(a_{m-1}\theta^{n-1}) \\ &= a_0 + a_1\sigma(\omega) + a_2\sigma(\theta) + a_3\theta\sigma(\omega) + \dots + a_{m-1}\theta^{n-1} \\ &= a_0 + a_1\omega^{-1} + a_2\theta + a_3\theta\sigma(\omega) + \dots + a_{m-1}\theta^{n-1} \end{aligned}$$

Since the elements of basis are linearly independent, each odd a_i must be equal to 0, and so β must be expressible as $a_0 + a_2\theta + \dots + a_{m-1}\theta^{n-1}$, and so $\mathbb{Q}[\theta]$ is an integral basis for $\mathbb{A} \cap \mathbb{Q}[\theta]$.

35. (g) Let p be an odd prime. Use exercise 23 to show that $\text{disc}(\theta) = \pm p^{(p-3)/2}$. Show the plus sign must hold.

By Exercise 23,

$$\begin{aligned} \text{disc}(1, \omega, \theta, \theta\omega, \dots, \theta^{n-1}) &= \text{disc}(\theta)^2 \text{N}_{\mathbb{Q}}^{\mathbb{Q}[\theta]} \text{disc}_{\mathbb{Q}[\theta]}^{\mathbb{Q}[\omega]}(\omega) \\ p^{p-2} &= \text{disc}(\theta)^2 \text{N}_{\mathbb{Q}}^{\mathbb{Q}[\theta]}(2\omega - \theta) \\ &= \text{disc}(\theta)^2 \text{N}_{\mathbb{Q}}^{\mathbb{Q}[\theta]}(\omega - \omega^{-1}) \\ &= \text{disc}(\theta)^2 \text{N}_{\mathbb{Q}}^{\mathbb{Q}[\theta]}(\omega^{-1}(\omega+1)(\omega-1)) \\ &= \text{disc}(\theta)^2 p \\ \pm p^{(p-3)/2} &= \text{disc}(\theta) \end{aligned}$$

As pointed out in the exercise, the square root of the discriminant is present in $\mathbb{Q}[\theta]$. Since $\mathbb{Q}[\theta] \subseteq \mathbb{R}$, $\text{disc}(\theta) = p^{(p-3)/2}$.

37. Let α be an algebraic integer of degree n over $\mathbb{Q}$ and let f and g be polynomials over $\mathbb{Q}$, each of degree $< n$, such that $f(\alpha) = g(\alpha)$. Show $f = g$.

Let $h(x)$ be the minimal polynomial for α. If $f(\alpha) = g(\alpha)$, then $(f - g)(\alpha) = 0$. Since h is the minimum polynomial for α, $h \mid f - g$. However, $f - g$ has degree $< n$, and so $f - g = 0$. Therefore $f = g$.

40. (a) Show $\operatorname{disc}(\alpha) = (d_1 d_2 \cdots d_{n-1})^2 \operatorname{disc}(R)$.

We first show $\operatorname{disc}(\alpha) = \operatorname{disc}(1, f_1(\alpha), \ldots, f_{n-1}(\alpha))$.

$$\operatorname{disc}(\alpha) = \operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1})$$

Since f_{n-1} is a monic polynomial with degree $n-1$ it is a linear combination of $\alpha, \ldots, \alpha^{n-1}$, and so generate the same additive subgroup of R_k. By Exercise 26,

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \operatorname{disc}(1, \alpha, \ldots, \alpha^{n-2}, f_{n-1}(\alpha))$$

Proceeding in this way we have

$$\operatorname{disc}(\alpha) = \operatorname{disc}(1, f_1(\alpha), \ldots, f_{n-1}(\alpha))$$

Finally, we have

$$\begin{aligned}
\operatorname{disc}(R) &= \operatorname{disc}(1, f_1(\alpha)/d_1, \ldots, f_{n-1}(\alpha)/d_{n-1}) \\
&= \frac{1}{d_1^2 \cdots d_{n-1}^2} \operatorname{disc}(1, f_1(\alpha)/d_1, \ldots, f_{n-1}(\alpha)/d_{n-1}) \\
&= \frac{1}{(d_1 \cdots d_{n-1})^2} \operatorname{disc}(\alpha)
\end{aligned}$$

Multiplying both sides by $(d_1 \cdots d_{n-1})^2$ gives the required result.

40. (b) We show that $R_k/\mathbb{Z}[\alpha]$ has order $d_1, \ldots, d_k$ by induction on k. Since $R = R_{n-1}$ the result with follow by induction.

For the base case we see that $1/\mathbb{Z}[\alpha]$ has order 1. Next let $R_k = R_{k-1} \oplus \frac{1}{d_k} f_k(\alpha)\mathbb{Z}$, so

$$R_k/\mathbb{Z}[\alpha] = R_{k-1}/\mathbb{Z}[\alpha] \oplus \frac{1}{d_k} f_k(\alpha)/\mathbb{Z}[\alpha]$$

By induction $R_{k-1}/\mathbb{Z}[\alpha]$ has order $d_1 \cdots d_{k-1}$. f_k is a monic polynomial in α and so $f_k(\alpha) \in \mathbb{Z}[\alpha]$, therefore $\frac{1}{d_k} f_k(\alpha)/\mathbb{Z}[\alpha] = \frac{1}{d_k}$ which has order d_k, so the order of $R_k = d_1 \cdots d_k$.

40. (c) Show if $i + j < n$ then $d_i d_j \mid d_{i+j}$.

Since $f_i(\alpha)/d_i$ and $f_j(\alpha)/d_j$ are members of the ring R, $f_i(\alpha) f_j(\alpha)/d_i d_j$ must also be a member of the ring R. $f_i(\alpha) f_j(\alpha)$ has order $i + j$. Since this is $< n$, this element by be generated by the basis elements of order $\le i+j$. Let a_k be the integers that generate this element. Then

$$\begin{aligned}\frac{f_i(\alpha)f_j(\alpha)}{d_i d_j} &= a_{i+j}\frac{f_{i+j}(\alpha)}{d_{i+j}} + \sum_{k=0}^{i+j-1} a_k \frac{f_k(\alpha)}{d_k} \\ f_i(\alpha)f_j(\alpha) &= a_{i+j}d_i d_j \frac{f_{i+j}(\alpha)}{d_{i+j}} + \text{Lower terms}\end{aligned}$$

We know $a_{i+j} \neq 0$. Since f_i, f_j, and f_{i+j} are each monic, the denominator must cancel with no remainder, giving $d_{i+j} = a_{i+j}d_i d_j$. Therefore $d_i d_j \mid d_{i+j}$.

40. (d) Take $\frac{f_1(\alpha)}{d_1}$ as the basis element of order 1, and raise this element to the i-th power. Each $(\frac{f_1(\alpha)}{d_1})^i$ is a polynomial of order i and so generated by the basis element $\frac{f_i(\alpha)}{d_i}$. By a similar argument as in 40. (c) (each of these terms is a monic polynomial and so the denominators must cancel with no remainder), $d_1^i \mid d_i$.

Let j_i be the remainder left when dividing d_i by d_1^i ($j_1 = 1$). Then:

$$\begin{aligned}\text{disc}(\alpha) &= (d_1 \cdots d_{n-1})^2 \text{disc}(R) \\ &= (d_1 d_1^2 \cdots d_1^{n-1} \prod_{i=0}^{n-1} j_i)^2 \text{disc}(R) \\ &= (d_1^{n(n-1)/2})^2 (\prod_{i=0}^{n-1} j_i)^2 \text{disc}(R) \\ &= d_1^{n(n-1)} (\prod_{i=0}^{n-1} j_i)^2 \text{disc}(R)\end{aligned}$$

Therefore $d^{n(n-1)} \mid \text{disc}(\alpha)$.

41. (a) Let m be a cubefree integer, $\alpha = \sqrt[3]{m}$, and write m as hk^2 with h, k relatively prime. Let $R = \mathbb{A} \cap \mathbb{Q}[\alpha]$. (Therefore k^2 has any square factors of m.). Show $\text{disc}(\alpha) = -27m^2$ (the 2018 edition has a typo).

Let $f(x) = x^3 - m$; $f(x)$ is the minimum polynomial of α over $\mathbb{Q}$ and has degree 3 (not $\equiv 0, 1$ (4)), so $\text{disc}(\alpha) = -\text{N}(f'(\alpha))$. $f'(\alpha) = 3\alpha^2$ so $\alpha f'(\alpha) = 3m$ and $f'(\alpha) = 3m/\alpha$. Note $\text{N}(\alpha) = m$ so $\text{N}(\alpha^{-1}) = 1/m$. Therefore we have

$$\text{N}(3m/\alpha) = 27m^3 \text{N}(\alpha^{-1}) = 27m^2$$
$$\text{disc}(\alpha) = -27m^2$$

Using Exercise 40, we see $-27m^2 = (d_1 d_2)^2 \text{disc}(R)$ and $d_1^2 | d_2$, so writing $d_2 = d_1^2 j$, we have

$$-27m^2 = d_1^4 j^2 \text{disc}(R)$$

Since d_1 has a sextic factor on the righthand-size, the only possibilities for d_1 are 1 or 3. If $d_1 = 3$ then $9 \mid m$.

41. (b) Show $d_1 = 1$ even when $9 \mid m$.

Suppose $9 \mid m$ and $d_1 = 3$. Then R has an integral basis with 1 and $(\alpha + a)/3$ as two of the three basis vectors.

