Solutions to exercises from Marcus' "Number Fields"

Wojciech Wawrów

Marcus' book "Number Fields" is famous for its great amount of exercises (303 to be precise, many of them splitting into sub-exercises), among which are also proofs of many major theorems (such as Kronecker-Weber theorem) and details necessary in future proofs (In Marcus' own words, "[the] purpose of this is to make the proofs cleaner and easier to read, and to promote involvement on the part of the reader.").

The exercises are structured in such a way that even during the first reading of the book the reader is able to solve all the problems, possibly refering to earlier exercises. However, to a reader encountering algebraic number theory for the first time, and probably also many who have only little background, many of these problems can cause trouble, which may cause a lot of inconvenience, especially given that these exercises often cover a major part of an argument further in the text.

It is very likely that a reader would like to, at this point, look up the solution to the exercise in order to proceed. Having a single file containing solutions to the exercises may come in very handy (I, personally, would very much appreciate having access to one during the reading of the book). My hope is that this file will at some point help at least some people struggling with the exercises and will allow them to progress.

I try to keep the notation consistent with notation used throughout Marcus' book. The only difference is the use of $\subseteq, \subsetneq$ to denote containment (possibly nonstrict and strict, respectively), whereas Marcus only uses $\subset$.

This file will be regularly updated on my blog. All questions and feedback are warmly welcome there.

Chapter 1

1. First solution: Let $\alpha = a + bi, \beta = c + di$ with $a, b, c, d \in \mathbb{R}$. Then

$$\begin{aligned} N(\alpha\beta) &= N((ac - bd) + (ad + bc)i) = (ac - bd)^2 + (ad + bc)^2 \\ &= (ac)^2 - 2abcd + (bd)^2 + (ad)^2 + 2abcd + (bc)^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = (a^2 + b^2)(c^2 + d^2) = N(\alpha)N(\beta) \end{aligned}$$

Second solution: Let $\alpha = a + bi, \beta = c + di$ with $a, b, c, d \in \mathbb{R}$. Then

$$\begin{aligned} N(\alpha)N(\beta) &= (a + bi)(a - bi)(c + di)(c - di) \\ &= (a + bi)(c + di)(a - bi)(c - di) \\ &= ((ac - bd) + (ad + bc)i)((ac - bd) - (ad + bc)i) \\ &= N((ac - bd) + (ad + bc)i) = N(\alpha\beta) \end{aligned}$$

Now suppose $\alpha \mid \gamma$ in $\mathbb{Z}[i]$, so that $\gamma = \alpha\beta, \beta \in \mathbb{Z}[i]$. Then we have

$$N(\gamma) = N(\alpha\beta) = N(\alpha)N(\beta)$$

and $N(\beta) \in \mathbb{Z}$. Therefore, $N(\alpha) \mid N(\gamma)$.

2. Suppose first that α is a unit, say $\alpha\beta = 1, \beta \in \mathbb{Z}[i]$. Then $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$, so $N(\alpha) \mid 1$. Since $N(\alpha) = a^2 + b^2$ for $\alpha = a + bi$, $N(\alpha)$ is a nonnegative integer, so $N(\alpha) = 1$.

Conversely, suppose $N(\alpha) = 1$. Writing $\alpha = a + bi$ we have $1 = N(\alpha) = N(a + bi) = (a + bi)(a - bi) = \alpha(a - bi)$ with $a - bi \in \mathbb{Z}[i]$. Hence α is a unit.

To find all units $\alpha = a + bi \in \mathbb{Z}[i]$, by above we just need to find solutions to $N(\alpha) = 1$, i.e. $a^2 + b^2 = 1$. It is easy to see the only solutions are $(a, b) = (1, 0), (-1, 0), (0, 1), (0, -1)$, which correspond to units $\alpha = a + bi = 1, -1, i, -i$.

3. Suppose $\alpha = \beta\gamma, \beta, \gamma \in \mathbb{Z}[i]$. Then $N(\alpha) = N(\beta)N(\gamma)$. If $N(\alpha)$ is prime, then one of $N(\beta), N(\gamma)$ must be 1, hence one of β, γ must be a unit by exercise 2. This means that α is irreducible.

If $N(\alpha) = p^2, p \equiv 3 \pmod 4$ and $N(\alpha) = N(\beta)N(\gamma)$, then, since only positive divisors of p^2 are $1, p, p^2$, either one of $N(\beta), N(\gamma)$ is 1, and as before one of β, γ is a unit, or $N(\beta) = N(\gamma) = p$. However, letting $\beta = a + bi, a, b \in \mathbb{Z}$ this means $a^2 + b^2 = p \equiv 3 \pmod 4$. However, a^2 and b^2 necessarily are either 0 or 1 modulo 4, so $a^2 + b^2$ is either $0, 1$ or 2 modulo 4, hence this congruence is not possible. Hence one of β, γ is a unit, which means α is irreducible.

4. We compute the norm of $1 - i$ to be $N(1 - i) = 2$, which is prime, so by exercise 3 $1 - i$ is irreducible. Also, $(1 - i)^2 = -2i$, so that $i(1 - i)^2 = -2i^2 = 2$, hence we can take $u = i$ (which we know is a unit).

5. We can relate these two factorizations by writing $1 + 2i = i(2 - i), 1 - 2i = -i(2 + i)$. Since $i, -i$ are units, this means that the two factorizations of 5 only differ by unit factors, which is allowed in the statement of unique factorization.

6. The conditions of α not being zero nor a unit are equivalent to (using exercise 2) statement $N(\alpha) \neq 0, 1$. Hence we assume $N(\alpha) \geq 2$.

As the base case, we will take $N(\alpha) = 2$. By exercise 4, this means α is irreducible, hence it is (trivially) a product of irreducible elements.

Now assume the statement for elements of norm smaller than $N(\alpha)$. If α is irreducible, it is a product of irreducible elements. Otherwise, we can write $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathbb{Z}[i]$ not units. We have $N(\alpha) = N(\beta)N(\gamma)$ and, by exercise 2, both $N(\beta), N(\gamma)$ are greater than 1, hence both are smaller than $N(\alpha)$. Therefore both β, γ are products of irreducible elements, say $\beta = \pi_1 \dots \pi_r, \gamma = \pi_{r+1} \dots \pi_{r+s}$. Then $\alpha = \beta\gamma = \pi_1 \dots \pi_{r+s}$ is a product of irreducible elements.

7. Let I be an ideal in $\mathbb{Z}[i]$. If $I = \{0\}$, then $I = (0)$ is principal. Otherwise, there exist elements in $I - \{0\}$. Following the suggestion, consider an $\alpha \in I - \{0\}$ such that $N(\alpha)$ is the least possible. I then contains the principal ideal (α), and we want to prove these two ideals are equal.

Geometrically, considering elements of $\mathbb{Z}[i]$ as vectors on the complex plane, the vectors $\alpha, i\alpha$ are perpendicular and have the same length $|\alpha|$. Since each element in (α) is of the form $(m + ni)\alpha = m\alpha + ni\alpha$, (α) is a square lattice on the complex plane generated by these two vectors (see figure 1).

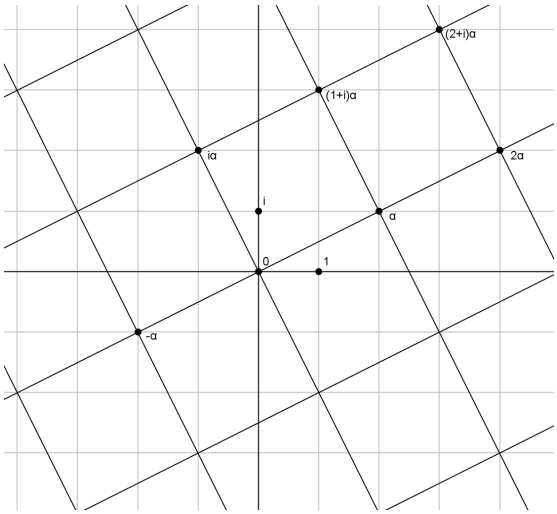

Figure 1: (α) on the complex plane

To say that I contains an element $\beta \notin (\alpha)$ means precisely that there is a point of I which isn't a vertex of the lattice, therefore it lies inside or on an edge of one of the squares, say it's a square with vertices $\gamma\alpha, (\gamma + 1)\alpha, (\gamma + i)\alpha, (\gamma + 1 + i)\alpha$. Divide this square into four smaller squares, then β lies in one of these (possibly on the boundary), say the one with vertex $\gamma\alpha$. Project β onto two closest sides of the square, say that the distances of the projections from $\gamma\alpha$ are x, y (see figure 2).

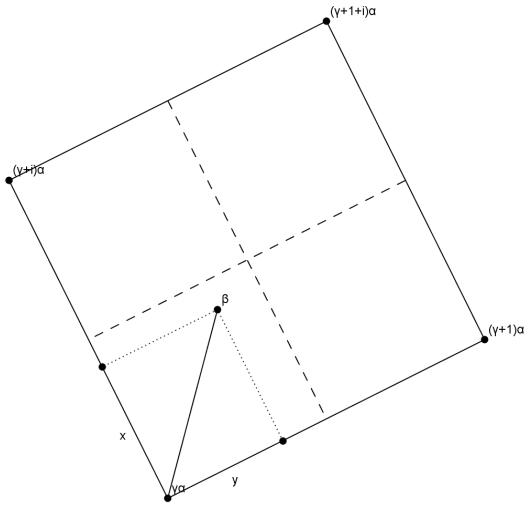

Figure 2: Bounding the distance between β and (α)

Note that $\beta - \gamma\alpha \in I - \{0\}$ and the length of this vector is the same as distance between $\gamma\alpha$ and β, which is by Pythagorean theorem

$$\sqrt{x^2+y^2} \leq \sqrt{\left(\frac{|\alpha|}{2}\right)^2 + \left(\frac{|\alpha|}{2}\right)^2} = \frac{|\alpha|}{\sqrt{2}} < |\alpha|,$$

so $|\beta - \gamma\alpha| < |\alpha|$. However, using Pythagorean theorem again, we find $|a + bi| = \sqrt{a^2+b^2} = \sqrt{N(a+bi)}$, so $\sqrt{N(\beta-\gamma\alpha)} < \sqrt{N(\alpha)}, N(\beta - \gamma\alpha) < N(\alpha)$. However, this contradicts the choice of α as the element of $I - \{0\}$ of minimal norm. Hence $I = (\alpha)$ is principal.

8.(a) If $p \equiv 1 \pmod 4$, the size of $\mathbb{Z}_p^*$, which is $p-1$, is divisible by 4. Since this group is cyclic, there is an element of order 4, say it's n. Then $n^2 \not\equiv 1 \pmod p$ while $(n^2)^2 = n^4 \equiv 1 \pmod p$. The polynomial $x^2 - 1 = (x-1)(x+1)$ has only $1, -1$ as its roots in $\mathbb{Z}_p$, hence, as $x = n^2$ satisfies $x^2 \equiv 1 \pmod p$ and is different from $1 \pmod p$, it must be $-1 \pmod p$, i.e. $n^2 \equiv -1 \pmod p$.

8.(b) Let n be as the one constructed in (a). Then $p \mid n^2 + 1$ in $\mathbb{Z}$, so $p \mid n^2 + 1 = (n+i)(n-i)$ in $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a UFD by exercise 7, if p were irreducible, this would imply $p \mid n + i$ or $p \mid n - i$. But any multiple of p can be written as $p(a+bi) = pa + pbi$, so it has imaginary part divisible by p. This isn't the case for $n \pm i$, so neither is divisible by p. This means that p cannot be irreducible.

8.(c) By (b) p isn't irreducible, so it can be written as $p = \alpha\beta$ with neither of two factors a unit. Then $p^2 = N(p) = N(\alpha)N(\beta)$. $N(\alpha), N(\beta)$ are both greater than 1, so both are smaller than p^2. Since p^2 has only $1, p, p^2$ as factors in $\mathbb{Z}$, we must have $N(\alpha) = p$. Letting $\alpha = a + bi$, this gives $p = a^2 + b^2, a, b \in \mathbb{Z}$.

9. The following is a complete characterization of irreducibles in $\mathbb{Z}[i]$:

Claim. *Every irreducible $\pi \in \mathbb{Z}[i]$ divides a unique positive prime $p \in \mathbb{Z}$. Moreover:*

- *if $p = 2$, then $\pi = u(1 - i)$ for some unit $u \in \mathbb{Z}[i]$,*
- *if $p \equiv 3 \pmod 4$, then $\pi = up$ for some unit $u \in \mathbb{Z}[i]$,*
- *if $p \equiv 1 \pmod 4$ and $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$ (by exercise 8 such a, b exist), then $\pi = u(a + bi)$ or $\pi = u(a - bi)$ for some unit $u \in \mathbb{Z}[i]$.*

Proof. We know $\pi \mid N(\pi)$ and $N(\pi)$ is a positive integer greater than 1, so it has a prime factorization in $\mathbb{Z}$, say $N(\pi) = p_1 \dots p_r$. Then, in $\mathbb{Z}[i]$, $\pi \mid p_1 \dots p_r$ so, as π is irreducible and $\mathbb{Z}[i]$ is a UFD, π divides one of p_i, as we claimed. We denote this p_i by p.

