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

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

Therefore

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

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 $d = \operatorname{disc}(\mathbb{A} \cap \mathbb{Q}[\sqrt{m}])$.

$m = -1$: $\sqrt{-1}$ 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 $r = \operatorname{lcm}(k,m)$ ($\operatorname{lcm}(k,m) = km/\gcd(k,m)$).

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.

(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.

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:

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

This is the required result.

28. (d) If $\alpha^3 = \alpha + 1$, then $a = -1$ and $b = -1$. By (c), $\operatorname{disc}(\alpha) = -27 - 4 = -31$, 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 $\operatorname{disc}(\alpha) = -27 + 4 = -23$ (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^2n^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. (a) TODO (Write Up)

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), $\bar{f} \mid \bar{f}_i\bar{f}_j$. However, $\bar{f} \nmid \bar{f}_i^{\,n}$ for any power of n (or else 3 would $\bar{f}_i^{\,n}$ which is not the case by (b)), so $\bar{f}_i\bar{f}_j \neq \bar{f}_i^{\,n}$ for any n. Therefore, since $\mathbb{Z}_3[x]$ is a UFD, $\bar{f}$ has an irreducible factor that does not divide $\bar{f}_i$ but does divide $\bar{f}_j$ for all $j \neq i$.

30. (d) The result of (c) is that $\bar{f}$ has at least 4 irreducible factors in $\mathbb{Z}_3[x]$. However, $\bar{f}$ 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 $\bar{f}$ 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. (TODO) Find two fields of degree 3 over $\mathbb{Q}$ whose composition has degree 6.

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.

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 $\operatorname{disc}(\theta) = \pm p^{(p-3)/2}$. Show the plus sign must hold.

By Exercise 23,

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

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

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

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

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

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

Proceeding in this way we have

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

Finally, we have

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

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 $d_1, \dots, d_k$ 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 $\leq i+j$. 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:

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

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

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 $\operatorname{disc}(\alpha) = -27m^2$ (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 $\operatorname{disc}(\alpha) = -\mathrm{N}(f'(\alpha))$. $f'(\alpha) = 3\alpha^2$ so $\alpha f'(\alpha) = 3m$ and $f'(\alpha) = 3m/\alpha$. Note $\mathrm{N}(\alpha) = m$ so $\mathrm{N}(\alpha^{-1}) = 1/m$. Therefore we have

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

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

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

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 $\mathrm{disc}(\alpha) = -27m^2$. By Exercise 40(a), $d_2^2\mathrm{disc}(R) = \mathrm{disc}(\alpha) = -27m^2 = -27h^2k^4$. We know $k \mid d_2$ so write $d_2 = jk$, thus $j^2k^2\mathrm{disc}(R) = -27h^2k^4$ and so $j^2\mathrm{disc}(R) = -27h^2k^2 = -27mh$. 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 $\mathrm{Tr}(\alpha^2) = \mathrm{Tr}(\alpha) = 0$, and so $3b/p \in \mathbb{Z}$. $p \neq 3$, therefore $p \mid b$. Therefore $(\alpha^2 + a\alpha)/p \in R$.

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

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:

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

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:

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

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.)

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

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 poylnomial

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

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

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

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):

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

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 $\mathrm{disc}(\alpha)$ 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

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

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 $\{1, \alpha, \ldots, \alpha_n\}$. As D is an integral domain each of these α_i are non-zero. Therefore $\alpha_{n+1} = 1$ so $\alpha^{-1} = \alpha_n$. Therefore every element in D has an inverse, and so it is 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.

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

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

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

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:

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

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

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

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 $\mathrm{disc}(\alpha_1 + \beta, \alpha_2, \dots, \alpha_n) = \mathrm{disc}(\alpha_1, \dots, \alpha_n)$.