Let $\beta = (\alpha + a)/3$ for some integer a. As suggested in the exercise hint we consider the trace of β^3. First, we determine the trace of α and α^2 as these will be important to evaluate $\mathrm{Tr}(\beta)$.

$$\mathrm{Tr}(\alpha) = \alpha + \omega\alpha + \omega^2\alpha = \alpha(\omega^2 + \omega + 1) = 0$$
$$\mathrm{Tr}(\alpha^2) = \alpha^2 + \omega^2\alpha^2 + \omega\alpha^2 = \alpha^2(\omega^2 + \omega + 1) = 0$$

With these in hand we now have

$$\beta^3 = \frac{(\alpha + a)^3}{27} = \frac{m + 3\alpha^2 a + 3a^2\alpha + a^3}{27}$$

By the additive linearity of trace, we have

$$\begin{aligned} \mathrm{Tr}(\beta^3) &= \frac{m}{9} + \frac{3a}{27}\mathrm{Tr}(\alpha^2) + \frac{3a^2}{27}\mathrm{Tr}(\alpha) + \frac{3a^3}{27} \\ &= \frac{m}{9} + \frac{3a^3}{27} \\ &= \text{Integer} + \frac{3a^3}{27} \end{aligned}$$

Since β is an algebraic integer, β^3 is also an algebraic integer, and its trace must be a member of $\mathbb{Z}$. Therefore $\frac{3a^3}{27}$ must be an integer, and so 27 must divide $3a^3$, which means that 9 divides a^3 and so 3 divides a.

Since 3 divides a, $\frac{\alpha+a}{3} = \frac{\alpha}{3} + \text{Integer}$. Therefore $\alpha/3$ is a member of R, so $(\alpha/3)^3 = m/27 \in R$. However, m is cubefree and so $m/27 \notin \mathbb{Z}$. This contradicts Corollary 1 of Theorem 1 - the only members of $\mathbb{Q}$ that are algebraic integers are members of $\mathbb{Z}$.

Therefore $d_1 = 1$ in all cases, and so R has a basis containing 1 and α. The third basis vector has yet to be determined.

41. (c) Write m as hk^2. Then $(\alpha^2/k)^3 = m^2/k^3 = (h^2k^4)(k^3) = h^2k$, and so α^2/k is the root of the polynomial $f(x) = x^3 - h^2k$, and so $\alpha^2/k \in R$.

41. (d) Suppose $m \equiv \pm 1\ (9)$. Let $\beta = (\alpha \mp 1)^2/3$. Show that

$$\beta^3 - \beta^2 + \frac{1 \pm 2m}{3}\beta - \frac{(m \mp 1)^2}{27} = 0$$

As suggested we calculate $(\beta - 1/3)^3$ in two ways:

$$\begin{aligned}
(\beta - 1/3)^3 &= ((\alpha \mp 1)^2/3 - 1/3)^3 \\
\beta^3 - \frac{3\beta^2}{3} + \frac{3\beta}{9} - \frac{1}{27} &= \frac{(\alpha(\alpha \mp 2))^3}{27} \\
\beta^3 - \beta^2 + \frac{\beta}{3} - \frac{1}{27} &= m\left(\frac{m \mp 6\alpha^2 + 12\alpha \mp 8}{27}\right) \\
\beta^3 - \beta^2 + \frac{\beta}{3} - \frac{m^2 \mp 2m + 1}{27} &= m\left(\frac{\mp 6\alpha^2 + 12\alpha \mp 6}{27}\right) \\
\beta^3 - \beta^2 + \frac{\beta}{3} - \frac{(m \mp 1)^2}{27} &= \mp\frac{2m}{3}\left(\frac{\alpha^2 \pm 2\alpha + 1}{3}\right) = \mp\frac{2m}{3}\beta
\end{aligned}$$

Moving the terms around, we have the required result:

$$\beta^3 - \beta^2 + \frac{1 \pm 2m}{3}\beta - \frac{(m \mp 1)^2}{27} = 0$$

Since $m \equiv \pm 1\ (9)$, $1 \pm 2m$ is divisible by 3, and $m \mp 1$ is divisible by 9, so $(m \mp 1)^2$ is divisible by 27. Therefore β is the root of a monic polynomial with integer coefficients and so $\beta \in R$.

41. (e) Using (c) and (d), show that if $m \equiv \pm 1\ (9)$ then

$$\frac{\alpha^2 \pm k^2\alpha + k^2}{3k} \in R$$

Since $\alpha^2/k \in R$, we can adding $k\alpha + k$ to the element to see that

$$\frac{\alpha^2 + k^2\alpha + k^2}{k} \in R$$

Next, observe that $k^2 \equiv 1\ (3)$ - it cannot be 0 since $m \equiv \pm 1\ (9)$. Therefore $(k^2 - 1)/3$ and $(k^2 + 2)/3$ are integers. Taking $(\alpha^2 \mp 2\alpha + 1)/3$, we add $(k^2 - 1)/3$ to see that

$$\frac{\alpha^2 \mp 2\alpha + k^2}{3} \in R$$

Next we have

$$\frac{\alpha^2 \mp 2\alpha + k^2}{3} \pm \frac{\alpha(k^2 - 2)}{3} = \frac{\alpha^2 \pm k^2\alpha + k^2}{3} \in R$$

Since $3 \nmid k$ and 3 is a prime, there exist integers a, b such that $3a + bk = 1$. Therefore

$$\begin{aligned}
b\left(\frac{\alpha^2 \pm k^2\alpha + k^2}{3}\right) + a\left(\frac{\alpha^2 \pm k^2\alpha + k^2}{k}\right) &= \frac{(kb + 3a)(\alpha^2 \pm k^2\alpha + k^2)}{3k} \\
&= \frac{\alpha^2 \pm k^2\alpha + k^2}{3k} \in R
\end{aligned}$$

This is the required result.

41. (f) We have $\operatorname{disc}(\alpha) = -27m^2$. By Exercise 40(a), $d_2^2\operatorname{disc}(R) = \operatorname{disc}(\alpha) = -27m^2 = -27h^2k^4$. We know $k \mid d_2$ so write $d_2 = jk$, thus $j^2k^2\operatorname{disc}(R) = -27h^2k^4$ and so $j^2\operatorname{disc}(R) = -27h^2k^2 = -27mh$. By assumption h is squarefree, so $j^2 \mid -27m$, implying either $j \mid 3$ or $j \mid m$. Therefore $j \mid 3m$.

41. (g) Letting p be a prime such that $p \neq 3$, $p \mid m$, $p^2 \mid m$. Let $p \mid d_2$, and write $d_2 = pj$. Therefore if $(\alpha^2 + a\alpha + b)/d_2 \in R$, then

$$j(\alpha^2 + a\alpha + b)/d_2 = (\alpha^2 + a\alpha + b)/p \in R$$

Since $(\alpha^2 + a\alpha + b)/p \in R$, its trace must be an integer; however $\operatorname{Tr}(\alpha^2) = \operatorname{Tr}(\alpha) = 0$, and so $3b/p \in \mathbb{Z}$. $p \neq 3$, therefore $p \mid b$. Therefore $(\alpha^2 + a\alpha)/p \in R$.

$$\operatorname{Tr}(((\alpha^2 + a\alpha)/p)^3) = \operatorname{Tr}((m^2 + a^3m)/p^3)$$

Therefore $p^3 \mid 3(m^2 + a^3m)$. Since $p \neq 3$, $p^3 \mid m(m + a^3)$. m is cubefree and $p^2 \nmid m$, so $p^2 \mid m + a^3$. Therefore $a^3 \equiv 0\ (p)$, meaning $a \equiv 0\ (p)$. Considering the equation modulo p^2 we then have $m \equiv 0\ (p^2)$, a contradiction. Therefore this case is impossible.

41. (h) Let $p \neq 3$ and $p^2 \mid m$. By the previous problem $(\alpha^2 + a\alpha)/p^2 \in R$ and so we consider the trace:

$$\operatorname{Tr}(((\alpha^2 + a\alpha)/p^2)^3) = \operatorname{Tr}((m^2 + a^3m)/p^6)$$

Therefore $p^6 \mid m(m + a^3)$. Since $p^2 \mid m$, $p^4 \mid m + a^3$. Considering the equation modulo p^2, we must have $a^3 \equiv 0\ (p^2)$, so $p^2 \mid a^3$. Therefore $p \mid a$ and so $p^3 \mid a^3$. Therefore $m + a^3 \equiv 0\ (p^3)$ and so $m \equiv 0\ (p^3)$ again contradicting m cubefree.

Together with (g) this shows that d_2 has no common prime factor with m that is not equal to 3.

41. (i) Take $(\alpha^2 + a\alpha + b)/d_2$.

$$\begin{aligned} \frac{(\alpha^2 + a\alpha + b)^2}{d_2^2} &= \frac{m\alpha + 2am + 2\alpha^2 b + a^2\alpha^2 + 2ab\alpha + b^2}{d_2^2} \\ &= \frac{\alpha^2(a^2 + 2b) + \alpha(m + 2ab) + (2am + b^2)}{d_2^2} \end{aligned}$$

Since this is an element of the ring and the basis element of order 2 has denominator d_2, d_2 must divide each of $a^2 + 2b$, $m + 2ab$, and $2am + b^2$.

41. (j) We now consider what power of 3 divides d_2. We know $d_2 \mid 3m$. If $3 \nmid m$, then $9 \nmid d_2$. Therefore, if $m \equiv \pm 1\ (9)$, $d_2 = 3k$; it cannot be any non-3 prime dividing m by (g) and (h), and 9 does not divide m.

We now consider the case where $m \not\equiv \pm 1\ (9)$ and $3 \nmid m$. We assume $3 \mid d_2$ (to show a contradiction).