If $p = 2$, then $\pi \mid 2 = u(1 - i)^2$ where u is a unit (see exercise 4). Hence $\pi \mid 1 - i$. But two irreducible elements divide each other iff they are unit multiples of each other. Hence π is a unit times $1 - i$.

If $p \equiv 3 \pmod 4$, then $N(p) = p^2$, and by exercise 3 p is irreducible. As above, we deduce that π is a unit multiple of p.

If $p \equiv 1 \pmod 4, p = a^2 + b^2 = (a + bi)(a - bi)$, then $N(a \pm bi) = a^2 + b^2 = p$ is a prime, so by exercise 3 $a \pm bi$ are irreducible. Since $\pi \mid (a + bi)(a - bi)$, π divides, and hence is a unit multiple of, one of the factors. □

Since from exercise 2 we know exactly what the units are, we can also phrase this result as follows: the irreducibles in $\mathbb{Z}[i]$ are precisely $\pm 1 \pm i$, $\pm p$ and $\pm pi$ for prime $p \equiv 3 \pmod 4$ in $\mathbb{Z}$, and $\pm a + \pm bi, \pm b + \pm ai$ for $p = a^2 + b^2$ prime in $\mathbb{Z}$.

10. We have $a + b\omega = a - \frac{b}{2} + \frac{\sqrt{3}}{2}bi$, so $u = a - \frac{b}{2}, v = \frac{\sqrt{3}}{2}b$ and

$$u^2 + v^2 = a^2 - ab + \frac{b^2}{4} + \frac{3}{4}b^2 = a^2 - ab + b^2 = N(a + b\omega)$$

11. First solution: Write $\alpha = a + bi, \beta = c + di$. Now we can proceed in exactly as in either solution to exercise 1.

Second solution: Let $\alpha = a + b\omega, \beta = c + d\omega$. Noting $\omega^2 = -1 - \omega$, we have $\alpha\beta = (ac - bd) + (ad + bc - bd)\omega$. We therefore have

$$\begin{aligned} N(\alpha\beta) &= (ac - bd)^2 - (ac - bd)(ad + bc - bd) + (ad + bc - bd)^2 \\ N(\alpha)N(\beta) &= (a^2 - ab + b^2)(c^2 - cd + d^2). \end{aligned}$$

Expanding both right-hand sides we get the same expression. Therefore $N(\alpha\beta) = N(\alpha)N(\beta)$.

If now $\alpha \mid \gamma$ in $\mathbb{Z}[\omega]$, say $\gamma = \alpha\beta$, we get by above $N(\gamma) = N(\alpha\beta) = N(\alpha)N(\beta)$ with $N(\beta) \in \mathbb{Z}$, so $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.

12. We note

$$\begin{aligned}(a+b\omega)((a-b)-b\omega) &= a^2 - ab + (ab - b^2 - ab)\omega - b^2\omega^2 \\ &= a^2 - ab - b^2\omega + b^2 + b^2\omega = a^2 - ab + b^2 = N(a+b\omega).\end{aligned}$$

In particular, if $N(a+b\omega) = 1$, then $a+b\omega$ is a unit, as $(a+b\omega)((a-b)-b\omega) = 1$.

Conversely, suppose $\alpha \in \mathbb{Z}[\omega]$ is a unit. Then $\alpha \mid 1$, so $N(\alpha) \mid N(1) = 1$ in $\mathbb{Z}$, so $N(\alpha)$ is 1 or -1. However, by exercise 10, $N(\alpha)$ can be expressed as $u^2 + v^2$, which is positive, so $N(\alpha) = 1$.

To find all the units, we need to find all the solutions to $a^2 - ab + b^2 = N(a + b\omega) = 1$. Multiplying by 4 and rearranging, this is the same as $(2a-b)^2 + 3b^2 = 4$, or $c^2 + 3b^2 = 4$ for $c = 2a - b \in \mathbb{Z}$. This is easily seen to have six solutions $(c, b) = (\pm 2, 0), (\pm 1, \pm 1)$, which correspond to $(a, b) = (\pm 1, 0), (0, \pm 1), (1, 1), (-1, -1)$. So the units are precisely $1, -1, \omega, -\omega, 1 + \omega, -1 - \omega$.

13. Suppose $1 - \omega = \alpha\beta, \alpha, \beta \in \mathbb{Z}[\omega]$. Then $N(\alpha)N(\beta) = N(1 - \omega) = 3$, so, since $N(\alpha), N(\beta)$ are nonnegative, one of them must be 1, i.e. one of α, β is a unit. So $1 - \omega$ is irreducible.

We have

$$(1-\omega)^2 = 1 - 2\omega + \omega^2 = 1 - 2\omega - 1 - \omega = -3\omega$$

and $-\omega$ is a unit, let its inverse be u. Then $3 = u(1 - \omega)^2$.

14. Let I be an ideal in $\mathbb{Z}[\omega]$. If $I = \{0\}$, then $I = (0)$ is principal. Otherwise, there are elements in $I - \{0\}$, so we can choose one with minimal norm, call it α. Then $(\alpha) \subseteq I$ and we want to show equality.

Interpreting points as vectors, (α) is easily seen to be a lattice generated by vectors $\alpha, \omega\alpha$, which have the same length $|\alpha|$ and form an angle $60°$ (see figure 3), therefore they form a regular triangular lattice.

If I contains an element $\beta \notin (\alpha)$, then the corresponding points lies either inside or on a side of one of the lattices triangle. It is a simple geometric fact that in an equilateral triangle, distance from any point inside or on the edge of a triangle apart from vertex to any vertex is smaller than the side of the triangle.

Taking $\gamma\alpha, \gamma \in \mathbb{Z}[\omega]$ to be any of the vertices of the triangle β lies in, this means $|\beta - \gamma\alpha| < |\alpha|$. But using exercise 10, $N(\alpha) = |\alpha|^2$, hence $N(\beta - \gamma\alpha) < N(\alpha)$. But $\beta - \gamma\alpha \in I - \{0\}$, contradicting the choice of α. Hence $I = (\alpha)$ is principal.

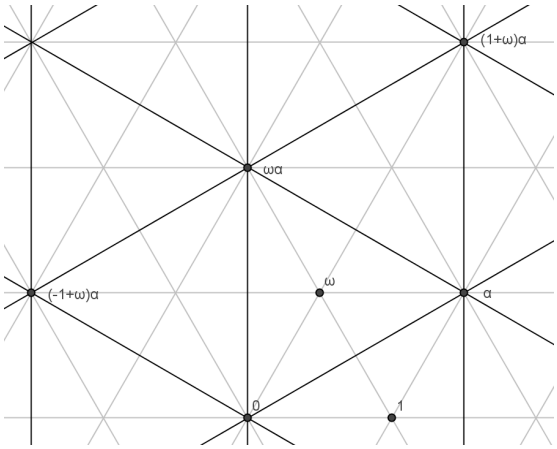

Figure 3: (α) on the complex plane

15.(a) We have $x^2+n^2=m^2$. m,n are relatively prime, so this is a primitive Pythagorean triple. Since out of x,n we know x is odd, we can write

$$x=r^2-s^2, n=2rs, m=r^2+s^2$$

with r,s relatatively prime and not both odd.

15.(b) We know r,s are relatively prime. If, for example, r,m had a common prime factor p, then it would also divide $m-r^2=s^2$, so it would divide both r,s, which is impossible. So r,s,m are pairwise relatively prime.

Since r,s are not both odd, and clearly not both even, m is odd and one of r,s is even, say r is (if s is even, we proceed analogously). Then $4r,s,m$ are also relatively prime, so $y^2=4r\cdot s\cdot m$ is a product of positive, relatively prime integers, so all of them must be a square, say $4r=d^2, s=b^2, m=c^2$. d is even, say $d=2a$, and then $r=a^2$.

15.(c) Equation $r^2+s^2=m$ now gives $a^4+b^4=c^2$. However, $c<c^2=m<m^2<m^2+n^2=w$, contradicting minimality of w. Therefore, $x^4+y^4=w^2$ has no solution in positive integers, hence neither does $x^4+y^4=z^4$.

16. Dividing equation (2) by $t-1$ gives us an equality of polynomials

$$(t-\omega)(t-\omega^2)\dots(t-\omega^{p-1})=\frac{t^p-1}{t-1}=t^{p-1}+\dots+t+1.$$

Setting $t=1$ clearly gives us

$$(1-\omega)(1-\omega^2)\dots(1-\omega^{p-1})=p.$$

17. Suppose π is a nonunit[1] common factor of $x + y\omega$ and $x + y\omega^k$, where $0 \leq k < p, k \neq 1$. Clearly $\pi \mid (x+y)(x+y\omega)\dots(x+y\omega^{p-1}) = z^p$ (see equation (1)).[2] Also, $\pi \mid (x + y\omega) - (x + y\omega^k) = y\omega(1 - \omega^{k-1})$. By assumption on k, $1-\omega^{k-1}$ is one of the factors in the product $(1-\omega)(1-\omega^2)\dots(1-\omega^{p-1})$, which by exercise 16 is equal to p. Hence $\pi \mid y\omega p$, so, as ω is a unit, $\pi \mid yp$.

On the other hand z^p and yp are relatively prime in $\mathbb{Z}$, since y, z are relatively prime and $p \nmid z$, so there are $m, n \in \mathbb{Z}$ such that $z^p m + ypn = 1$. It follows that $\pi \mid z^p m + ypn = 1$, which is a contradiction, since π is not a unit. Therefore, $x + y\omega, x + y\omega^k$ share no nonunit factors.

18. By equation (1) z^p can be expressed as a product of $x + y\omega$ and another factor, which by exercise 17 is relatively prime to it. By comparing the factorizations, every irreducible factor has exponent divisible by p on the z^p side, and since no irreducible factor appears in both $x + y\omega$ and the other factor, each factor appearing in $x + y\omega$ must appear in it a multiple of p times. Extracting the unit factors, it follows that $x + y\omega$ can be written as a unit times a pth power.

19. Suppose ideals $(x+y\omega), (x+y\omega^k)$ for some $0 \leq k < p, k \neq 1$ share a prime ideal factor P. This prime ideal clearly then also divides $(x+y)(x+y\omega)\dots(x+y\omega^{p-1}) = (z)^p$ (equation (1')), so, since it's prime, it must divide (z), hence $(z) \subseteq P$.

On the other hand, since P divides $(x + y\omega), (x + y\omega^k)$, it also divides, and hence contains, $(x + y\omega) + (x + y\omega^k) = (x + y\omega, x + y\omega^k) = (x + y\omega, x + y\omega^k - (x + y\omega)) = (x + y\omega, y(\omega - \omega^k))$, which in turn contains $(y(\omega - \omega^k)) = (y\omega(1 - \omega^{k-1})) = (y)(1 - \omega^{k-1})$. This last ideal divides, therefore contains, $(y)(1 - \omega)\dots(1 - \omega^{p-1}) = (y)(p) = (yp)$.

To sum up so far, we have that P contains (z) and (yp), and hence also $(z) + (yp)$. However, there are m, n such that $zm + ypn = 1$, since y, z are relatively prime and $p \nmid z$, so $1 \in (z) + (yp) \subseteq P$. This is a contradiction, since P is a proper ideal, so it cannot contain 1. It follows $(x + y\omega), (x + y\omega^k)$ share no prime ideal factor.

20. Equation (1') tells us $(z)^p$ is a product of $(x + y\omega)$ and another ideal factor. Exercise 19 tells us the two factors share no common prime ideal factors. Considering the prime ideal factorizations of both sides of equation (1'), we see that every prime ideal appears with exponent divisible by p. Since factors appearing in $(x+y\omega)$ don't appear in the other factor, they appear with exponent divisible by p, showing $(x + y\omega)$ is a pth power of an ideal.

[1] Clearly every unit divides both numbers, so we need to assume π is nonunit.

[2] Unless we assume π is irreducible, it is unclear to me how to deduce $\pi \mid z$. If we do assume that π is irreducible, we can simply replace z^p by z in what follows.

21. First we show that such a representation is possible. By definition, every element of $\mathbb{Q}[\omega]$ can be represented as

$$b_0 + b_1\omega + \cdots + b_n\omega^n$$

for some n and $b_i \in \mathbb{Q}$ for all i. By induction on n we will show this element can be expressed in the desired form. It is clear for $n \leq p-2$.

Assume $n \geq p-1$. Since $1 + \omega + \cdots + \omega^{p-1} = 0$, we can write

$$\begin{aligned} b_0 + b_1\omega + \cdots + b_n\omega^n &= b_0 + b_1\omega + \cdots + b_{n-1}\omega^{n-1} + b_n\omega^{n-p+1}\omega^{p-1} \\ &= b_0 + b_1\omega + \cdots + b_{n-1}\omega^{n-1} \\ &\quad + b_n\omega^{n-p+1}(-1 - \omega - \cdots - \omega^{p-2}) \\ &= c_0 + c_1\omega + \cdots + c_{n-1}\omega^{n-1}, \end{aligned}$$

where $c_i = b_i$ for $i < n-p+1$ and $c_i = b_i - b_n$ for $n-p+1 \leq i \leq n-1$. Using induction we now can express $c_0 + c_1\omega + \cdots + c_{n-1}\omega^{n-1}$ in the form $a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}$, so we are done.

To show uniqueness, suppose we have an equality

$$a_0 + a_1\omega + \cdots + a_{n-2}\omega^{p-2} = b_0 + b_1\omega + \cdots + b_{n-2}\omega^{p-2}.$$

Setting $c_i = a_i - b_i$, this implies that ω is a root of the polynomial

$$g(t) = c_0 + c_1 t + \cdots + c_{p-2}t^{p-2}.$$

Because ω is the root of $f(t)$ as defined in the exercise, if we show $f(t)$ is irreducible, it will follow that $f(t)$ is the minimal polynomial for ω over $\mathbb{Q}$, so $f(t) \mid g(t)$. This is only possible if $g(t) = 0$, since otherwise $g(t)$ has degree smaller than degree of $f(t)$, so divisibility cannot hold. Hence $c_i = 0, a_i = b_i$, thus the representation is unique.

To show $f(t)$ is irreducible, we will show $f(t+1)$ is irreducible (if $f(t)$ was reducible, so would be $f(t+1)$). Note that $f(t) = \frac{t^p-1}{t-1}$, so

$$f(t+1) = \frac{(t+1)^p - 1}{t} = \frac{\sum_{k=1}^{n} \binom{p}{k} t^k}{t} = \sum_{n=1}^{p} \binom{p}{n} t^{n-1}.$$

The leading coefficient is $\binom{p}{p} = 1$ and the constant coefficient is $\binom{p}{1} = p$, divisible by p but not p^2. All other coefficients are $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ for $1 < k < p$. The numerator is divisible by p, but denominator isn't, so $p \mid \binom{p}{k}$. Therefore Eisenstein's criterion directly implies $f(t+1)$ is irreducible.

22. Just as in exercise 21 we can show that any element in $\mathbb{Z}[\omega]$ can be expressed as $a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}$ with $a_i \in \mathbb{Z}$, and this exercise directly implies that this representation is unique.

Suppose $p \mid \alpha$, say $\alpha = p\beta$. Writing $\alpha = a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}, \beta = b_0 + b_1\omega + \cdots + b_{p-2}\omega^{p-2}$, this gives

$$\begin{aligned} a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2} &= p(b_0 + b_1\omega + \cdots + b_{n-2}\omega^{n-2}) \\ &= pb_0 + pb_1\omega + \cdots + pb_{n-2}\omega^{n-2}. \end{aligned}$$

By uniqueness of representation this means that $a_i = pb_i$ for all i, so $p \mid a_i$.

23. If $\beta \equiv \gamma \pmod{p}$, then $\beta - \gamma = \delta p$ for some $\delta \in \mathbb{Z}[\omega]$. Conjugating both sides, this gives $\overline{\beta} - \overline{\gamma} = \overline{\delta}p = \delta p$. From $\overline{\omega} = \omega^{p-1}$ it's quite clear $\delta \in \mathbb{Z}[\omega]$, so $\overline{\beta} \equiv \overline{\gamma} \pmod{p}$.

24. Using binomial theorem

$$(\beta + \gamma)^p - (\beta^p + \gamma^p) = \sum_{k=1}^{p-1} \binom{p}{k} \beta^k \gamma^{p-k}.$$

Because $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, numerator is divisible by p, while for $0 < k < p$ denominator isn't, so $p \mid \binom{p}{k}$. It clearly follows $(\beta + \gamma)^p \equiv \beta^p + \gamma^p \pmod{p}$.

We prove $(\beta_1 + \cdots + \beta_n)^p \equiv \beta_1^p + \cdots + \beta_n^p, n \geq 2$ by induction on n. The above argument gives it for $n = 2$. Assuming the result for given n, we then have

$$(\beta_1 + \cdots + \beta_n + \beta_{n+1})^p \equiv (\beta_1 + \cdots + \beta_n)^p + \beta_{n+1}^p \equiv \beta_1^p + \cdots + \beta_n^p + \beta_{n+1}^p,$$

the first equality being case $n = 2$. Hence the congruence holds for all $n \geq 2$.

25. Write $\alpha = a_0 + a_1\omega + \cdots + a_{n-2}\omega^{n-2}$ with all $a_i \in \mathbb{Z}$. We then have

$$\alpha^p \equiv a_0^p + a_1^p\omega^p + \cdots + a_{n-2}^p\omega^{p(n-2)} \equiv a_0^p + a_1^p + \cdots + a_{n-2}^p \pmod{p}$$

since all ω^i are pth roots of unity. Clearly $a_0^p + a_1^p + \cdots + a_{n-2}^p \in \mathbb{Z}$, so we are done.

26. By Kummer's lemma $\frac{u}{\overline{u}}$ is a power of ω, say $u = \omega^k\overline{u}$. Using exercise 25 choose $n \in \mathbb{Z}$ such that $\alpha^p \equiv n \pmod{p}$. We therefore have

$$x + y\omega \equiv u\alpha^p \equiv un \pmod{p}$$

Using exercise 23 we can conjugate both sides of the congruence, so, using $\overline{\omega} = \omega^{-1}$,

$$x + y\omega^{-1} \equiv \overline{u}n \pmod{p}.$$

We therefore have

$$x + y\omega \equiv un \equiv \omega^k\overline{u}n \equiv \omega^k(x + y\omega^{-1}) \pmod{p}.$$

27. Because the value of ω^k depends only on congruence class of $k \pmod p$, we may assume $1 \le k \le p$. Congruence from exercise 26 implies $x + y\omega \equiv x\omega^k + y\omega^{k-1} \pmod p, p \mid x + y\omega - y\omega^{k-1} - x\omega^k$. Let $a = x + y\omega - y\omega^{k-1} - x\omega^k$, so $p \mid a$.

Suppose first $k = p$. Then $a = y(\omega - \omega^{p-1}) = y(\omega - 1 - \omega - \cdots - \omega^{p-2})$, hence coefficients of all powers of ω are y, and this contradicts exercise 22, since $p \nmid y$.

Next suppose $k = p - 1$. We can now write $a = x + y\omega - y\omega^{p-2} - x\omega^{p-1} \equiv x + y\omega - y\omega p - 2 - x(-1 - \omega - \cdots - \omega^{p-2})$. Therefore coefficient of $p - 3$ is exactly x (recall $p \ge 5$), which is indivisible by p, again contradicting exercise 22.

Therefore $k \le p - 2$ and so $x + y\omega - y\omega^{k-1} - x\omega^k$ is already written in the form with all exponents between 0 and $p - 2$. Hence, by exercise 22, coefficient of ω^0 is divisible by p. But $p \nmid x$, so it must be the case that $k - 1 = 0$, otherwise there would be no more terms with ω^0. Therefore $k = 1$.

28. Since $k \equiv 1 \pmod p$ by exercise 27, $\omega^k = \omega$, so $x + y\omega \equiv (x + y\omega^{-1})\omega \equiv x\omega + y \pmod p$, so $p \mid (x - y) + (y - x)\omega$. By exercise 22, $p \mid x - y, x \equiv y \pmod p$.

29. Expanding the product, we get

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 + 3\omega^5 + 3\omega^6 + 3\omega^7 + \omega^8 + 3\omega^9 + 3\omega^{10} + 7\omega^{11}$$
$$+3\omega^{12} + 3\omega^{13} + \omega^{14} + 3\omega^{15} + 3\omega^{16} + 3\omega^{17} + \omega^{18} + \omega^{19} + \omega^{20} + \omega^{21} + \omega^{22}.$$

However, $1 + \omega + \cdots + \omega^{22} = 0$, so this product is equal to

$$2\omega^5 + 2\omega^6 + 2\omega^7 + 2\omega^9 + 2\omega^{10} + 6\omega^{11} + 2\omega^{12} + 2\omega^{13} + 2\omega^{15} + 2\omega^{16} + 2\omega^{17}$$

which is clearly divisible by 2. On the other hand, neither factor is divisible by 2 by exercise 22.

30. Suppose first ideals A, B are in the same ideal class, say $\alpha A = \beta B, \alpha, \beta \in R - \{0\}$. Define a map $f : A \to B$ by $f(a) = \frac{\alpha}{\beta}a$.[3] First we note this mapping is indeed into B: since $\alpha a \in \alpha A = \beta B$, so $\alpha a = \beta b$ for some $b \in B$, i.e. $f(a) = \frac{\alpha a}{\beta} = b \in B$.

If $f(a_1) = f(a_2)$, then $\frac{\alpha}{\beta}a_1 = \frac{\alpha}{\beta}a_2$, so $a_1 = a_2$ since $\frac{\alpha}{\beta} \ne 0$, so f is injective. For any $b \in B$, we have $\beta b \in \beta B = \alpha A$, so $\beta b = \alpha a$ for some a, so $b = \frac{\alpha}{\beta}a = f(a)$, so f is surjective. Therefore f is a bijection.

Verification that f is a homomorphism of R-modules is rather immediate: for $a_1, a_2 \in A$ we have

$$f(a_1 + a_2) = \frac{\alpha}{\beta}(a_1 + a_2) = \frac{\alpha}{\beta}a_1 + \frac{\alpha}{\beta}a_2 = f(a_1 + a_2)$$

[3]If we want to avoid having to go into the fraction field of R, we may define $f(a)$ to be an element of R such that $\alpha a = \beta f(a)$ and show such an element exists.

and for $r \in R, a \in A$ we have

$$f(ra) = \frac{\alpha}{\beta} ra = r\frac{\alpha}{\beta} a = rf(a).$$

For the converse, suppose $f : A \to B$ is an isomorphism of R-modules. For any $\alpha \in A$, set $\beta = f(\alpha)$. We claim $\beta A = \alpha B$. To see that, take any $a \in A$. Then

$$\beta a = af(\alpha) = f(a\alpha) = \alpha f(a) \in \alpha B,$$

so $\beta A \subseteq \alpha B$. Similarly we conclude $\alpha B \subseteq \beta A$ using isomorphism f^{-1} which maps β to α. Hence $\beta A = \alpha B$ and A, B are similar.

31. We need to assume $\alpha \neq 0$. Suppose αA is principal, say $\alpha A = (\beta)$. Then $\beta = \alpha a$ for some $a \in A$. We claim $A = (a)$. Indeed, clearly $(a) \subseteq A$. Conversely, take any $b \in A$. Then $\alpha b \in \alpha A = (\beta) = (\alpha a)$, so $\alpha b = \gamma \alpha a$ for some $\gamma \in R$. Then $b = \gamma a \in (a)$. Hence $A = (a)$ is principal.

To conclude principal ideals form an ideals class, we need to check any two principal ideals are similar and an ideal similar to a principal ideal is principal. For the former claim, take $(a), (b)$ to be two principal ideals. Then $b(a) = (ab) = a(b)$, so $(a), (b)$ are similar. For the latter claim, suppose (a) is a principal ideal similar to an ideal A, say $\alpha A = \beta(a) = (\beta a)$. This means αA is principal, so by above A is principal.

32. First suppose ideal classes form a group. This implies that for any ideal class C_1 there is an ideal class C_2 such that $C_1 C_2 = C_0$, the class of principal ideals (which is a class by exercise 31) (it is true in every group that $ax = b$ is solvable for any a, b, just take $a^{-1}b$). Take any ideal A and let C_1 be its ideal class. By above, for any ideal $B \in C_2$ we have $AB \in C_0$, i.e. AB is principal.

Conversely, suppose for any A there is B such that AB is principal. Associativity of ideal class multiplication follows directly from associativity of ideal multiplication. We verify C_0 is the identity element - consider product $C_0 C_1$. Take ideal $(1) \in C_0$ and any ideal $A \in C_1$. Then $(1)A = A \in C_1$. So $C_0 C_1 = C_1$. To verify every ideal class has an inverse, let C_1 be any class and A any of its elements. By assumption, there is an ideal B such that $AB \in C_0$. Letting C_2 be the ideal class of B, this means $C_1 C_2 = C_0$, i.e. C_2 is the inverse of C_1. Hence the ideal classes form a group.