We evaluate the congruences obtained in (i) modulo 3. Since $a^2+2b \equiv 0\ (3)$, $a^2 - b \equiv 0\ (3)$, and so $b \equiv a^2\ (3)$. Substituting b with a^2 in the equation $m + 2ab \equiv 0\ (3)$, we have $m + 2a^3 \equiv 0\ (3)$ and so $m - a^3 \equiv m - a \equiv 0\ (3)$, so therefore $a \equiv m\ (3)$. Substituting m for a in the equivalence $b^2 + 2am \equiv 0\ (3)$, we have $b^2 \equiv -2a^2 \equiv a^2\ (3)$. Therefore since $a^2 + 2b \equiv 0\ (3)$, we have $b(b+2) \equiv b(b-1) \equiv 0\ (3)$. $b \not\equiv 0\ (3)$ (as this would imply $m \equiv 0\ (3)$) so we must have $b \equiv 1\ (3)$.

Therefore we can write the basis element of order 2 as $\frac{\alpha^2+(m+3l)\alpha+(3j+1)}{3i}$ for some i, l, j, and so by multiplying through by i and subtracting the term $3l\alpha + 3j$ from the resulting fraction, we have:

$$\frac{\alpha^2 + m\alpha + 1}{3} \in R$$

We now proceed by case on m congruence to 3. (Almost there!)

Suppose $m \equiv 1\ (3)$. Then $\frac{\alpha^2+\alpha+1}{3} \in R$ and so by subtracing α, $\frac{\alpha^2-2\alpha+1}{3} = \frac{(\alpha-1)^2}{3} \in R$.

We raise this to the fourth power and take the trace. The only terms that contribute to the trace are those where α is raised to a power divisible by 3, so we have:

$$\begin{aligned} \mathrm{Tr}(\frac{(\alpha-1)^8}{3^4}) &= \frac{3}{3^4}\left(\binom{8}{6}\alpha^6(-1)^2 + \binom{8}{3}\alpha^3(-1)^5 + (-1)^8\right) \\ &= \frac{1}{27}\left(28m^2 - 56m + 1\right) \end{aligned}$$

Therefore, 27 must divide $28m^2 - 56m + 1$. Congruent to 9, this equation reduces to $m^2 - 2m + 1 \equiv 0\ (9)$ so $(m-1)^2 \equiv 0\ (9)$ and $m \equiv 1\ (9)$. This contradicts $m \not\equiv \pm 1\ (9)$. So m cannot be congruent to 1 mod 3.

Next, suppose $m \equiv 2\ (3)$. Threefore $\frac{\alpha^2+2\alpha+1}{3} = \frac{(\alpha+1)^2}{3} \in R$. Again we raise this to the fourth power and take the trace. (The equation is the same except for the negative terms.)

$$\mathrm{Tr}(\frac{(\alpha+1)^8}{3^4}) = \frac{1}{27}\left(28m^2 + 56m + 1\right)$$

Modulo 9 we have $m^2+2m+1 \equiv 0\ (9)$ so $(m+1)^2 \equiv 0\ (9)$ and so $m \equiv -1\ (9)$, again contradicting $m \not\equiv \pm 1\ (9)$.

Therefore if $3 \nmid m$ and $m \not\equiv \pm 1\ (9)$, $3 \nmid d_2$.

41. (k) Suppose $3 \mid m$ but $9 \nmid m$. We assume $3 \mid d_2$ to show a contradiction. By (i), $a^2 + 2b \equiv 0\ (3)$, so $a^2 \equiv b\ (3)$ (*). Plugging this into $m + 2ab \equiv 0\ (3)$ we have $m - a^3 \equiv 0\ (3)$. Since $a^3 \equiv a\ (3)$, we thus have $m \equiv a\ (3)$ and so $a \equiv 0\ (3)$, and also $b \equiv 0\ (3)$ by (*).

Therefore we can write the basis element of order 2 as $\frac{\alpha^2+3i\alpha+3j}{3l}$, and by multiplying through by l and subtracting $i\alpha + j$, we have $\frac{\alpha^2}{3} \in R$. Cubing this element and taking the trace we must have $m^2/9 \in \mathbb{Z}$, contradicting $9 \nmid m$. Therefore $3 \nmid d_2$.

41. (l) Suppose $9 \mid m$. We show $9 \nmid d_2$. Assume $9 \mid d_2$ (to show a contradiction). By (i), $9 \mid ab$ and $9 \mid b^2$ so either $9 \mid b$ or $3 \mid b$. Assume $3 \mid b$, therefore since $a^2 + 2b \equiv 0$ (9), we must have $a^2 \equiv -6 \equiv 3$ (9). However, 3 is not the square of any element mod 9, so this equation is unsatisfiable. We must have $9 \mid b$.

Therefore, $(a^2+a\alpha)/9 \in R$. Taking this to the third power and considering the trace, we must have $9^3 \mid 3(m^2+ma^3)$ and $9^2 3 \mid m(m+a^3)$. Since m is cubefree and $9 \mid m$, therefore $27 \mid m+a^3$. Considering $m+a^3$ modulo 9, we have $a^3 \equiv 0$ (9); therefore a must be congruent to 0, 3, or 6 modulo 9. In all these cases we have $a^2 \equiv 0$ (9). Since $9^2 \mid a^3$ and $9^2 \mid (m+a^3)$, $9^2 \mid m$, which contradicts m being cube-free. Therefore $9 \nmid d_2$.

43. (a) Let $f(x) = x^5 + ax + b$ with $a, b \in \mathbb{Z}$ and f irreducible over $\mathbb{Q}$. Let α be a root of f. Show $\operatorname{disc}(\alpha) = 4^4a^5 + 5^5b^4$.

We proceed in a similar fashion to Exercise 28: first, we determine $f'(\alpha)$, then we determine $\mathrm{N}(f'(\alpha))$ by collecting the most and least significant the coefficients of its polynomial.

$f'(x) = 5x^4 + a$, so $\alpha f'(x) = 5\alpha^5 + a = -5(a\alpha + b) + a = -4a\alpha - 5b$ and $f'(\alpha) = (-4a\alpha - 5b)/\alpha$. The expression $4a\alpha + 5b$ is a root of the polynomial $(\frac{x-5b}{4a})^5 + a(\frac{x-5b}{4a}) + b$. The norm $\mathrm{N}(4a\alpha + 5b)$ is the negative of the x^0 coefficient divided by the x^5 coefficient (again, negative because 5 is odd), so we calculate those values.

The x^0 coefficient is $(\frac{-5b}{4a})^5 + a(\frac{-5b}{4a}) + b = (\frac{-5b}{4a})^5 + \frac{-b}{4}$, and the x^5 coefficient is $(\frac{1}{4a})^5$, so $\mathrm{N}(4a\alpha + 5b) = 5^5b^5 + 4^4a^5b$.

Therefore,

$$\operatorname{disc}(\alpha) = \mathrm{N}(-(4a\alpha + 5b)/\alpha) = -\frac{5^5b^5 + 4^4a^5b}{-b} = 5^5b^4 + 4^4a^5$$

This is the required result. (The plus sign for the discriminant holds because $5 \equiv 1$ (4))

43. (b) Suppose $\alpha^5 = \alpha + 1$. We are given that this polynomial is irreducible because it is irreducible modulo 3. (The options are 0, 1, and 2: $0^5 \not\equiv 0 + 1$ (3), $1^5 \not\equiv 1 + 1$ (3), and $2^5 = 2 \not\equiv 1 + 2 = 0$ (3).)

In this case $a = -1$ and $b = -1$ so the above formula gives $\operatorname{disc}(\alpha) = 5^5 - 4^4 = 125 \cdot 25 - 16 \cdot 16 = 2869 = 19 \cdot 151$. Since the discriminant is squarefree, $\mathbb{A} \cap \mathbb{Q}[\alpha] = \mathbb{Z}[\alpha]$.

43. (c) Let a be squarefree and not equal to ± 1. Let α be a root and d_1, d_2, d_3, d_4 be as in Theorem 13. Prove that if $4^4 a + 5^5$ is squarefree then $d_1 = d_2 = 1$ and $d_3 d_4 \mid a^2$.

By exercise 40,

$$\operatorname{disc}(\alpha) = 5^5 a^4 + 4^4 a^5 = a^4(5^5 + 4^4 a) = (d_1 d_2 d_3 d_4)^2 \operatorname{disc}(R)$$

Here $d_1 d_2 \mid d_3$, $d_1 d_2 \mid d_4$, and $d_1 d_3 \mid d_4$. Therefore d_1 and d_2 both have 6 factors represented in the $\operatorname{disc}(\alpha)$ expression which is impossible unless they are both 1. Since $5^5 + 4^4 a$ is squarefree, $(d_3 d_4)^2$ must divide a^4 and so $d_3 d_4 \mid a^2$.

Verify that $4^4 a + 5^5$ is squarefree when $a = -2, -3, -6, -7, -10, -11, -13$, and -15.

```
sage: [(factor(x), is_squarefree(x)) for x in
       map(lambda a: 5^5 + 4^4 *a,
       [-2, -3, -6, -7, -10, -11, -13, -15])]

[(3 * 13 * 67, True),
    (2357, True),
    (7 * 227, True),
    (31 * 43, True),
    (5 * 113, True),
    (3 * 103, True),
    (-1 * 7 * 29, True),
    (-1 * 5 * 11 * 13, True)]
```

Experimenting a bit more with Sage, we can quickly test integers using the following code:

```
sage: def test_poly_degree_5(a):
....:     return (is_squarefree(5^5 + 4^4 *a) and
....:             is_squarefree(a))
....:
sage: filter(lambda x: test_poly_degree_5(x),
....:        range(2, 30))
[2, 3, 5, 6, 7, 10, 11, 14, 15, 17, 19, 21, 23, 26, 29]
sage: filter(lambda x: test_poly_degree_5(x),
....:        range(-2, -30, -1))
[-2, -3, -6, -7, -10, -11, -13, -15, -17, -19, -21,
 -22, -26, -29]
```

43. (d) Let α be as in part (c) (α is the root of a polynomial $f(x) = x^5 + ax + a$). Show $\alpha + 1$ is a unit.