Chapter 2

1.(a) Any quadratic extension of $\mathbb{Q}$ is an extension of the form $\mathbb{Q}[\alpha]$ for α a root of some quadratic polynomial $ax^2 + bx + c \in \mathbb{Q}[x]$. By multiplying this polynomial by a common multiple of denominators, we may assume $ax^2+bx+c \in \mathbb{Z}[x]$. Using the quadratic formula, we see that $\alpha = \frac{-b+\sqrt{m}}{2a}$ for $m = b^2-4ac \in \mathbb{Z}$. It is now clear than $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\sqrt{m}]$. Also, $\sqrt{m} = 2a\alpha + b$, so $\mathbb{Q}[\sqrt{m}] \subseteq \mathbb{Q}[\alpha]$. Therefore $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{m}]$.

1.(b) Consider first the case $n, m \neq 1$. Suppose $(a+b\sqrt{n})^2 = m$ with $a, b \in \mathbb{Q}$, so $a^2 + 2ab\sqrt{n} + b^2n = m, 2ab\sqrt{n} = m - a^2 - b^2n \in \mathbb{Q}$. Since $\sqrt{n}$ is irrational, so we must have $ab = 0$. If $b = 0$, then $m = a^2$, so, as a squarefree integer, $m = 1$, which we assumed isn't the case. If $a = 0$, then $b^2n = m$, so, by comparing the prime factorizations, we must have $m = n$. Therefore if $m \neq n$, then $\mathbb{Q}[\sqrt{m}]$ contains an element square of which is m, while $\mathbb{Q}[\sqrt{n}]$ doesn't, so these two fields are nonisomorphic, hence unequal.

Now suppose one of n, m is 1, say $n = 1, m \neq 1$. Then $\mathbb{Q}[\sqrt{n}] = \mathbb{Q}$ has no element square of which is m, so again $\mathbb{Q}[\sqrt{m}], \mathbb{Q}[\sqrt{n}]$ are nonisomorphic and unequal.

2. We have $1 + \sqrt{-3} \in I$, but $1 + \sqrt{-3} \notin (2)$, since every element of (2) has the form $2(a + b\sqrt{-3}) = 2a + 2b\sqrt{-3}, a, b \in \mathbb{Z}$, so $I \neq (2)$.

We have $2I = 2(2, 1 + \sqrt{-3}) = (4, 2 + 2\sqrt{-3})$, and $I^2 = (2, 1 + \sqrt{-3})(2, 1 + \sqrt{-3}) = (4, 4 + 2\sqrt{-3}, 4 + 2\sqrt{-3}, 4 + 2\sqrt{-3}) = (4, 2 + 2\sqrt{-3})$. Hence $2I = I^2$.

Now we shall show I is a prime ideal. It's easy to see I is the set of $a+b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ such that $a \equiv b \pmod 2$, so $1 \notin I$. Suppose $(a+b\sqrt{-3})(c+d\sqrt{-3}) \in I$, i.e. $ac - 3bd + (ad + bc)\sqrt{-3} \in I$, so that $ac - 3bd \equiv ad + bc \pmod 2$. If $a \not\equiv b, c \not\equiv d \pmod 2$, then exactly one of the products $ac, -3bd, ad, bc$ is odd, but then $ac - 3bd \equiv ad + bc \pmod 2$ cannot hold.

If ideals of $\mathbb{Z}[\sqrt{-3}]$ factored uniquely into prime ideals, then we could represent $(2) = P_1 \dots P_k$ for prime ideals P_i. But since $(2)I = 2I = I^2$, we would have

$$P_1 \dots P_k P = P^2,$$

which are two distinct factorizations of the same ideal, since $P_1 \dots P_k = (2) \neq I$.

Suppose J is a prime ideal containing (2). Then $(2) \subsetneq J$, because (2) is not prime, for example $1+\sqrt{-3} \notin (2)$, but $(1+\sqrt{-3})^2 \in (2)$. Let $a+b\sqrt{-3} \in J-(2)$. Then at least one of a, b is odd. If $a = 2k + 1, b = 2l$ for $k, l \in \mathbb{Z}$, then $1 = (a+b\sqrt{-3}) - 2(k+l\sqrt{-3}) \in J$, which is impossible for a prime ideal. Similarly, if $a = 2k, b = 2l + 1, k, l \in \mathbb{Z}$, then $\sqrt{-3} \in J$, so $-3 = \sqrt{-3}\sqrt{-3} \in J$, hence $1 = -3 + 2 \cdot 2 \in J$, which is again impossible. So $a = 2k + 1, b = 2l + 1, k, l \in \mathbb{Z}$ and we see $1 + \sqrt{-3} \in J$, from which we see J contains all $a + b\sqrt{-3}$ with a, b of the same parity, but no others, so $J = I$.

It follows that I is the only prime ideal which divides (2). Hence, if (2) is a product of prime ideals, it must be a power of I. However, $(2) \subsetneq I$, and we

easily see $I^2 = (4, 2+2\sqrt{-3}) \subsetneq (2)$, so $I^k \subsetneq (2)$ for $k \geq 2$. It follows that (2) is not a power of I, so it doesn't have a prime factorization.

3. If $2r$ is an integer, call it k, then $r = \frac{k}{2}$. Then $r^2 - ms^2 \in \mathbb{Z}$ iff $\frac{k^2}{4} - ms^2 \in \mathbb{Z}$ iff $k^2 - 4ms^2$ is an integer divisible by 4. We note that, because m is squarefree, $4ms^2 \in \mathbb{Z}$ iff $4s^2 \in \mathbb{Z}$ iff $2s \in \mathbb{Z}$. If this is the case, say $2s = l, s = \frac{l}{2}$. Hence we want to know for which k, l $\frac{k^2}{4} - m\frac{l^2}{4} \in \mathbb{Z}$, i.e. $4 \mid k^2 - ml^2$.

If $m \equiv 2, 3 \pmod 4$, then, by looking at possible parities of k, l, we find $4 \mid k^2 - ml^2$ iff k, l are both even, i.e. $r, s \in \mathbb{Z}$. Hence, in this case, $r + s\sqrt{m}$ is an algebraic integer iff $r, s \in \mathbb{Z}$.

If $m \equiv 1 \pmod 4$, we similarly find $4 \mid k^2 - ml^2$ iff k, l have the same parity. Therefore, $r + s\sqrt{m}$ is an algebraic integer iff it is of the form $\frac{k}{2} + \frac{l}{2}\sqrt{m}$ with $k, l \in \mathbb{Z}$. This clearly implies Corollary 2.

4. Let $d_0, \ldots, d_{n-1}$ be the degrees of $a_0, \ldots, a_{n-1}$, respectively. We claim that the products $a_0^{m_0} \ldots a_{n-1}^{m_{n-1}} \alpha^m$ for $0 \leq m_i < d_i, 0 \leq m < n$ generate the additive group of $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$.

Claim. *For any $k \geq 0$, α^k can be represented as*

$$\beta_0 + \beta_1\alpha + \cdots + \beta_{n-1}\alpha^{n-1}$$

with $\beta_i \in \mathbb{Z}[a_0, \ldots, a_{n-1}]$.

Proof. This is clear for $k \leq n-1$, then we proceed by induction. Suppose $\alpha^k = \beta_0 + \beta_1\alpha + \cdots + \beta_{n-1}\alpha^{n-1}$. Then

$$\begin{aligned}\alpha^{k+1} &= (\beta_0 + \beta_1\alpha + \cdots + \beta_{n-1}\alpha^{n-1})\alpha = \beta_0\alpha + \beta_1\alpha^2 + \cdots + \beta_{n-1}\alpha^n \\ &= -a_0\beta_{n-1} + (\beta_0 - a_1\beta_{n-1})\alpha + \cdots + (\beta_{n-2} - a_{n-1}\beta_{n-1})\alpha^{n-1}.\end{aligned}$$

It's clear new coefficients are in $\mathbb{Z}[a_0, \ldots, a_{n-1}]$, so this completes induction step. □

In entirely the same manner, using a monic polynomials from $\mathbb{Z}[x]$ roots of which are a_i we can show

Claim. *For any $k \geq 0$, a_i^k can be represented as*

$$b_0 + b_1 a_i + \cdots + b_{d_i-1} a_i^{d_i-1}$$

with $b_j \in \mathbb{Z}$.

Now take any element $\beta \in \mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$. It can be represented as integer linear combination of terms $a_0^{m_0} \ldots a_{n-1}^{m_{n-1}} \alpha^m$ (with possibly unbounded exponents). We first replace in each such term a power α^m with an expression as in the first claim. Expanding all products, we get a representation in which all exponents m are below n. Afterwards, we use the second claim to replace all powers of a_i, so that after expanding brackets we get integer linear combination

of products in which $m_i < d_i, m < n$. Thus we have given a finite set generating the additive group of $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$.

Clearly, $\alpha\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha] \subseteq \mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$. By Theorem 2, this implies α is an algebraic integer, since $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$ has a finitely generated additive group.

5. Every polynomial $f(x) \in \mathbb{Z}_p[x]$ can be written as $a_0 + a_1 x + \cdots + a_n x^n, a_i \in \mathbb{Z}_p$. By exercise 24, chapter 1 (the proof works just fine for polynomials) we have an equality in $\mathbb{Z}_p[x]$

$$(f(x))^p = (a_0 + a_1 x + \cdots + a_n x^n)^p = a_0^p + a_1^p x^p + \ldots a_n^p x^{np}.$$

Every element $a_i \in \mathbb{Z}_p$ can be written as $1 + \cdots + 1$ with finite number of terms. Hence

$$a_i^p = (1 + \cdots + 1)^p = 1^p + \cdots + 1^p = 1 + \cdots + 1 = a_i$$

thus

$$(f(x))^p = a_0^p + a_1^p x^p + \ldots a_n^p x^{np} = a_0 + a_1 x^p + \cdots + a_n (x^p)^n = f(x^p).$$

6. Suppose $g = f^2 h$ with $h \in \mathbb{K}[x]$. Differentiating both sides, we get

$$g' = (f^2 h)' = (f^2)' h + f^2 h' = 2 f f' h + f^2 h' = f(2 f' h + f h'),$$

so $f \mid g'$.

7. For $k \in \mathbb{Z}_m^*$ denote by σ_k the automorphism sending ω to ω^k. Then

$$(\sigma_k \circ \sigma_l)(\omega) = \sigma_k(\omega^l) = \omega^{kl} = \sigma_{kl}(\omega).$$

Since an automorphism is determined by its value at ω, this gives $\sigma_k \circ \sigma_l = \sigma_{kl}$, thus composition of automorphisms corresponds to multiplication modulo m.

8.(a) Clearly, from the definition of discriminant, $\mathrm{disc}(\omega)$ is a square of an element of $\mathbb{Q}[\omega]$. Because p is odd, the same is true for $p^{p-3} = (p^{(p-3)/2})^2$. Hence their ratio, $\frac{\mathrm{disc}(\omega)}{p^{p-3}} = \pm p$, is a square of an element of $\mathbb{Q}[\omega]$, which means precisely that $\sqrt{\pm p} \in \mathbb{Q}[\omega]$, with $+$ sign iff $p \equiv 1 \pmod 4$.

To find the square root in a cyclotomic field, we compute the determinant which appears in the definition of discriminant. For $m = 3$ it is

$$\begin{vmatrix} \omega & \omega^2 \\ \omega^2 & \omega \end{vmatrix} = \omega^2 - \omega.$$

We can check $(\omega^2 - \omega)^2 = \omega + \omega^2 - 2 = -3$. For $m = 5$, the matrix is

$$\begin{vmatrix} \omega & \omega^2 & \omega^3 & \omega^4 \\ \omega^2 & \omega^4 & \omega & \omega^3 \\ \omega^3 & \omega & \omega^4 & \omega^2 \\ \omega^4 & \omega^3 & \omega^2 & \omega \end{vmatrix} = \omega - \omega^2 - \omega^3 + \omega^4.$$

Indeed, we can check that this expression squared is 5, so it's a square root of 5.

8.(b) Letting ω be a primitive 8th root of unity, we have $(\omega + \omega^{-1})^2 = \omega^2 + \omega^{-2} + 2 = 2$, so $\sqrt{2} \in \mathbb{Q}[\omega]$.

8.(c) By exercise 1 every quadratic field is of the form $\mathbb{Q}[\sqrt{m}]$ for $m \in \mathbb{Z}$. Moreover, we can easily take m to be squarefree. We then have $d = \text{disc}(\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]) = m$ or $4m$, depending on whether $m \equiv 1 \pmod 4$ or $m \equiv 2, 3 \pmod 4$. Let ω be a primitive dth root of unity.

By taking prime factorization of $|m|$ and changing signs of primes $3 \pmod 4$, we can write $m = sap_1 \dots p_k$, where $s = \pm 1$, $a = 1$ or 2, and p_i is either an odd prime prime or a negative odd prime, whichever is $1 \pmod 4$, so that $p_1 \dots p_k \equiv 1 \pmod 4$. By (a), $\sqrt{p_i}$ is contained in $|p_i|$th cyclotomic field, and hence in $\mathbb{Q}[\omega]$.

If $m \equiv 1 \pmod 4$, then $a = s = \pm 1$, so that

$$\sqrt{m} = \sqrt{p_1 \dots p_k} = \sqrt{p_1} \dots \sqrt{p_k} \in \mathbb{Q}[\omega].$$

If $m \equiv 3 \pmod 4$, then $a = 1, s = -1$. Since then $4 \mid 4m = d$, this means that a primitive fourth root of unity, $\sqrt{-1}$, is in $\mathbb{Q}[\omega]$. Hence

$$\sqrt{m} = \sqrt{-p_1 \dots p_k} = \sqrt{-1}\sqrt{p_1} \dots \sqrt{p_k} \in \mathbb{Q}[\omega].$$

Finally, if $m \equiv 2 \pmod 4$, then $a = 2$ and $8 \mid 4m = d$, so that $\mathbb{Q}[\omega]$ contains the 8th root of unity and hence, by (b), $\sqrt{2}$. Also, as $4 \mid d$, it contains $\sqrt{s}$, regardless of whether it's 1 or -1. Hence

$$\sqrt{m} = \sqrt{2sp_1 \dots p_k} = \sqrt{2}\sqrt{s}\sqrt{p_1} \dots \sqrt{p_k} \in \mathbb{Q}[\omega].$$

It follows that in all cases $\mathbb{Q}[\sqrt{m}] \subseteq \mathbb{Q}[\omega]$.

9. Let $\theta = e^{2\pi i h/k}, \gcd(h, k) = 1$. Moreover, let $d = \gcd(m, k)$, so that $r = \frac{mk}{d}$. We want to show there is an integer solution u, v to

$$e^{2\pi id/mk} = e^{2\pi i/r} = \omega^u \theta^v = e^{2\pi i(u/m + vh/k)} = e^{2\pi i(uk + vhm)/mk},$$

hence it's enough to show that there is a solution to $d = uk + vhm$. But there is a solution, because $\gcd(k, hm) = \gcd(k, m) = d$ (recall $\gcd(k, h) = 1$).

10. Write $m = p_1^{e_1} \dots p_k^{e^k}$, such that all $e_i > 0$, and $r = p_1^{f_1} \dots p_k^{f_k} q_1^{g_1} \dots q_l^{g_l}$ with $f_i \geq e_i, g_j > 0, q_j \nmid m$. Clearly $r \geq m$. Suppose $r > m$. Then either $f_a > e_a$ for some a or $l > 0$.

If $f_i > e_i$, then we have

$$\varphi(r) = \prod_{i=1}^{k}(p_i-1)p_i^{f_i-1}\prod_{j=1}^{l}(q_j-1)q_j^{g_j-1} \geq \prod_{i=1}^{k}(p_i-1)p_i^{f_i-1}$$
$$\geq p_a\prod_{i=1}^{k}(p_i-1)p_i^{e_i-1} = p_a\varphi(m) > \varphi(m).$$

If $l > 0$, then

$$\varphi(r) = \prod_{i=1}^{k}(p_i-1)p_i^{f_i-1}\prod_{j=1}^{l}(q_j-1)q_j^{g_j-1} \geq (q_1-1)\prod_{i=1}^{k}(p_i-1)p_i^{e_i-1}$$
$$= (q_1-1)\varphi(m) > \varphi(m),$$

since $2 \mid m$, so $2 \neq q_1, q_1 - 1 > 1$.

In either case, we have $\varphi(r) > \varphi(m)$, so if $\varphi(r) \leq \varphi(m)$, $r = m$.

11.(a) Let $f = (x-\alpha_1)\dots(x-\alpha_n)$, so that $|\alpha_i| = 1$. The coefficient of x^r is, up to a sign, precisely the sum of all products of $n-r$ roots of f. All these products have absolute value 1, and there are precisely $\binom{n}{n-r} = \binom{n}{r}$ products in this sum. Hence this coefficient has absolute value at most $\binom{n}{r}$.

11.(b) Suppose α is an algebraic integer of degree n. Then its irreducible polynomial $f(x)$ over $\mathbb{Q}$, which has degree n, by Theorem 1 has coefficients in $\mathbb{Z}$. Let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ be the conjugates of α, which are precisely the roots of f. Then, by (a), coefficient of x^r in $f(x)$ has absolute value at most $\binom{n}{r}$. Since coefficients are integers, there are only finitely many possibilities for this coefficient.

It follows that there is a finite set of polynomials of degree n such that any algebraic integer α of degree n with all conjugates of absolute value 1 is a root of one of these polynomials. Since a polynomial of degree n has at most n roots, it follows there are only finitely many such algebraic integers.

11.(c) From (b) it follows that for any n, there are only finitely many algebraic integers of degree at most n which have all conjugates of absolute value 1. Taking α as in (b), from $\mathbb{Q}[\alpha^k] \subseteq \mathbb{Q}[\alpha]$ it follows that all α^k have degree at most n. We now show that all its conjugates have absolute value 1.

Claim. *Letting $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ be the conjugates of α, the conjugates of α^k are precisely α_i^k.*

Proof. First take any α_i. There is an embedding of $\mathbb{Q}[\alpha]$ into $\mathbb{C}$ which sends α to α_i. This embedding sends α^k to α_i^k, so α_i^k is a conjugate of α^k.

Now let β be any conjugate of α^k. There is an embedding of $\mathbb{Q}[\alpha^k]$ into $\mathbb{C}$ sending α^k to β. Extend this embedding to an embedding of $\mathbb{Q}[\alpha]$. α is then mapped to some α_i, and hence α^k is taken to α_i^k, so $\beta = \alpha_i^k$. Hence all conjugates of α^k are of the form α_i^k. □

Therefore, by what was said above, all powers α have degree at most n and all conjugates with absolute value 1, so they are all members of certain finite set. Therefore, some two powers of α are equal, say $\alpha^k = \alpha^l, k > l$. Then $\alpha^{k-l} = 1$, so α is a root of unity.

12.(a) Since $\overline{\omega} = \omega^{-1}$, complex conjugation is one of the automorphisms of $\mathbb{Q}[\omega]$. Because by Corollary 2 to Theorem 3 the Galois group of this field is isomorphic to $\mathbb{Z}_m^*$, this group is abelian. In particular, any automorphism commutes with complex conjugation. Therefore for any automorphism σ

$$|\sigma(u/\overline{u})| = |\sigma(u)/\sigma(\overline{u})| = \left|\sigma(u)/\overline{\sigma(u)}\right| = |\sigma(u)| \,/\, \left|\overline{\sigma(u)}\right| = |\sigma(u)| \,/\, |\sigma(u)| = 1,$$

so all conjugates of $u/\overline{u}$ have absolute 1. By exercise 11.(c) it follows that $u/\overline{u}$ is a root of unity. By Corollary 3 to Theorem 3 the only roots of unity in $\mathbb{Q}[\omega]$ are $2p$th roots of unity, i.e. ω^k and $-\omega^k$ for $k \in \mathbb{Z}$. Therefore $u/\overline{u} = \pm\omega^k$ for some k.

12.(b) By exercise 25, chapter 1 $u^p \equiv a \pmod{p}$ for some $a \in \mathbb{Z}$. By exercise 23, chapter 1 it follows $-\overline{u^p} \equiv -\overline{a} \equiv -a \pmod{p}$, so if $u^p \equiv -\overline{u^p} \pmod{p}, a \equiv -a \pmod{p}$, so, as p is odd, $u^p \equiv a \equiv 0 \pmod{p}$, so $p \mid u^p$, which is impossible, as u^p is a unit, but p isn't.

13. Suppose first $m \equiv 2, 3 \pmod 4$. Then, by Corollary 2 to Theorem 1, elements of $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$ are precisely $a + b\sqrt{m}, a, b \in \mathbb{Z}$. The norm of such an element is $a^2 - mb^2$. Recalling that an element is a unit iff its norm is ± 1 we see that for $m \neq -1$, if $b \neq 0$, $a^2 - mb^2 > 1$. So all the units have $b = 0, a^2 = \pm 1$. It follows that all the units are ± 1.

If $m \equiv 1 \pmod 4$, then elements of $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$ are $\frac{a+b\sqrt{m}}{2}, a, b \in \mathbb{Z}, a \equiv b \pmod 2$. Norm of this element is $\frac{a^2-mb^2}{4}$, which is ± 1 iff $a^2 - mb^2 = \pm 4$. If $m \neq -3$, then $m \leq -7$, so unless $b = 0$ we have $a^2 - mb^2 \geq 7 > 4$. So all the units have $b = 0, a^2 = 4$, hence they are ± 1.

The cases $m = -1, -3$ were dealt with, respectively, in exercises 2 and 12, chapter 1. There we have shown that there are respectively 4 and 6 units in these two rings.

14. $1 + \sqrt{2}$ is a unit, since $N(1 + \sqrt{2}) = 1^2 - 2 \cdot 1^2 = -1$. It is not a root of unity, since its absolute value is greater than 1. Therefore, no two numbers $(1 + \sqrt{2})^k$ for $k \in \mathbb{Z}$ are equal (otherwise $(1 + \sqrt{2})^{k-l} = 1$, contradicting $1 + \sqrt{2}$ not being a root of unity). All of them can be written as $a + b\sqrt{2}$, and they are all units, so have norm ± 1. Hence $a^2 - 2b^2 = \pm 1$, and this way we get infinitely many distinct such pairs a, b.

15.(a) An element $a + b\sqrt{-5}$ has norm 2 or 3 iff $a^2 + 5b^2 = 2$ or 3, respectively. We can't have $|b| \geq 1$ in this case, as otherwise $a^2 + 5b^2 \geq 5$, so $b = 0$. But $a^2 = 2, 3$ have no integer solutions. So $2, 3$ are not norms of any elements of $\mathbb{Z}[\sqrt{-5}]$.

15.(b) Elements $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ have norms, respectively, $4, 9, 6, 6$. If either of these were not irreducible, they would have a factor norm of which is a nontrivial factor of either $4, 9$ or 6, so it would be 2 or 3. By (a) there are no elements of such norm, so all factors are irreducible. Moreover, no element on the left hand side is a unit multiple of an element on the right hand side, since they have different norms. Therefore these are two really different factorizations of 6 in $\mathbb{Z}[\sqrt{-5}]$.

16. Suppose $\sqrt{3} \in \mathbb{Q}[\alpha]$. Then $\mathbb{Q}[\sqrt{3}] \subseteq \mathbb{Q}[\alpha]$. Every embedding of $\mathbb{Q}[\sqrt{3}]$ extends into the same number (namely, 2) of embeddings of $\mathbb{Q}[\alpha]$. Hence two embeddings map $\sqrt{3}$ to itself, and the other two map it to its additive inverse. It follows that $T(\sqrt{3}) = 0$. Similarly, $T(\alpha^2) = T(\sqrt{2}) = 0$. Also, $T(\alpha) = \alpha + i\alpha - \alpha - i\alpha = 0$ and $T(\alpha^3) = \alpha^3 + i\alpha^3 - \alpha^3 - i\alpha^3 = 0$. We can now get

$$\begin{aligned} 0 = T(\sqrt{3}) &= T(a + b\alpha + c\alpha^2 + d\alpha^3) \\ &= aT(1) + bT(\alpha) + cT(\alpha^2) + dT(\alpha^3) = 4a, \end{aligned}$$

so $a = 0$.

Consider $\frac{\sqrt{3}}{\alpha} = \sqrt[4]{\frac{9}{2}}$. The inner fraction is not a perfect square, hence it has four conjugates $\frac{\sqrt{3}}{\alpha}, i\frac{\sqrt{3}}{\alpha}, -\frac{\sqrt{3}}{\alpha}, -i\frac{\sqrt{3}}{\alpha}$ which sum to zero. Thus

$$0 = T\left(\frac{\sqrt{3}}{\alpha}\right) = T(b + c\alpha + d\alpha^2) = 4b,$$

so $b = 0$.

Now $\frac{\sqrt{3}}{\alpha^2} = \sqrt{\frac{3}{2}}$ has trace zero, just like $\sqrt{3}$ had. From there we get $c = 0$. Lastly, by considering $\frac{\sqrt{3}}{\alpha^3} = \sqrt[4]{\frac{9}{8}}$, we get $d = 0$. But at this point we get $\sqrt{3} = 0$, which is absurd. Therefore $\sqrt{3} \notin \mathbb{Q}[\alpha]$.