We have $\alpha^5 = -a(\alpha+1)$, so we take the norm of both sides. $\mathrm{N}(\alpha^5) = -a^5 = \mathrm{N}(-a)\mathrm{N}(\alpha+1) = -a^5\mathrm{N}(\alpha+1$, so $\mathrm{N}(\alpha+1) = 1$. Therefore $\alpha+1$ is a unit in $\mathbb{A}\cap\mathbb{Q}[\alpha]$.

44. (a) Let $f(x) = x^5+ax^4+b$ where $a,b\in\mathbb{Z}$, and let α be a root of f. To determine the discriminant of α, we proceed as in exercise 28 and 43. The derivative of $f(x)$ is $f'(x) = 5x^4+4ax^3$, so

$$f'(\alpha) = \alpha^3(5\alpha+4a)$$

$\mathrm{N}(a^3) = -b^3$ so determine the norm of $5\alpha+4a$ by observing it is the root of the polynomial $(\frac{x-4a}{5})^5+(\frac{x-4a}{5})^4+b$. The x^0 term is $(\frac{-4a}{5})^5+(\frac{-4a}{5})^4+b$ while the x^5 term is $\frac{1}{5^5}$,

$$\mathrm{N}(5\alpha+4a) = (4a)^5 - 5a(4a)^4 - 5^5b = -(4a)^5\cdot(-4+5) - 5^5b = -(4^5a^5+5^5b)$$

Therefore $\mathrm{disc}(\alpha) = (4^5a^5+5^5b)b^3$ as required (the discriminant is positive since $5\equiv 1\ (4)$).

44. (b) TODO

45. Let α be the root of the polynomial $f(x) = x^n+ax+b$. Find a formula for $\mathrm{disc}(\alpha)$.

We proceed in similar fashion to exercise 43. $f'(\alpha) = n\alpha^{n-1}+a$, so we have:

$$\begin{aligned}
\alpha f'(\alpha) &= n\alpha + a\alpha \\
&= -n(a\alpha+b)+a\alpha \\
&= -((n-1)a\alpha+bn) \\
f'(\alpha) &= -((n-1)a\alpha+bn)/\alpha
\end{aligned}$$

We now calculate $\mathrm{N}((n-1)a\alpha+bn))$. This is the root of the polynomial

$$g(x) = \left(\frac{x-bn}{(n-1)a}\right)^n + a\left(\frac{x-bn}{(n-1)a}\right)+b$$

The norm is equal to $(-1)^n$ times the x_0 coordinate multiplied by the inverse of x_n coordinate. Therefore,

$$\mathrm{N}((n-1)a\alpha+bn) = (bn)^n + (-1)^{n+1}a^nb(n-1)^{n-1}$$

The inverse of the x_n coordinate is seen to be $((n-1)a)^n$

The discriminant is then (with the $\pm$ positive if $n\equiv 0,1\ (4)$, negative otherwise):

$$\begin{aligned}
\mathrm{disc}(\alpha) &= \frac{\pm(-1)^n\mathrm{N}((n-1)a\alpha+bn)}{b(-1)^n} \\
&= \frac{\pm(bn)^n+(-1)^{n+1}a^nb(n-1)^{n-1}}{b} \\
&= \pm[b^{n-1}n^n+(-1)^{n+1}a^n(n-1)^{n-1}]
\end{aligned}$$

Plugging values in gives:

$$
\begin{aligned}
n = 2 &= -(2^2 b - a^2) = a^2 - 4b \\
n = 3 &= -(27b^2) + a^3 2^2) = -27b^2 + 4a^3 \\
n = 4 &= b^3 4^4 - a^4 3^3 = 256b^3 - 27a^4 \\
n = 5 &= b^4 5^5 + a^5 4^4
\end{aligned}
$$

These agree with the known values of these polynomials.

Next, we calculate $\operatorname{disc}(\alpha)$ if α is a root of $x^n + ax^{n-1} + b$. The derivative $f'(\alpha) = n\alpha^{n-1} + a(n-1)\alpha^{n-2} = \alpha^{n-2}(\alpha n + a(n-1))$, so

$$\operatorname{disc}(\alpha) = \pm \mathrm{N}(f'(\alpha)) = \pm \mathrm{N}(\alpha^{n-2})\mathrm{N}(n\alpha + (n-1)a)$$

The norm $\mathrm{N}(\alpha^{n-2}) = \mathrm{N}(\alpha)^{n-2} = (-1)^n b^{n-2}$, so we only need to calculate $\mathrm{N}(n\alpha + (n-1)a)$. This is a root of the polynomial

$$\left(\frac{x - (n-1)a}{n}\right)^n + a\left(\frac{x - (n-1)a}{n}\right)^{n-1} + b$$

We now calculate the norm of this. The x_n coefficient is $\frac{1}{n^n}$, and the x_0 coefficient is

$$\left(-\frac{(n-1)a}{n}\right)^n + a\left(-\frac{(n-1)a}{n}\right)^{n-1} + b$$

Multiplying through by n^n gives us:

$$
\begin{aligned}
\mathrm{N}(n\alpha + (n-1)a) &= (-1)^n[(-1)^n(n-1)^n a^n + (-1)^{n-1} a^n (n-1)^{n-1} n + bn^n] \\
&= (n-1)^n a^n - a^n (n-1)^{n-1} n + (-1)^n bn^n \\
&= a^n (n-1)^{n-1}(n - 1 - n) + (-1)^n bn^n \\
&= -a^n (n-1)^{n-1} + (-1)^n bn^n
\end{aligned}
$$

Multiplying the norm by $(-1)^n b^{n-2}$ we have

$$\operatorname{disc}(\alpha) = \pm[bn^n + (-1)^{n-1} a^n (n-1)^{n-1}] b^{n-2}$$

This agrees with the answer to Exercise 44 (a) ($n = 5$) and I confirmed via Sage that the formula holds for some examples where $n = 4$ and $n = 6$:

```
sage: a = 4; b = -7; n = 4
sage: K.<g> = QQ.extension(x^4 + a*x^3 + b)
sage: K.disc([1, g, g^2, g^3])
-426496
sage: (b*n^n - a^n * (n - 1)^(n - 1))*b^(n-2)
-426496
sage: a = 3; b = -5; n = 6
sage: K.<g> = QQ.extension(x^6 + a*x^5 + b)
sage: K.disc([1, g, g^2, g^3, g^4, g^5])
1569628125
sage: -(b*n^n - a^n * (n - 1)^(n - 1))*b^(n-2)
1569628125
```

Chapter 3

2. Prove that every finite integral domain D is a field.

   For $\alpha \in D$, consider the set $\{1, \alpha, \alpha^2, \ldots\}$. Since D is finite this set must also be finite, so there must be some i, j, $i \neq j$ such that $\alpha^i = \alpha^j$. Thus $\alpha^{j-i} = 1$, and $\alpha^{j-i-1}\alpha = \alpha^{j-i} = 1$, so every element in D has an inverse, and D is therefore a field.

3. Let G be a free abelian group of rank n, with additive notation. Show for any $m \in \mathbb{Z}$, G/mG is the direct sum of n cyclic group of order m.

   Since G is a free abelian group of rank n,

   $$G \simeq \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ copies}}$$

   Therefore
   $$G/mG \simeq \underbrace{\mathbb{Z}/m\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m\mathbb{Z}}_{n \text{ copies}}$$

   Each $\mathbb{Z}/m\mathbb{Z}$ is a cyclic group of order m, so the order of G/mG is m^n.

4. Let K be any number field of degree n over $\mathbb{Q}$. Prove that every nonzero ideal I in $R = \mathbb{A} \cap K$ is a free abelian group of rank n.

   As an additive subgroup of R, I must be a free abelian group of order $\leq n$. Let $\{\beta_1, \ldots, \beta_n\}$ be a basis for R, and take $\alpha \in I$. $\{\alpha\beta_1, \ldots, \alpha\beta_n\} \subseteq I \subseteq R$ is a free abelian group of order n. Since I contains αI, the rank of I must also be n.

7. If $I + J = 1$ then there exist $\alpha \in I, \beta \in J$ such that $\alpha + \beta = 1$. Raising both powers to the $m + n$th power, we have $(\alpha + \beta)^{m+n} = 1^{m+n} = 1$. By the binomial theorem, $(\alpha + \beta)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n-k}{k} \alpha^{m+n-k}\beta^k$. If $k < n$, this element is a member of I^m (as $\alpha^{n+\text{positive}} \in I^m$); otherwise this element is a member of J^n. Therefore $(\alpha + \beta)^{m+n} \in I^m + J^n$.

8. (a) Suppose $I = (2, x)$ was generated by some $\alpha \in I$. Therefore there are $\beta, \gamma \in \mathbb{Z}[x]$ such that $\alpha\beta = 2$ and $\alpha\gamma = x$. Since $\alpha\beta = 2$, the rank of α must be 0; $\alpha \in \mathbb{Z}$. The only option is $\alpha = 2$ (since $1 \notin I$). However 2 is not a factor of x in $\mathbb{Z}[x]$. Therefore the ideal $(2, x)$ is not principal in $\mathbb{Z}[x]$.