17. Let d be the degree of α. Let $\{\beta_1, \ldots, \beta_e\}$ for $e = \frac{n}{d}$ be the basis for L over $K[\alpha]$. Then

$$\beta_1, \alpha\beta_1, \ldots, \alpha^{d-1}\beta_1, \ldots, \beta_e, \alpha\beta_e, \ldots, \alpha^{d-1}\beta_e$$

is a basis for L over K. Writing minimal polynomial of α as $x^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0$, multiplication by α acts on the basis as follows:

$$\begin{aligned} \alpha \cdot \alpha^i\beta_j &= \alpha^{i+1}\beta_j \text{ for } i < d-1 \\ \alpha \cdot \alpha^{d-1}\beta_j &= \alpha^d\beta_j = -c_0\beta_j - c_1\alpha\beta_j - \cdots - c_{d-1}\alpha^{d-1}. \end{aligned}$$

From there, we easily see matrix of this transformation consists of e diagonal

blocks, all equal to

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{d-1} \end{bmatrix}.$$

Each block has trace $-c_{d-1}$ and determinant (seen by expanding along the first column) $(-1)^{n-1}(-c_0) = (-1)^n c_0$. However, by well-known formulas, these are equal, in notation of Theorem 4', to $t(\alpha), n(\alpha)$. Hence the whole transformation has trace and determinant, respectively, $et(\alpha) = \frac{n}{d}t(\alpha, n(\alpha)^e = (n(\alpha))^{n/d}$, which are $T(\alpha), N(\alpha)$ by Theorem 4'.

18. Suppose $\sigma_i\tau_j, \sigma_{i'}\tau_{j'}$ have the same restriction to M. Then they have the same restriction to L. Since on L $\tau_j, \tau_{j'}$ are identity, $\sigma_i\tau_j = \sigma_i, \sigma_{i'}\tau_{j'} = \sigma_{i'}$ on L. However, distinct σ_i are distinct on L by assumption, so $\sigma_i = \sigma_{i'}$ pointwise on L, hence their extensions to N are the same as well. Hence also $\tau_j = \tau_{j'}$. Thus $i = i', j = j'$.

19. Suppose $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$. Then we can construct the latter matrix from the former by adding c_0 times the first column, c_1 times the second column, ..., c_{n-1} times the nth column to the $n+1$th column, which won't change the determinant.

Take $f(x) = (x - a_1)\ldots(x - a_n)$. Then the last column is all zeroes, except for the last entry, which is $(a_{n+1} - a_1)\ldots(a_{n+1} - a_n)$. Expanding along the last column and using the $n \times n$ Vandermonde determinant, the $(n+1) \times (n+1)$ Vandermonde determinant is equal to

$$(a_{n+1} - a_1)\ldots(a_{n+1} - a_n) \prod_{1 \le r < s \le n} (a_s - a_r) = \prod_{1 \le r < s \le n+1} (a_s - a_r)$$

as we wanted.

20. Since $f(x)$ is irreducible, it has no multiple roots. Therefore $f(x) = (x - \alpha)g(x)$, where $g(x) = \prod_{\beta \neq \alpha} (x - \beta)$. Differentiating, we get $f'(x) = (x - \alpha)g'(x) + g(x)$. Setting $x = \alpha$ gives

$$f'(\alpha) = g(\alpha) = \prod_{\beta \neq \alpha} (\alpha - \beta).$$

21. Denote by $g(x)$ the minimal polynomial of α. Since α is a root of $f(x)$, $f(x)$ must be divisible by $g(x)$ in $\mathbb{Q}[x]$, and hence, by lemma in the proof of

Theorem 1, $f(x) = g(x)h(x)$ for some $h \in \mathbb{Z}[x]$. Differentiating and letting $x = \alpha$, we find

$$f'(\alpha) = g'(\alpha)h(\alpha) + g(\alpha)h'(\alpha) = g'(\alpha)h(\alpha).$$

Taking norms, this gives

$$N(f'(\alpha)) = N(g'(\alpha)h(\alpha)) = N(g'(\alpha))N(h(\alpha)) = \pm\text{disc}(\alpha)N(h(\alpha)),$$

where last equality follows from Theorem 8. Since $h \in \mathbb{Z}[x]$, $h(\alpha)$ is an algebraic integer, so $N(h(\alpha)) \in \mathbb{Z}$ by Corollary 2 to Theorem 4. For the same reason $N(f'(\alpha))$ is an integer, which is now clearly divisible by $\text{disc}(\alpha)$.

22. P and N are sums of $\frac{n!}{2}$ products each, and each of product has factors of the form $\sigma_i(\alpha_j)$, which are algebraic integers. Therefore, P and N are algebraic integers. Thus $P + N$ and PN are algebraic integers as well.

Let L be any normal extension of $\mathbb{Q}$ containing K. Let σ be any automorphism of L. Then for any i $\sigma\sigma_i$ is another embedding of K into $\mathbb{C}$. Indeed, sequence $\sigma\sigma_i$ is a permutation of σ_i (as we can recover σ_i from $\sigma\sigma_i$ using σ^{-1}), say it takes σ_i to $\sigma_{\pi(i)}$, where π is a permutation of $\{1, \ldots, n\}$.

Suppose first π is even. Take any even permutation τ of $\{1, \ldots, n\}$. We then have

$$\sigma(\sigma_{\tau(1)}(\alpha_1) + \cdots + \sigma_{\tau(n)}(\alpha_n)) = \sigma_{\pi\tau(1)}(\alpha_1) + \cdots + \sigma_{\pi\tau(n)}(\alpha_n),$$

and $\pi\tau$ is an even permutation. Therefore, every summand in the definition of P is taken to another such summand. We deduce that $\sigma(P) = P$. Similarly $\sigma(N) = N$, so we clearly have $\sigma(P + N) = P + N, \sigma(PN) = PN$.

Now suppose π is odd. Using a similar argument, we can show that $\sigma(P) = N$ and $\sigma(N) = P$. But then we still have $\sigma(P+N) = N+P = P+N, \sigma(PN) = NP = PN$.

This means that $P + N, PN$ are preserved by all automorphisms of L, so, as L is a normal extension, $P + N, PN \in \mathbb{Q}$. Since they are algebraic integers, they are integers.

To deduce $\text{disc}(\mathcal{A} \cap K) \equiv 0, 1 \pmod 4$, we note that taking α_i to be an integral basis of the integer ring, $d = \text{disc}(\mathcal{A} \cap K)$ (by definition). Since $P + N, PN$ are integers, $d = (P + N)^2 - 4PN \equiv (P + N)^2 \equiv 0, 1 \pmod 4$.

23.(a) The proofs of these results are almost the same as of original Theorems, except one replaces $\mathbb{Q}, K$ with K, L and remember that traces, norms and discriminants are relative.

Theorem 6

$$\text{disc}_K^L(\alpha_1, \ldots, \alpha_n) = |T_K^L(\alpha_i\alpha_j)|$$

Corollary. $\text{disc}_K^L(\alpha_1, \ldots, \alpha_n) \in K$*; and if all* α_i *are algebraic integers, then* $\text{disc}_K^L(\alpha_1, \ldots, \alpha_n) \in \mathbb{A} \cap K$.

Theorem 7 $\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n) = 0$ iff $\alpha_1, \ldots, \alpha_n$ are linearly dependent over K.

Theorem 8 Suppose $L = K[\alpha]$, and let $\alpha_1, \ldots, \alpha_n$ denote the conjugates of α over K. Then

$$\mathrm{disc}_K^L(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \le r < s \le n} (\alpha_r - \alpha_s)^2 = \pm N_K^L(f'(\alpha))$$

where f is the monic irreducible polynomial for α over K; the $+$ sign holds iff $n \equiv 0$ or $1 \pmod 4$.

23.(b) Let $\sigma_1, \ldots, \sigma_n$ be embeddings of L fixing K pointwise and $\tau_1, \ldots, \tau_m$ embeddings of M fixing L pointwise. Let N be a fixed extension of M normal over K. Define matrices A, B as in the suggestion.

We first evaluate $|A|^2$. A is block-diagonal, denote by $B_1, \ldots, B_n$ the blocks. Then

$$|A| = |A_1| \cdot \cdots \cdot |A_n|$$
$$|A|^2 = |A_1|^2 \cdot \cdots \cdot |A_n|^2.$$

We may suppose, without loss of generality, that σ_1 is the embedding of L which is identity. Then $A_1 = [\tau_h(\beta_k)]$, so, by definition, $|A_1|^2 = \mathrm{disc}_L^M(\beta_1, \ldots, \beta_m)$. Moreover, we have $A_i = \sigma_i(A_1)$, so

$$\begin{aligned} |A|^2 = |A_1|^2 \cdot \cdots \cdot |A_n|^2 &= \sigma_1(|A_1|^2) \ldots \sigma_n(|A_1|^2) \\ &= N_K^L(|A_1|^2) = N_K^L(\mathrm{disc}_L^M(\beta_1, \ldots, \beta_m). \end{aligned}$$

Next, we rearrange the rows and columns of matrix B. We need not to worry about the signs of determinants, as it will be ignored upon squaring.

We permute the rows and columns so that the row which originally was $m(i-1)+k$th is now $m(k-1)+i$th, and column which originally was $m(j-1)+h$ is not $m(h-1)+j$th. More visually, recalling that B is composed of a number of scaled identity matrices, we rearrange the matrix so that first diagonal entry of each of these matrices is now in the first diagonal block, second diagonal entry of each is now in the second diagonal block and so on, so that the rearranged matrix is a block-diagonal matrix, with m blocks, each of which is a matrix $C = [\sigma_i(\alpha_j)]$. Therefore

$$|B|^2 = (|C|^2)^m = (\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n))^m.$$

Finally, we look at matrix AB. It is a product of two matrices consisting of $m \times m$ matrices, so we can view it as a block matrix as well. Since A is block-diagonal, and blocks of B are scaled identity matrices, we can see that blocks of AB will be matrices $\sigma_i(\alpha_j)[\sigma_i\tau_h(\beta_k)] = [\sigma_i\tau_h(\alpha_j\beta_k)]$ (recall $\tau_h(\alpha_j) = \alpha_j$). It follows that

$$|AB|^2 = \mathrm{disc}_K^M(\alpha_1\beta_1, \ldots, \alpha_n\beta_m).$$

Because $|AB|^2 = (|A| \cdot |B|)^2 = |B|^2|A|^2$, desired equality follows.

23.(c) By Corollary 1 to Theorem 12, $T = RS$, so that, if $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ are integral bases for respectively R, S, then $\alpha_1\beta_1, \ldots, \alpha_m\beta_n$ is an integral basis for T. $\beta_1, \ldots, \beta_n$ is easily seen to be a basis for $M = KL$ over K (somewhat confusingly, here $\mathbb{Q}$ takes role of K from (b)), (b) gives us

$$\begin{aligned}\mathrm{disc}^{KL}(\alpha_1\beta_1, \ldots, \alpha_m\beta_n) &= (\mathrm{disc}^K(\alpha_1, \ldots, \alpha_m))^n N^K(\mathrm{disc}_K^{KL}(\beta_1, \ldots, \beta_n)) \\ &= (\mathrm{disc}R)^{[L:\mathbb{Q}]} N^K(\mathrm{disc}_K^{KL}(\beta_1, \ldots, \beta_n)).\end{aligned}$$

If we now show $\mathrm{disc}_K^{KL}(\beta_1, \ldots, \beta_n) = \mathrm{disc}^L(\beta_1, \ldots, \beta_n) = \mathrm{disc}L$, we will be done, since then

$$\begin{aligned}\mathrm{disc}T = \mathrm{disc}^{KL}(\alpha_1\beta_1, \ldots, \alpha_m\beta_n) &= (\mathrm{disc}R)^{[L:\mathbb{Q}]} N^K(\mathrm{disc}L) \\ &= (\mathrm{disc}R)^{[L:\mathbb{Q}]}(\mathrm{disc}L)^{[K:\mathbb{Q}]},\end{aligned}$$

since $\mathrm{disc}L \in \mathbb{Q}$.

Using lemma in the proof of Theorem 12, for any embedding τ of L there exists an embedding of KL which is identity on K and restricts to τ on L. Call this embedding τ'. Since $[KL : K] = [L : \mathbb{Q}]$, the embeddings of KL into $\mathbb{C}$ are precisely $\tau_1', \ldots, \tau_n'$ for all embeddings $\tau_1, \ldots, \tau_n$ of L. Hence

$$\mathrm{disc}_K^{KL}(\beta_1, \ldots, \beta_n) = |\tau_i'(\beta_j)| = |\tau_i(\beta_j)| = \mathrm{disc}^L(\beta_1, \ldots, \beta_n) = \mathrm{disc}L,$$

as we wanted.

24.(a) K is easily seen to be $\{0\} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ with $n-1$ copies of $\mathbb{Z}$, which is a free abelian group of rank $n-1$. $H \cap K$ is then its subgroup, so, by inductive assumption, it is a free abelian group of rank $\leq n-1$.

24.(b) Suppose $\pi(H)$ is infinite cyclic generated by $\pi(h) \neq 0$. We will first show that $\mathbb{Z}h$ and $H \cap K$ have trivial intersection. To see that, suppose $kh \in H \cap K$ for $k \in \mathbb{Z}$. In particular, $\pi(kh) = 0$, since K is kernel of π. However, $\pi(kh) = k\pi(h)$ and $\pi(h) \neq 0$, so $k = 0$ and kh is identity. Thus identity is the only element of $\mathbb{Z}h \cap (H \cap K)$.