8. (b) Let $f, g \in \mathbb{Z}[x]$ and let m, n be the gcd of the coefficients of f and g respectively. Prove mn is the gcd of the coefficients of fg.

   Since m and n are the gcds of f and g we can write

   $$f = m(a_0 + a_1 x + \ldots + a_j x^j) \tag{3}$$
   $$g = n(b_0 + b_1 x + \ldots + b_k x^k) \tag{4}$$

where $(a_0, \ldots, a_j) = 1$ and $(b_0, \ldots, b_k) = 1$. Let d be the GCD of the coefficients of fg. As

$$fg = mn(\sum_{0 \le l \le j} \sum_{0 \le m \le k} a_l b_m)$$

we know that $mn \mid d$.

Suppose there is some prime p such that p divides $a_l b_m$ for all l, m. Since $(a_0, \ldots, a_j) = 1$ and $(b_0, \ldots, b_m) = 1$, there is some first a_l and first b_m such that $p \nmid a_l$ and $p \nmid b_m$; so $p \mid a_0, \ldots, a_{l-1}$ but $p \nmid a_l$ and similarly $p \mid b_0, \ldots, b_{m-1}$ but $p \nmid b_m$. The x^{l+m} term in fg has coefficient $a_l b_m + a_{l+1} b_{m-1} + \ldots a_{l-1} b_{m+1} + \ldots$. Taken modulo p, $a_l b_m \not\equiv 0 \ (p)$ but p divides every other term in the expansion. This contradicts p being dividing the sum, and so there must be no other factor d beyond mn.

8. (c) Let $f \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Z}$. Show f is irreducible over $\mathbb{Q}$.

Suppose f is irreducible over $\mathbb{Z}$ but reducible over $\mathbb{Q}$, i.e. $f = gh$ for $g, h \in \mathbb{Q}[x]$. Then we can pull out the denominators from g, h, giving us $gh = \frac{g'h'}{d}$ where $g', h' \in \mathbb{Z}[x]$. Let a and b tbe the GCD of the coefficients of g' and h' respectively. We must have $ab! = d$ because otherwise then f would be reducible into the product of two polynomials in $\mathbb{Z}[x]$. Therefore, reducing to lowest terms if necessary, we have $ab \nmid d$. However, multiplying both sides of the equation by d gives $df = g'h' = ab(g''h'')$ for some g'' and h'' and so by (b), $ab \mid d$; this is a contradiction. Therefore f must be also irreducible over $\mathbb{Q}[x]$.

9. Let K and L be number fields, $K \subset L$, $R = \mathbb{A} \cap K, S = \mathbb{A} \cap L$.

9. (a) - TODO Let I and J be ideals in R and suppose $IS \mid JS$. Show $I \mid J$.

10. Show e and f are multiplicative in terms of towers.

Let $K \subset L \subset M$ and $R \subset S \subset T$ be the associated number fields and $P \subset Q \subset U$ prime ideals.

f is multiplicative: By the third isomorphism theorem, there is the field series of field inclusions: $R/P \to S/Q \to T/U$. $[S/Q : R/P] = f(Q|P)$ and $[T/U : S/Q] = f(U|Q)$; therefore the composition map from $R/P \to T/U$ must have degree $f(U|P) = f(Q|P)f(U|Q)$ by the tower law for field extensions.

e is multiplicative: $P = Q^{e(Q|P)} I$ and $Q = U^{e(U|Q)} J$ for ideals I, J such that $I + Q$ and $J + U$ are relatively prime. Therefore $P = U^{e(U|Q)e(Q|P)} IJ$ with $U^{e(Q|P)e(U|Q)}$ and IJ relatively prime; the factor of U dividing P is $e(U|P)$ so $e(U|P) = e(U|Q)e(Q|P)$.

11. Since $\alpha \in I$, $I \mid (\alpha)$, and so $I \cdot J = (\alpha)$. Taking norms of both sides, $\|I\| \cdot \|J\| = \|(a)\|$. By Theorem 22 (c), $\|(\alpha)\| = \mathrm{N}_{\mathbb{Q}}^{K}(\alpha)$, so $\|I\| \mid \mathrm{N}_{\mathbb{Q}}^{K}(\alpha)$, with equality holding if I is principal.

12. (a) Verify that $5S = (5, \alpha+2)(5, \alpha^2+3\alpha-1)$ in $S = \mathbb{Z}[\sqrt[3]{2}]$, $\alpha = \sqrt[3]{2}$.

Let $I = (5, \alpha+2)(5, \alpha^2+3\alpha-1)$. The generators of I are:

$$5^2 \tag{1}$$
$$5(\alpha^2+3\alpha-1) \tag{2}$$
$$5(\alpha+2) \tag{3}$$
$$(\alpha+2)(\alpha^2+3\alpha-1) = \alpha^3+(3+2)\alpha^2+(-1+6)\alpha-2 = 5(\alpha^2+\alpha) \tag{4}$$

All generators have a factor of 5 so $1 \notin I$; therefore $5 \subset I$. We have $\alpha \cdot (3) - (1) + 3 \cdot (2) = 45$, so $\gcd(45, 5^2) = 5 \in I$. Therefore $(3) - 10 = 5\alpha \in I$ and also $5\alpha^2 \in I$ by subtracting factors from (2); therefore $I = 5S$.

12. (b) Show there is an isomorphism between $\mathbb{Z}[x]/(5, x^2+3x-1)$ and $\mathbb{Z}_5[x]/(x^2+3x-1)$.

Let $a \in \mathbb{Z}[x]/(5, x^2+3x-1)$. Then a can be associated with a coset representative $f(x)+5g(x)+(x^2+3x-1)h(x)$ where all of the coefficients of $f(x)$ and $h(x)$ are less than 5 (other terms can be placed in $g(x)$).

Let ρ be the mapping of $\mathbb{Z}[x] \to \mathbb{Z}_5[x]$ by reducing the coefficients mod 5. $\rho(a) = \rho(f(x)) + (x^2+3x-1)\rho(h(x)) = f(x) + (x^2+3x-1)h(x)$ and so ρ is an isomorphism from the quotient ring $\mathbb{Z}[x]/(5, x^2+3x-1)$ to $\mathbb{Z}_5[x]/(x^2+3x-1)$.

12. (c) Show there is a surjective homomorphism from $\mathbb{Z}[x]/(5, x^2+3x-1)$ onto $S/(5, \alpha^2+3\alpha-1)$.

The ring homomorphism ψ from $\mathbb{Z}[x] \to S$ defined by $\psi(x) = \alpha$ is a surjective. Let $\beta \in S$; $\beta = m_0 + m_1\alpha + m_2\alpha^2$ for integers m_0, m_1, m_2, so $f(m_0 + m_1 x + m_2 x^2) = \beta$. Therefore the surjective ψ induces a surjection $\hat{\psi}$ on the quotient rings:

$$\mathbb{Z}[x]/(5, x^2+3x+1) \to S/(5, \alpha^2+3\alpha-1)$$

This utilizes the following lemma on ring homomorphisms:

Lemma 1. *Let R and R' be rings and ψ be a sujection $R \to R'$. Let I be an ideal of R. Then the mapping that ψ induces between the quotient groups $R/I \to R/\psi(I)$ is also a surjection.*

Proof. Take $a \in R/\psi(I)$; then $a = r' + \psi(I)$ for $r' \in R'$. Since ψ is surjective there must be some $r \in R$ such that $\psi(r) = r'$; therefore the coset $r + I$ is mapped to $r' + \psi(I)$, and the mapping between the quotient groups is also surjective. □

12. (d) In $\mathbb{Z}_5$, the polynomial $f(x) = x^2+3x-1 = x^2+3x+4$ is irreducible. Any factor must be a a root, and manual testing gives $f(0) = 4, f(1) = 3, f(2) =$

4, $f(3) = 2$, and $f(4) = 2$, so the polynomial has no root and is irreducible. Therefore $\mathbb{Z}_5/(x^2 + 3x - 1)$ is a field of order $5^2 = 25$.

Let $I = (5, \alpha^2 + 3\alpha - 1)$. By (b) and (c) there is a surjection $\hat{\psi}$ from $\mathbb{Z}_5/(x^2+3x-1)$ onto S/I. As $\hat{\psi}$ is onto and the source ring has cardinality 25, S/I must have a cardinality dividing 25; the options are 1 ($R = S$), 5, and 25 ($S/I \simeq \mathbb{Z}_5/(x^2 + 3x - 1)$).

Assume $|S/I| = 5$; we derive a contradiction. Since $\alpha^3 = 2$, we must have $2 \notin \operatorname{kern}(\psi)$ (otherwise $\alpha^3 = 0$ and so $\alpha \in \operatorname{kern}(\psi)$, giving $S \subset \operatorname{kern}(\psi)$). The only cube root of 2 modulo 5 is 3, so $\psi(\alpha) = 3$. However then $\psi(\alpha^2) = 4 + I$, $\psi(3\alpha) = 4 + I$, and $\psi(-1) = 4 + I$; thus $\psi(\alpha^2 + 3\alpha - 1) = 2$. But we know $\psi(\alpha^2 + 3\alpha - 1) = 0$. This is a contradiction, so $|S/I| \neq 5$.

Therefore $I = (5, \alpha^2 + 3\alpha - 1)$ is either the whole ring or a prime ideal inducing S/I to be a field of order 25.