Now we only need to show any $a \in H$ is a sum of an element of $\mathbb{Z}h$ and an element of $H \cap K$. Because $\pi(a) \in \pi(H)$ which is generated by $\pi(h)$, $\pi(a) = k\pi(h)$ for some $k \in \mathbb{Z}$. Then $\pi(a - kh) = \pi(a) - k\pi(h) = 0$, so $a - kh \in K$. But clearly $a - kh \in H$, so $a - kh \in H \cap K$. Hence a is sum of $kh \in \mathbb{Z}h$ and an element of $H \cap K$, as we wanted.

Hence H is a direct sum of $\mathbb{Z}h$ and $H \cap K$. In particular, it's a free abelian group of rank $\leq n$.

25. Let $g \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Multiplying by a common denominator, we get a polynomial $f \in \mathbb{Z}[x]$ which has α as a root, say

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0 = 0.$$

Multiplying this equality by a_n^{n-1} we get

$$a_n^n\alpha^n + a_{n-1}a_n^{n-1}\alpha^{n-1} + a_{n-2}a_n^{n-1}\alpha^{n-2} + \cdots + a_1a_n^{n-1}\alpha + a_0a_n^{n-1} = 0$$
$$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_{n-2}a_n(a_n\alpha)^{n-2} + \cdots + a_1a_n^{n-2}(a_n\alpha) + a_0a_n^{n-1} = 0,$$

so $a_n\alpha$ is a root of monic polynomial with coefficients in $\mathbb{Z}$, i.e. an algebraic integer.

To generalize this to any number of algebraic numbers, for each α_i choose m_i such that $m_i\alpha_i$ is an algebraic integer. Letting m be any nonzero common multiple of m_i, we see $m\alpha_i \in \mathbb{A}$ for each i.

26. In the proof of Theorem 11, the only property of the two sets $\{\beta_1, \ldots, \beta_n\}$ and $\{\gamma_1, \ldots, \gamma_n\}$ we have used is that they are two bases of the same additive group, namely additive group of R. Because of that, the proof of stated generalization can be rewritten verbatim.

27.(a) Let $g_1, \ldots, g_n$ and $h_1, \ldots, h_n$ be bases for, respectively, G and H. For any i the set $h_1, \ldots, h_n, g_i$ cannot be a basis of a subgroup of G it generates, since otherwise it would be a rank $n+1$ subgroup of a free abelian group of rank n, contradicting exercise 24. Hence there is a nontrivial relation between these elements, say

$$a_1h_1 + \cdots + a_nh_n + bg_i = 0,$$

where 0 denotes the group identity, $a_1, \ldots, a_n, b$ are integers, not all zero. If $b = 0$, then there would be a nontrivial relation between $h_1, \ldots, h_n$, which is impossible, since $h_1, \ldots, h_n$ form a basis. So $b \neq 0$. Taking additive inverse if necessary, this implies that for any g_i there is an integer $b_i > 0$ such that $b_ig_i \in H$.

From that we can deduce that any coset of H in G has a representative $a_1g_1 + \cdots + a_ng_n$ for which $0 \leq a_i < b_i$. Therefore H has at most $b_1 \ldots b_n$ cosets in G, so G/H is finite.

27.(b) [4] We can prove this by induction on n. This is rather clear for $n = 1$, so assume the result for $n-1$.

For any basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ of G look at all elements $h \in H$ which, when expressed in this basis, have positive coefficient of α_1. Of all possible bases and elements of H choose these which make this coefficient the least possible, say equal to d_1. We claim that every element of H has every coefficient with respect to this basis divisible by d_1. We first prove this for h: if h had a coefficient a of α_i not divisible by d_i, then we could write $a = qd_i + r, 0 < r < d_i$. But then if we replaced the basis $\alpha_1, \ldots, \alpha_n$ with $\alpha_1 + q\alpha_i, \ldots, \alpha_n$ (easily seen to be another basis), then we easily see the coefficient of α_i would be r, so rearranging the basis would contradict the choice of d_1. Hence $\beta_1 = \frac{\alpha_1}{d_1} \in G$.

[4] This solution doesn't use the structure theorem; I don't know a proof which does.

Similarly, we establish that for every $h' \in H$, the coefficient of α_1 is divisible by d_1, say it's qd_1. Then $h' - qh$ is contained in the group G_1 generated by $\alpha_2, \ldots, \alpha_n$. Let $H_1 = H \cap G_1$. Also, let H_0 be the group generated by α_1. As in the solution of exercise 24.(b), it follows that $H = H_0 \oplus H_1$. By induction, there is a basis $\beta_2, \ldots, \beta_n$ for G_1 and integers $d_2, \ldots, d_n$ such that $d_2\beta_2, \ldots, d_n\beta_n$ are a basis for H_1. Then $\beta_1, \ldots, \beta_n$ and $d_1, \ldots, d_n$ work for G and H.

27.(c) Choose generating set $\{\beta_1, \ldots, \beta_n\}$ for G and $d_1, \ldots, d_n$ as in (b). Then $d_1\beta_1, \ldots, d_n\beta_n$ is a generating set for H. Elements $a_1\beta_1 + \cdots + a_n\beta_n$ for $0 \leq a_i < d_i$ are easily seen to be a complete set of representatives for cosets of H in G, so that $|G/H| = d_1 \ldots d_n$. On the other hand,

$$\begin{aligned}\mathrm{disc}(H) &= \mathrm{disc}(d_1\beta_1, \ldots, d_n\beta_n) = |\sigma_i(d_j\beta_j)|^2 = d_1^2 \ldots d_n^2 |\sigma_i(\beta_j)|^2 \\ &= (d_1 \ldots d_n)^2 |\sigma_i(\beta_j)| = |G/H|^2 \mathrm{disc}(\beta_1, \ldots, \beta_n) = |G/H|\mathrm{disc}(G).\end{aligned}$$

27.(d) Solution using (c): If $\alpha_1, \ldots, \alpha_n$ are linearly dependent, then they aren't an integral basis and, by Theorem 7, $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0 \neq \mathrm{disc}(R)$.

Suppose $\alpha_1, \ldots, \alpha_n$ are linearly independent. Let G be the additive group generated by them. Then both G and R (viewed as an additive group) have rank n and $G \subseteq H$. By (c), $\mathrm{disc}(R) = |R/G|^2\mathrm{disc}(G)$. Then $\mathrm{disc}(R) = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ iff $\mathrm{disc}(R) = \mathrm{disc}(G)$ iff $|R/G|^2 = 1$ iff $R = G$ iff $\alpha_1, \ldots, \alpha_n$ are an integral basis for R.

Solution not using (c): Express each α_i using some fixed integral basis $\gamma_1, \ldots, \gamma_n$ for R and collect the coefficients in a matrix M, so that

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}.$$

As in the proof of Theorem 11, this gives

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = |M|^2\mathrm{disc}(\gamma_1, \ldots, \gamma_n) = |M|^2\mathrm{disc}(R).$$

Therefore $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(R)$ iff $|M| = \pm 1$ iff M is invertible iff γ_j can be expressed as integer linear combination of α_i iff $\alpha_1, \ldots, \alpha_n$ form an integral basis for R.

27.(e) Solution not using Theorem 9: Since the discriminant is nonzero, $\alpha_1, \ldots, \alpha_n$ are linearly independent. Let G be the additive group generated by $\alpha_1, \ldots, \alpha_n$. Then $\mathrm{disc}(G) = |R/G|^2\mathrm{disc}(R)$ by (c). But since $\mathrm{disc}(G)$ is squarefree, $|R/G| = 1$, so $R = G$ and $\alpha_1, \ldots, \alpha_n$ is an integral basis for R.

Solution using Theorem 9: Take $\alpha \in R$. By Theorem 9, it can be written as

$$\alpha = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d},$$

where $m_j \in \mathbb{Z}, d \mid m_j^2$. But since d is squarefree, this implies $d \mid m_j$, so that

$$\alpha = \frac{m_1}{d}\alpha_1 + \cdots + \frac{m_n}{d}\alpha_n \tag{1}$$

is an integer linear combination of $\alpha_1, \ldots, \alpha_n$. So $\alpha_1, \ldots, \alpha_n$ is an integral basis for R.

28.(a) We have $xf'(x) = x(3x^2 + a) = 3x^3 + ax$, so, given that $\alpha^3 = -a\alpha - b$, $\alpha f'(\alpha) = 3\alpha^3 + a\alpha = -2a\alpha - 3b$, hence $f'(\alpha) = \frac{-(2a\alpha+3b)}{\alpha}$.

28.(b) For $x = 2a\alpha+3b$ we have $\frac{x-3b}{2a} = \alpha$, so, by choice of α, $2a\alpha+3b$ is a root of $\left(\frac{x-3b}{2a}\right)^3 + a\left(\frac{x-3b}{2a}\right) + b$. The norm of $2a\alpha+3b$ is now negative of the ratio of the coefficient of x^0 and x^3 in this polynomial. Expanding, we find these coefficients are $-\frac{27b^3}{8a^3} - \frac{3b}{2} + b$ and $\frac{1}{8a^3}$, their ratio is $-27b^3 - 12ba^3 + 8ba^3 = -27b^3 - 4ba^3$, so $N(2a\alpha + 3b) = 27b^3 + 4ba^3$.

28.(c) $N(-1) = -1$ and $N(\alpha) = -b$, so, by Theorem 8,

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

28.(d) If $\alpha^3 = \alpha + 1$, then α is a root of polynomial $x^3 - x - 1$, which is irreducible (as it's a cubic with no rational root). Here $a = b = -1$, so, by (c), $\operatorname{disc}(\alpha) = -23$, which is squarefree, so by exercise 27e $1, \alpha, \alpha^2$ forms an integral basis for $R = \mathbb{A} \cap \mathbb{Q}[\alpha]$.

If $\alpha^3 + \alpha = 1$, then α is a root of irreducible polynomial $x^3 + x - 1$. $a = 1, b = -1$, so by (c) $\operatorname{disc}(\alpha) = -31$, again squarefree, so by 27e $1, \alpha, \alpha^2$ is an integral basis for $\mathbb{A} \cap \mathbb{Q}[\alpha]$.

29.(a) We have $\operatorname{disc}(\mathbb{A} \cap \mathbb{Q}[\sqrt{n}]) = n, \operatorname{disc}(\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]) = m$. These two values are relatively prime, so, since $K = \mathbb{Q}[\sqrt{n}]\mathbb{Q}[\sqrt{m}]$, by Corollary 1 to Theorem 12 we have $\mathbb{A} \cap K = (\mathbb{A} \cap \mathbb{Q}[\sqrt{n}])(\mathbb{A} \cap \mathbb{Q}[\sqrt{m}])$. The last two rings have integral bases $1, \frac{1+\sqrt{n}}{2}$ and $1, \frac{1+\sqrt{m}}{2}$ respectively, so

$$1, \frac{1 + \sqrt{n}}{2}, \frac{1 + \sqrt{m}}{2}, \left(\frac{1 + \sqrt{n}}{2}\right)\left(\frac{1 + \sqrt{m}}{2}\right)$$

is an integral basis for $\mathbb{A} \cap K$.

29.(b) This time we have $\text{disc}(\mathbb{A} \cap \mathbb{Q}[\sqrt{n}]) = n, \text{disc}(\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]) = 4m$, and these two values are also relatively prime, since $2 \nmid n$. So again integer ring is a product of integer rings, which means

$$1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \left(\frac{1+\sqrt{m}}{2}\right)\sqrt{n}$$

is an integral basis for $\mathbb{A} \cap K$.

30.(a) Suppose $g(\alpha)$ is divisible by 3 in $\mathbb{Z}[\alpha]$. Then $g(\alpha) = 3h(\alpha)$ for some $h \in \mathbb{Z}[x]$, so α is a root of $g - 3h$. Hence $f \mid g - 3h$. Reducing modulo 3, $\overline{f}$ divides $\overline{g - 3h} = \overline{g}$.

Conversely, if $\overline{f}$ divides $\overline{g}$ in $\mathbb{Z}_3[x]$, then $\overline{fk} = \overline{g}$, so $fk - g = 3h$ for some $h \in \mathbb{Z}$. Plugging in $x = \alpha$, this gives $g(\alpha) = -3h(\alpha)$, so $g(\alpha)$ is divisible by 3.

30.(b) For any $i \neq j$, either one of α_i, α_j has a factor $1 + \sqrt{7}$ and the other has $1 - \sqrt{7}$, or one has a factor $1 + \sqrt{10}$ and the other has $1 - \sqrt{10}$. In either case, $\alpha_i\alpha_j$ is divisible by $(1+\sqrt{7})(1-\sqrt{7}) = -6$ or by $(1+\sqrt{10})(1-\sqrt{10}) = -9$. In either case, $\alpha_i\alpha_j$ is divisible by 3.