12. (e) Suppose $(5, \alpha^2 + 3\alpha - 1) = S$. Then by (a), $5S = (5, \alpha + 2)S$; however, $\alpha + 2 \notin 5$, so $S/(5, \alpha^2 + 3\alpha - 1)$ must be a field of order 25.

13. (a) Let $S = \mathbb{Z}[\alpha]$, $\alpha^3 = \alpha + 1$. Verify $23S = (23, \alpha - 10)^2(23, \alpha - 3)$.

Let $I = (23, \alpha - 10)^2(23, \alpha - 3)$. The generators of I are:

$$23^3 \tag{1}$$
$$23^2(\alpha - 3) \tag{2}$$
$$23^2(\alpha - 10) \tag{3}$$
$$(\alpha - 10)^2(\alpha - 3) = -23(\alpha^2 - 7\alpha + 13) \tag{4}$$
$$23(\alpha - 10)^2 = 23(\alpha^2 - 20\alpha + 100) \tag{5}$$
$$23(\alpha - 10)(\alpha - 3) = 23(\alpha^2 - 13\alpha + 30) \tag{6}$$

From the generators it is clear that 23 divides every member of I, and so $23S \subset I$. To show the required result we need to show $\{23, 23\alpha, 23\alpha^2\} \in I$.

$$(4) + (5) = 23(-13\alpha + 87) \tag{7}$$
$$2 \cdot (6) - (5) + (4) = 23\alpha + 53 \cdot 23 \tag{8}$$
$$13 \cdot (8) - (7) = 23 \cdot 602 \tag{9}$$

From (1), (2), and (3), we must have $23^2 \in I$ as this is the GCD of (1) with the sum of (2) and (3); since $23 \cdot 602 \in I$, therefore $23 \in$I as it is the GCD of these two integers. Subtracting a multiple of $23 \in$I from (8) gives us $23\alpha \in I$, and we thus have $23\alpha^2 \in I$ as well by subtracting the appropriate terms from (5) or (6). This verifies $\{23, 23\alpha, 23\alpha^2\} \in I$ and so $23S = (23, \alpha - 10)^2(23, \alpha - 3)$.

13. (b) Show that $(23, \alpha - 10, \alpha - 3) = S$. Conclude that $(23, \alpha - 10)$ and $(23, \alpha - 3)$ are relatively prime.

Since $-10 \cdot [(\alpha - 10) - (\alpha - 3)] - 3 \cdot 23 = 1$, $(23, \alpha - 10, \alpha - 3) = S$. Since $(23, \alpha - 10) \mid 23S$ and $(23, \alpha - 3) \mid 23S$, neither is the whole ring S and so they must be relatively prime ideals in S.

14. Let K and L are number fields, $K \subset L$, $R = \mathbb{A} \cap K, S = \mathbb{A} \cap L$. Assume L is normal over K and let G be the Galois group of L over K. Let $|G| = [K : L] = n$.

14. (a) Suppose Q and Q' are two primes of S lying over a prime P of R. Show the number of automorphisms σ such that $\sigma(Q) = Q$ is the same number of $\sigma \in G$ such that $\sigma(Q) = Q'$. Conclude this number is $e(Q|P)f(Q|P)$.

Enumerate the distinct automorphisms fixing Q as $\sigma_0, \dots, \sigma_k$, and the automorphisms taking Q to Q' as $\tau_0, \dots, \tau_l$. Let τ be one of the automorphisms taking Q to Q' (by Theorem 23, this must exist) and consider the automorphisms $\sigma_0\tau, \dots, \sigma_k\tau$. These are k distinct automorphisms taking Q to Q' (if $\sigma_i\tau = \sigma_j\tau$ then $\sigma_i = \sigma_j$), so $k \le l$. Conversely, consider the automorphisms $\tau\tau_0^{-1}, \dots, \tau\tau_l^{-1}$ taking Q to Q. Each of these must be one of the σ_k, and each must be distinct; if $\tau\tau_i^{-1} = \tau\tau_j^{-1}$ then $\tau_i = \tau_j$, so $l \le k$. Therefore $l = k$.

We count the number of permutations in G so as to determine the number of permutations fixing Q (call this number k). For each prime P, there are r distinct primes $Q_1, \dots, Q_r$ lying over P, and so there are k automorphisms taking Q_1 to Q_1, k automorphisms taking Q_1 to Q_2, etc. Therefore $n = kr$; since $n = re(Q|P)f(Q|P)$, $k = e(Q|P)f(Q|P)$.

14. (b) For an ideal $I \subset S$, define $\mathrm{N}_K^L(I)$ to be the ideal $R \cap \prod_{\sigma \in G} \sigma(I)$. Show that for a prime Q lying over P, $\mathrm{N}_K^L(Q) = P^{f(Q|P)}$.

Let $e = e(Q|P)$, $f = f(Q|P)$. and $Q_1, \dots, Q_r$ be the ideals of S lying over P. By (a) there are ef automorphisms sending Q to Q_1, Q to Q_2, etc. Therefore

$$\begin{aligned} \mathrm{N}_K^L(I) &= R \cap (Q_1^{ef} \cdots Q_l^{ef})S \\ &= R \cap (Q_1 \cdots Q_l)^{ef} S \\ &= R \cap P^f S \\ &= P^f \end{aligned}$$

□

14. (c) Let I be an ideal of S. Show $\prod_{\sigma \in G} \sigma(I) = (\mathrm{N}_K^L(I))S$.

Let $I = Q_1 \cdots Q_r S$; then $\prod_{\sigma \in G} \sigma(I) = \prod_{\sigma \in G} \sigma(Q_1) \cdots \sigma(Q_r)S$. With the product taken over all $\sigma \in Q$, $\prod \sigma(Q_i) = P_i$ for some prime ideal P_i of R lying under I; therefore $\prod_{\sigma \in G} \sigma(I) = P_1 \cdots P_r S = \mathrm{N}_K^L(I)S$.

14. (d)

$$
\begin{aligned}
\mathrm{N}_K^L(IJ) &= R \cap \prod_{\sigma\in G} \sigma(IJ) \\
&= R \cap \prod_{\sigma\in G} \sigma(IJ) \\
&= R \cap \prod_{\sigma\in G} \sigma(I) \prod_{\sigma\in G} \sigma(J) \\
&= R \cap (\mathrm{N}_K^L(I)\mathrm{N}_K^L(J)) \\
&= \mathrm{N}_K^L(I)\mathrm{N}_K^L(J)
\end{aligned}
$$

The final equality holds since $\mathrm{N}_K^L(I)$ and $\mathrm{N}_K^L(J)$ are ideals in R.

14. (e) If $\beta \in \mathrm{N}_K^L((\alpha))$, then $\beta = \sigma_1(\alpha)\cdots\sigma_k(\alpha)\gamma = \mathrm{N}_K^L(\alpha)\gamma$; since $\beta \in R$ and $\mathrm{N}_K^L(\alpha) \in R$, γ must also be in R. Thus $\mathrm{N}_K^L((\alpha))$ is the ideal generated by $\mathrm{N}_K^L(\alpha)$.

15. (a) Show for three fields $K \subset L \subset M$, that $\mathrm{N}_K^M(I) = \mathrm{N}_K^L\mathrm{N}_L^M(I)$ for an ideal $I \subset \mathbb{A} \cap M$.

We show the result for a prime U of $T = \mathbb{A} \cap M$. Let R, S be the ring of integers of K, L, M respectively, and let P and Q be the primes of R and S lying under U. Then using the multiplicativity of towers as shown in exercise 10,

$$\mathrm{N}_K^M(U) = P^{f(U|P)} = P^{f(U|S)f(S|P)} = \mathrm{N}_K^L\mathrm{N}_L^M(U)$$

If $I = U_1 \cdots U_r$, then

$$\mathrm{N}_K^M(I) = \prod_{i=0}^{r} \mathrm{N}_K^M(U_i) = \prod_{i=0}^{r} \mathrm{N}_K^L\mathrm{N}_L^M(U_i) = \mathrm{N}_K^L\mathrm{N}_L^M(I)$$

15. (b) Let $K \subset L$, where L is not necessarily normal. Extend L to a normal extension M. Let $[M : L] = n$. We then have:

$\mathrm{N}_K^M((\alpha))$	$= (\mathrm{N}_K^M(\alpha))$	(exercise 14. (e))
	$= (\mathrm{N}_K^L(\mathrm{N}_L^M(\alpha)))$	Definition of relative norm
	$= (\mathrm{N}_K^L(\alpha^n))$	$\alpha \in L$ and $L \subset M$
	$= (N_K^L(\alpha))^n$	Factorization of ideals

We also have the following transformation on the norm ideal of M over K:

$\mathrm{N}_K^M((\alpha))$	$= \mathrm{N}_K^L\mathrm{N}_L^M((\alpha))$	part (a)
	$= \mathrm{N}_K^L((\alpha^n))$	Exercise 14. (e), M is normal over L
	$= \mathrm{N}_K^L((\alpha)^n)$	Factorization of ideals
	$= \mathrm{N}_K^L((\alpha))^n$	Exercise 14. (d)

We therefore have
$$(\mathrm{N}_K^L(\alpha))^n = \mathrm{N}_K^L((\alpha))^n$$
and conclude that $\mathrm{N}_K^L(\alpha) = \mathrm{N}_K^L((\alpha))$.

15. (c) For the case where $K = \mathbb{Q}$, show that $\mathrm{N}_{\mathbb{Q}}^L(I)$ is the principal ideal in $\mathbb{Z}$ generated by the number $\|I\|$.

For a prime Q of L lying over a prime ideal $P \subset \mathbb{Z}$ containing the prime $p \in P$, $\mathrm{N}_{\mathbb{Q}}^L(Q) = P^f$, and $\|I\| = |R/Q| = p^f$. Next, suppose $I = Q_1 \cdots Q_r$ where Q_i lies over a prime P_i. By Theorem 22 (a), $\|I\| = \prod_{i=1}^r \|Q_i\| = \prod_{i=1}^r (P_i)^{f(Q_i|P_i)}$, this number then generates the principal ideal $\mathrm{N}_{\mathbb{Q}}^L(I) = \prod_{i=1}^r \mathrm{N}_{\mathbb{Q}}^L(Q_i) = \prod_{i=1}^r (P_i)^{f(Q_i|P_i)}$.

16. Let K and L be number fields, $K \subset L$, $R = \mathbb{A} \cap K, S = \mathbb{A} \cap L$. Denote by $G(R)$ and $G(S)$ the ideal class groups of R and S respectively.

16. (a) Show that the mapping $\psi : G(S) \to G(R)$ defined by taking any I in a given class C and sending C to the class containing $\mathrm{N}_K^L(I)$ is a homomorphism.

We first show that ψ homomorphism is well-defined. Take $I, J \in C$, so there is some element α, β such that $\alpha I = \beta J$. Therefore

$$\begin{aligned}
\mathrm{N}_K^L(\alpha I) &= \mathrm{N}_K^L(\beta J) \\
\mathrm{N}_K^L((\alpha))\mathrm{N}_K^L(I) &= \mathrm{N}_K^L((\beta))\mathrm{N}_K^L(J) \\
\mathrm{N}_K^L(\alpha)\mathrm{N}_K^L(I) &= \mathrm{N}_K^L(\beta)\mathrm{N}_K^L(J)
\end{aligned}$$

Therefore the image of I and J are in the same ideal class, ψ does not depend on the choice of ideal in the class C.

$\psi((\alpha)) = N_K^L((\alpha))$ and so the identity element of the class group maps to the identity element. $\psi(IJ) = \mathrm{N}_K^L(IJ) = \mathrm{N}_K^L(I)\mathrm{N}_K^L(J)$ and so the mapping respects operation. Therefore it is a homomorphism.

16. (b) Let Q be a prime of S lying over a prime P of R. Let d_Q denote the order of the class containing Q in $G(S)$, d_P denote the order of the class containing P in $G(R)$. Prove that $d_P \mid d_Q f$, where $f = f(Q|P)$.

Take $\psi : G(S) \to G(R)$ be the homomorphism defined in 1. Then $|\psi(Q)| \mid |Q|$. $\psi(Q) = P^f$; if $f \mid d_P$, $|\psi(Q)| = d_P/f$; otherwise $|\psi(Q)| = d_P$. In both cases we have $d_P \mid d_Q f$.

17. Let $K = \mathbb{Q}[\sqrt{23}], L = \mathbb{Q}[\omega]$, where $\omega = e^{2\pi i/23}$. Let P be one of the primes of K lying over 2; take $P = (2, \theta)$ where $\theta = (1 + \sqrt{-23})/2$, and let Q a prime of $\mathbb{Q}[\omega]$ lying over P.

17. (a)] By Theorem 25, $f(Q|2)$ is the multiplicative order of 2 mod 23; $2^{11} = 2048 \equiv 1$ (23). Since $f(P|2) = 1$ ($ref = [K : \mathbb{Q}] = 2$ and $r = 2$) and f is multiplicative in towers, $f(Q|P) = 11$.

17. (b) $P^3 = (\theta - 2)$:

$$P = (2, \theta), P^2 = (4, 2\theta, \theta - 6) = (4, \theta + 2)$$

and

$$P^3 = (8, 4\theta, 2\theta + 4, 3(\theta - 2)) = (\theta - 2)$$

First $\theta - 2 \in P^3 : 4\theta - 3(\theta - 2) - 8 = \theta - 2$. Then, we have $8 = (\theta - 2)(-\theta - 1)$, $4\theta = 4(\theta - 2) + 8$, $2\theta + 4 = 2(\theta - 2) + 8$, so every element of P^3 is representable as $\theta - 2$ and this is a principal ideal.

However, P is not principal: since $(2, \theta)(2, \overline{\theta}) = (2)$ and the norm of (2) is 4, the ideal $(2, \theta)$ must have norm 2. For it to be generated by a single α we would need some $(a + b\sqrt{-23})/2 \in \mathbb{Z}[\theta]$ where $a^2 + 23b^2 = 8$. This has no integer solution so $(2, \theta)$ is not a principal ideal.

Since P^3 is a principal ideal the ideal class group of $\mathbb{Q}[\sqrt{-23}]$ must have an order dividing 3.

17. (c) By 16. (b), the order of P divides the order of Q multiplied by $f(Q|P)$; therefore $3 \mid d_Q 11$ and so $3 \mid d_Q$. Therefore Q must also not be a principal ideal.

17. (d) Suppose $2 = \alpha\beta$ in $\mathbb{Z}[\omega]$ and neither α nor β is a unit, therefore $2\mathbb{Z}[\omega] = (\alpha)(\beta) = (2, \theta)(2, \overline{\theta})$. By the uniqueness of ideal factorization, $(2, \theta)$ must be principal; however, we have seen that this is not the case in part (c). This is a contradiction; therefore either α or β must be a unit.

18. (a) Show $\mathrm{disc}(r\alpha_1, \alpha_2, \ldots, \alpha_n) = r^2 \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$.

Writing the discriminant as the determinant of each of the σ_j conjugates of α_n, we have:

$$\mathrm{disc}(r\alpha_1, \alpha_2, \ldots, \alpha_n) = \begin{vmatrix} \sigma_1(r\alpha_1) & \cdots & \sigma_k(\alpha_n) \\ \sigma_2(r\alpha_1) & \cdots & \sigma_k(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_k(r\alpha_1) & \cdots & \sigma_k(\alpha_n) \end{vmatrix}^2$$

Let A_{ij} be the matrix minor corresponding to row i, column j. Since $r \in \mathbb{Q}$, $\sigma_k(r\alpha_1) = r\sigma_k(\alpha_1)$ for all k. Taking the determinant along the first column, we have:

$$\begin{aligned}
\mathrm{disc}(r\alpha_1, \alpha_2, \ldots, \alpha_n) &= \left(\sum_{i=0}^{n} (-1)^i \sigma_i(r\alpha_1) A_{1i} \right)^2 \\
&= \left(\sum_{i=0}^{n} (-1)^i r\sigma_i(\alpha_1) A_{1i} \right)^2 \\
&= r^2 \left(\sum_{i=0}^{n} (-1)^i \sigma_i(\alpha_1) A_{1i} \right)^2 \\
&= r^2 \mathrm{disc}(\alpha_1, \ldots, \alpha_n)
\end{aligned}$$

18. (b) Let β be a linear combination of $\alpha_2, \ldots, \alpha_n$ with coefficients in $\mathbb{Q}$. Show $\operatorname{disc}(\alpha_1 + \beta, \alpha_2, \ldots, \alpha_n) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$.

For all σ_k, $\sigma_k(\alpha_1+\beta) = \sigma_k(\alpha_1)+\sigma_k(\beta)$. If $\beta = p_2\alpha_2+\ldots+p_n\alpha_n$, then $\sigma_k(\beta) = p_2\sigma_k(\alpha_2) + \ldots + p_n\sigma_k(\alpha_n)$ for $p_i \in \mathbb{Q}$. Writing $\operatorname{disc}(\alpha_1 + \beta, \alpha_2, \ldots, \alpha_n)$ in matrix form, the k-th row of the first column has the form $\sigma_k(\alpha_1) + p_2\sigma_k(\alpha_2) + \ldots + p_n\sigma_k(\alpha_n)$.

Subtracting a column times a linear factor has no effect on the determinant of the matrix, so by subtracting p_i multiplied by column i from the first column for each i, we see $\operatorname{disc}(\alpha_1 + \beta, \alpha_2, \ldots, \alpha_n) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$.

19. Let K and L be number fields, $K \subset L$, and let $R = \mathbb{A} \cap K$, $S = \mathbb{A} \cap L$. Let P be a prime of R.

19. (a) - TODO Show that if $\alpha \in S$, $\beta \in R$, and $\alpha\beta \in PS$, then either $\alpha \in PS$ or $\beta \in P$.

24. Let R, K, S, L be as usual. A prime $P \subset R$ is *totally ramified* if $PS = Q^n$, $n = [L : K]$.

24. (a) Suppose P is totally ramified in S; then $PS = Q^n$. Let M be an extension field such that $K \subset M \subset L$ with $\mathbb{A} \cap M = T$. and U be a prime of M lying over P. Then $U \subset Q$ and $US = Q^{[M:L]}$. Since the ramification degree is multiplicative in towers, $[L : K] = e(Q|P) = e(Q|U)e(U|P) = [L : M]e(U|P)$; therefore $e(U|P) = [M : K]$ and so P is totally ramified in M.

24. (b) If P is totally ramified in some extension of L and unramified in L', then take $L \cap L'$ By (a), if $L \cap L' \subset L$ then $L \cap L'$ must be totally ramified. However $L \cap L' \subset L'$ and so must be unramified by assumption. We conclude $[L \cap L' : K] = 1$ so $L \cap L' = K$.

24. (c) Let $m = p_1^{e_1} \cdots p_r^{e_r}$. We prove $[\mathbb{Q}[\omega] : \mathbb{Q}] = \phi(m)$ by induction on r; TODO

28. Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ where all $a_i \in \mathbb{Z}$ and let p be a prime divisor of a_0 with p^r the exact power of p dividing a_0 and suppose all a_i are divisible by p^r. Assume f is irreducible over $\mathbb{Q}$ and let α be a root of f. Let $K = \mathbb{Q}[\alpha], R = \mathbb{A} \cap K$.

28. (a) $\alpha^n = -(a_{n-1}\alpha^{n-1}+\ldots+a_0) = p^r(\frac{-a_{n-1}}{p^r}\alpha^{n-1}+\ldots\frac{-a_0}{p^r})$, and let $\beta = \frac{-a_{n-1}}{p^r}\alpha^{n-1} + \ldots + \frac{-a_0}{p^r}$. Then $(\alpha^n) = (p^r)(\beta)$.

Let α have the factorization $\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m}$ in R; then $(\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m})^n = (p^r)(\beta)$ and so

$$\mathfrak{q}_1^{ne_1} \cdots \mathfrak{q}_m^{ne_m} = (p^r)(\beta)$$

If (p) is not relatively prime with (β), then there is some $\alpha' \in K$ such that $\beta\alpha' = p$; therefore $\beta\alpha' - p = 0$ would give a linear dependence of the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ over $\mathbb{Q}$, but this set is linearly independent. Therefore (p) and (β) have mutually exclusive factors in R and so (reordering the $\mathfrak{q}_i$ if necessary),

$$(p^r) = \mathfrak{q}_1^{ne_1} \cdots \mathfrak{q}_k^{ne_k} = \left(\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_k^{e_k}\right)^n$$

. Therefore (p^r) is an n-th power in R.

28. (b) Given the factorization from part (a), we know r divides ne_i for all i; if $(n,r) = 1$, then r must divide each of the e_i. Since p^r is an nr-th power, p is an n-th power.

Since the primes lying over p must have $ref = 1$, we conclude in the factorization of (p^r) must have $e_i = r$ and $f = 1$ and so we have the factorizations $(p^r) = (\mathfrak{q}^r)^n$ and $(p) = (\mathfrak{q})^n$; therefore p is totally ramified in R.

28. (c) If r is relatively prime to n, p is totally ramified in R and so $\sum f_i = 1$ and thus by Exercise 21 (b), $p^{n-1} \mid \mathrm{disc}(R)$.

We now examine the scenario where $\gcd(n,r) = m$ and take the factorization from part (a). As in (b), we know r must divide ne_i for all i, and so $\frac{r}{m}$ divides $\frac{n}{m}e_i$ for each of the e_i. Since (p^r) is an n-th power, then

$$\begin{aligned}(p)^r &= \left(\mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_k^{e_k}\right)^n \\ (p)^{r/m} &= \left(\mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_k^{e_k}\right)^{n/m} \\ (p) &= \left(\mathfrak{q}_1^{\frac{me_1}{r}}\cdots\mathfrak{q}_k^{\frac{me_k}{r}}\right)^{n/m}\end{aligned}$$

Therefore, if $d \neq n$, (p) is ramified with ramification degree at least n/d.

We know that for any prime of $\mathbb{Z}$, $ref = n$; therefore

$$\sum_{i=0}^{k} \frac{n}{m}\frac{me_if_i}{r} = \frac{n}{m}\sum_{i=0}^{k}\frac{me_if_i}{r}$$

and so we must have $\sum_{i=0}^{k} \frac{me_if_i}{r} = m$. Each of the terms are integers and so $\sum f_i \leq m$; therefore by applying Exercise 21 (b), we have $p^{n-m} \mid \mathrm{disc}(R)$.

This bound is as good as possible. Let $K = \mathbb{Q}[\alpha]$ where α is a root to the irreducible polynomial $x^4 + 3^2$ and let $R = \mathbb{A} \cap K$. $\mathrm{disc}(K) = 2^8 \cdot 3^2$, so 3^2 is the greatest power dividing the discriminant $(2 = 4 - \gcd(4,2))$. The prime 3 has the factorization $3R = (\alpha)^2$, and so the inertial degree of $(\alpha) = 2$.

28. (d) In both 43 (c) and 44 (d) we have α a root of a degree 5 polynomial satisfying the conditions of 28 (a) with the a_0 coefficient $= a$ where a is squarefree.

For both equations, we have $p \mid a$, by (c) that $p^4 \mid \mathrm{disc}(R)$. We have shown for both that $d_3d_4 \mid a^2$, and we know $d_3 \mid d_4$.

43 (c): $\mathrm{disc}(\alpha) = a^4(4^4a + 5^5) = (d_3d_4)^2\mathrm{disc}(R)$. By assumption $4^4a + 5^5$ is squarefree. Suppose $p \mid d_3$ or $p \mid d_4$; then $p^6 \mid (d_3d_4)^2\mathrm{disc}(R)$. This implies $a^2 \mid 4^4a + 5^5$, contradicting $4^4a + 5^5$ squarefree.

44 (d): $\mathrm{disc}(\alpha) = a^4[(4a)^4 + 5^5] = (d_3d_4)^2\mathrm{disc}(R)$. As in the previous case, $p^6 \mid (d_3d_4)^2\mathrm{disc}(R)$ and so $a^2 \mid (4a)^4 + 5^5$, contradicting the assumption that this quantity is squarefree.

29. Let α be an algebraic integer and let f be a monic irreducible polynomial for α over $\mathbb{Z}$. Let $R = \mathbb{A} \cap \mathbb{Q}[\alpha]$ and suppose p is a prime in $\mathbb{Z}$ such that f has a root r in $\mathbb{Z}_p$ and $p \nmid |R/\mathbb{Z}[\alpha]$.

29. (a) Show there is a ring homomorphism $R \to \mathbb{Z}_p$ that takes α to r.

Since $f(r) \equiv 0\ (p)$ and $p \nmid |R/\mathbb{Z}[\alpha]|$, by Theorem 27, the prime ideal $Q = (p, \alpha - r)$ lies over P. As $x - r$ is a factor of $f(x)$ mod p, the inertial degree of Q is 1, and so $|R/Q| = |p|$, so $R/Q \simeq \mathbb{Z}_p$. Let ψ be the mapping from R to its quotient ring R/Q: since $\alpha - r \in Q$, $\psi(\alpha) = r$.

29. (b) Let $\alpha^3 = \alpha + 1$. Show $\sqrt{\alpha} \notin \mathbb{Q}[\alpha]$.

By exercise 2.28, $\mathbb{A} \cap \mathbb{Q}[\alpha] = \mathbb{Z}[\alpha]$, so $|\mathbb{Z}[\alpha]/\mathbb{Z}[\alpha]| = 1$. Since $\mathbb{Z}[\alpha]$ is integrally closed in $\mathbb{Q}[\alpha]$ it suffices to show $\sqrt{\alpha} \notin \mathbb{Z}[\alpha]$: we will do this by finding appropriate r, p such that r is a root of $x^3 - x - 1$ mod p and r is not a square mod p.

As suggested in the hint, we take $r = 2$ and $p = 5$. $2^3 - 2 - 1 \equiv 0\ (5)$ and there is a ring homomorphism ψ from $\mathbb{Z}[\alpha] \to \mathbb{Z}_5$ where $\psi(\alpha) = 2$. If $\sqrt{\alpha} \in \mathbb{Z}[\alpha]$, then $\psi(\sqrt{\alpha})^2 = 2$; however, 2 is not a square mod 5. Therefore $\sqrt{\alpha} \notin \mathbb{Z}[\alpha]$ and so $\sqrt{\alpha} \notin \mathbb{Q}[\alpha]$.

29. (c) Show $\sqrt[3]{\alpha}$ and $\sqrt{\alpha + 2}$ are not in $\mathbb{Q}[\alpha]$.

$\sqrt[3]{\alpha} \notin \mathbb{Q}[\alpha]$: Let $r = 5$; then $5^3 - 5 - 1 = 119 \equiv 0\ (7)$; however there is no element such that $x^3 \equiv 5\ (7)$. Therefore $\sqrt[3]{\alpha} \notin \mathbb{Q}[\alpha]$.

$\sqrt{\alpha + 2}$: Let $r = 3$; then $3^3 - 3 - 1 = 23 \equiv 0\ (23)$; however 5 is not a quadratic residue mod 23. Therefore $\sqrt{\alpha + 2} \notin \mathbb{Q}[\alpha]$.

29. (d) Let $\alpha^5 + 2\alpha = 2$. Prove $x^4 + y^4 + z^4 = \alpha$ has no solutions in $\mathbb{A} \cap \mathbb{Q}[\alpha]$. By exercise 2.43, $\operatorname{disc}(\alpha) = 4^4(2)^5 + 5^5(-2)^4 = 58192 = 2^4 * 3637$ so all primes except 2 and 3637 satisfy $|\mathbb{A} \cap Q[\alpha] : \mathbb{Z}[\alpha]|$.

Taking $r = 4$ and $p = 5$, we see $4^5 + 2 \cdot 4 - 2 = 130 \equiv 0\ (5)$. Letting ψ be the homomorphism from (a), we observe that if there were x, y, z such that $x^4 + y^4 + z^4 = \alpha$, we would have $\psi(x^4 + y^4 + z^4) = \psi(\alpha) = 4$. However in $\mathbb{Z}_5$, $x^4 \equiv 1$ for all x so $\psi(x^4 + y^4 + z^4) = \psi(x)^4 + \psi(y)^4 + \psi(z)^4 = 3 \neq 4$. Therefore there are no $x, y, z \in \mathbb{Q}[\alpha]$ such that $x^4 + y^4 + z^4 = \alpha$.