For any positive integer n we can write

$$\begin{aligned}\alpha_1^n &= ((1+\sqrt{7})(1+\sqrt{10}))^n = (1+\sqrt{7})^n(1+\sqrt{10})^n \\ &= (a_n + b_n\sqrt{7})(c_n + d_n\sqrt{10}).\end{aligned}$$

We can then check that $\alpha_i^n = (a_n \pm b_n\sqrt{7})(c_n \pm d_n\sqrt{10})$ for suitable choice of signs, so that α_i^n are the conjugates of α_1^n. Therefore

$$T(\alpha_1^n) = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n.$$

To see why this is congruent to $(\alpha_1+\alpha_2+\alpha_3+\alpha_4)^n$ modulo 3, consider expanding this last product. We will then get four terms $\alpha_1^n, \alpha_2^n, \alpha_3^n, \alpha_4^n$, and all other terms will involve a product of some α_i and α_j for $i \neq j$. By what was said above, 3 divides $\alpha_i\alpha_j$, so 3 divides all other terms. So the difference

$$(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n - T(\alpha_1^n)$$

is divisible by 3, establishing congruence

$$T(\alpha_1^n) \equiv (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n \equiv 4^n \equiv 1 \pmod 3$$

(the second congruence is in fact an equality). Hence $\frac{T(\alpha_1^n)-1}{3}$ is an algebraic integer. But it's also in $\mathbb{Q}$, so $T(\alpha_1^n) \equiv 1 \pmod 3$ in $\mathbb{Z}$. In particular, $\frac{\alpha_1^n}{3}$ has noninteger trace, so isn't algebraic integer. Hence α_1^n is not divisible by 3. Similar argument goes for other α_i^n.

30.(c) By (b) $f_i(\alpha)f_j(\alpha) = \alpha_i\alpha_j$ is divisible by 3, so by (a) $\overline{f} \mid \overline{f_if_j}$. On the other hand, by (b) $f_i(\alpha)^n = \alpha_i^n$ is not divisible by 3, so again by (a) $\overline{f} \nmid \overline{f_i}^n$.

If all irreducible factors of $\overline{f}$ divided $\overline{f_i}$, then $\overline{f}$ would divide $\overline{f_i}^n$, where n is the greatest exponent of irreducible factor of $\overline{f}$, but we know this isn't the case. So some irreducible $\overline{g}$ divides $\overline{f}$ but not $\overline{f_i}$. Since $\overline{f} \mid \overline{f_if_j}, \overline{g} \mid \overline{f_if_j}$ hence $\overline{g} \mid \overline{f_j}$ for $j \neq i$. We use unique factorization in the last step, since we use that $\overline{g}$ is a prime element.

30.(d) Let $\overline{g_1}, \overline{g_2}, \overline{g_3}, \overline{g_4}$ be distinct monic irreducible factors of $\overline{f}$. Then (again we have to use unique factorization) $\overline{g_1g_2g_3g_4}$ divides $\overline{f}$. Since $\overline{f}$ has degree at most 4, and $\overline{g_i}$ have degree at most 1, all of $\overline{g_i}$ have degree 1. But there are only three monic polynomials in $\mathbb{Z}_3[x]$. This contradicts the fact that $\overline{g_i}$ are distinct.

31. Let $\alpha = \frac{\sqrt{3}+\sqrt{7}}{2}$. Then $\beta = \alpha^2 = \frac{10+2\sqrt{21}}{4} = \frac{5+\sqrt{21}}{2}$. Since $21 \equiv 1 \pmod 4$ and $5 \equiv 1 \pmod 2$, β is an algebraic integer, say it's a root of $x^2+ax+b, a, b \in \mathbb{Z}$. Then α is a root of monic polynomial $x^4+ax^2+b \in \mathbb{Z}$, so is an algebraic integer.

32. Let $K = \mathbb{Q}[\sqrt[3]{2}]$ and $L = \mathbb{Q}[\omega\sqrt[3]{2}]$, where ω is a complex cube root of unity. Both K, L have degree 3, since they are extensions by a root of $x^3 - 2$. Then $KL = \mathbb{Q}[\omega, \sqrt[3]{2}]$. Since ω is a root of $x^2 + x + 1$, $[KL : K] \leq 2$. At the same time, $KL \not\subseteq \mathbb{R}$, while $K \subseteq \mathbb{R}$, so $K \subsetneq KL, [KL : K] > 1$. Thus $[KL : K] = 2$ so $[KL : \mathbb{Q}] = [KL : K][K : \mathbb{Q}] = 6$.

33. We can match conjugates of ω into pairs $\omega^i, \overline{\omega^i} = \omega^{m-i}$ for all i with $\gcd(i, m) = 1$. Because $m > 2$, ± 1 are not conjugates of ω, so all these pairs have two distinct elements. Product of elements of a pair is 1, so $N(\omega)$, which is the product of all conjugates of ω, is 1.

34.(a) Since k, m are relatively prime, there is $h \in \mathbb{Z}$ such that $hk \equiv 1 \pmod m$, so $\omega^{hk} = \omega$, so

$$\frac{\omega - 1}{\omega^k - 1} = \frac{\omega^{hk} - 1}{\omega^k - 1} = 1 + \omega^k + \cdots + \omega^{(h-1)k} \in \mathbb{Z}[\omega].$$

But then

$$\frac{\omega - 1}{\omega^k - 1}(1 + \omega + \cdots + \omega^{k-1}) = \frac{\omega - 1}{\omega^k - 1} \cdot \frac{\omega^k - 1}{\omega - 1} = 1,$$

implying $1 + \omega + \cdots + \omega^{k-1}$ is a unit.

34.(b) Lemma 2, Theorem 10 states that

$$p = \prod_k (1 - \omega^k),$$

product over $1 \leq k \leq p^r$ $\gcd(k, p^r) = 1$, i.e. $p \nmid k$. (a) shows that for these k we have $1 - \omega^k = u_k(1 - \omega)$ for certain unit $u_k \in \mathbb{Z}[\omega]$. Thus

$$p = \prod_k (1 - \omega^k) = \prod_k u_k(1 - \omega) = u(1 - \omega)^n$$

with $u = \prod_k u_k$ a unit and n the number of terms in the product, i.e. $\varphi(p^r)$.

35.(a) We have $\theta\omega = \omega^2 + 1$, so ω is a root of $x^2 - \theta x + 1$, which lies in $\mathbb{Q}[\theta]$.

35.(b) From (a) it follows that $\mathbb{Q}[\omega]$ has degree at most 2 over $\mathbb{Q}[\theta]$. However, $\omega \notin \mathbb{R}$ while $\mathbb{Q}[\theta] \subseteq \mathbb{R}$, so $\mathbb{Q}[\omega] \neq \mathbb{Q}[\theta]$, to $\mathbb{Q}[\omega]$ has degree 2.

We clearly have $\mathbb{Q}[\omega] \supsetneq \mathbb{R} \cap \mathbb{Q}[\omega] \supseteq \mathbb{Q}[\theta]$. Moreover,

$$[\mathbb{R} \cap \mathbb{Q}[\omega] : \mathbb{Q}[\theta]] = \frac{[\mathbb{Q}[\omega] : \mathbb{Q}[\theta]]}{[\mathbb{Q}[\omega] : \mathbb{R} \cap \mathbb{Q}[\omega]]} < \frac{2}{1} = 2,$$

so $\mathbb{R} \cap \mathbb{Q}[\omega] = \mathbb{Q}[\theta]$.

35.(c) Since $\sigma(\omega) = \omega^{-1} = \overline{\omega}$, σ is just the restriction of complex conjugation to $\mathbb{Q}[\omega]$. Hence $\alpha \in \mathbb{Q}[\omega]$ is fixed by σ iff $\alpha \in \mathbb{R}$ iff, by (b), $\alpha \in \mathbb{Q}[\theta]$.

35.(d) We have

$$\mathbb{A} \cap \mathbb{Q}[\theta] = \mathbb{A} \cap \mathbb{Q}[\omega] \cap \mathbb{R} = \mathbb{Z}[\omega] \cap \mathbb{R}$$

by Corollary 2 to Theorem 12.

35.(e) Since ω is an algebraic integer of degree $\varphi(m) = 2n$, $\{1, \omega, \ldots, \omega^{2n-1}\}$ is an integral basis for $\mathbb{Z}[\omega]$. Since $\omega^{-(n-1)}$ is a unit in $\mathbb{Z}[\omega]$,

$$\begin{aligned}\omega^{-(n-1)}\{1, \omega, \ldots, \omega^{2n-1}\} &= \{\omega^{-(n-1)}, \omega^{-(n-2)}, \ldots, \omega^{n-1}, \omega^n\} \\ &= \{1, \omega, \omega^{-1}, \ldots, \omega^{n-1}, \omega^{-(n-1)}, \omega^n\}\end{aligned}$$

is another integral basis.

To see $\{1, \omega, \theta, \ldots\}$ generates the same group, we need to show the transition matrix is invertible over $\mathbb{Z}$, i.e. has determinant ± 1. But it's easy to see θ^k only involves $\theta^{\pm l}$ for $l = 0, \ldots, k$ with ω^{-k} having coefficient 1 and $\theta^k\omega$ only additionally involves ω^{k+1} with coefficient 1. But this means that this matrix is upper triangular with ones on its diagonal, so it has determinant 1. So $\{1, \omega, \theta, \ldots\}$ is an integral basis.

35.(f) According to (e), every element of $\mathbb{Z}[\omega]$ can be uniquely written as

$$a_1 + a_2\omega + a_3\theta + \cdots + a_{2n-1}\theta^{n-1} + a_{2n}\theta^{n-1}\omega = \alpha + \omega\beta$$

with $\alpha, \beta \in \mathbb{R}$. By (c), this element is in $\mathbb{R}$ iff it's fixed by complex conjugation, so iff $\beta = 0$. Hence every element of $\mathbb{R} \cap \mathbb{Z}[\omega]$ can be uniquely written as

$$a_1 + a_3\theta + a_5\theta^2 + \cdots + a_{2n-1}\theta^{n-1},$$

showing $\{1, \theta, \ldots, \theta^{n-1}\}$ is an integral basis for $\mathbb{R} \cap \mathbb{Z}[\omega] = \mathbb{A} \cap \mathbb{Q}[\theta]$ (see (d)). $\mathbb{A} \cap \mathbb{Q}[\theta] = \mathbb{Z}[\theta]$ follows.

35.(g) Using exercise 23.(b) with $K = \mathbb{Q}, L = \mathbb{Q}[\theta], M = \mathbb{Q}[\omega]$ and bases $\{1, \theta, \ldots, \theta^{n-1}\}, \{1, \omega\}$ we get, using (e),

$$\mathrm{disc}(\omega) = (\mathrm{disc}(\theta))^2 N^{\mathbb{Q}[\theta]}(\mathrm{disc}^{\mathbb{Q}[\omega]}_{\mathbb{Q}[\theta]}(1, \omega)).$$

We know that $\mathrm{disc}(\omega) = \pm p^{p-2}$. In (a) we have found a polynomial $f \in \mathbb{Q}[\theta][x]$ a root of which is ω, and from (b) it follows it's irreducible. Hence, by generalization of Theorem 8 established in exercise 23.(a) we have

$$\mathrm{disc}^{\mathbb{Q}[\omega]}_{\mathbb{Q}[\theta]}(1, \omega) = \pm N^{\mathbb{Q}[\omega]}_{\mathbb{Q}[\theta]}(f'(\omega))$$

and hence, by Theorem 5,

$$N^{\mathbb{Q}[\theta]}(\mathrm{disc}^{\mathbb{Q}[\omega]}_{\mathbb{Q}[\theta]}(1, \omega)) = \pm N^{\mathbb{Q}[\omega]}(f'(\omega))$$

We see $f'(\omega) = 2\omega - \omega\theta = -(\omega - \omega^{-1})^2 = -\omega^{-2}(\omega + 1)(\omega - 1)$. Therefore

$$N(f'(\omega)) = N(-\omega^{-2}(\omega + 1)(\omega - 1)) = \pm N(\omega + 1)N(\omega - 1)$$

(from here on N stands for $N^{\mathbb{Q}[\omega]}$). By Lemma 2, Theorem 10 we have $N(\omega - 1) = p$, while $1 + \omega$ is a unit by exercise 34.(a), so $N(\omega + 1) = \pm 1$. From all of the above we conclude $(\mathrm{disc}(\theta))^2 = \pm p^{p-3}$.

All conjugates of θ are real (because any embedding of $\mathbb{Q}[\omega]$ sends θ to $\omega^k + \omega^{-k} \in \mathbb{R}$ for some k), so, recalling the definition of discriminant, $\sqrt{\mathrm{disc}(\theta)} \in \mathbb{R}$, hence $(\mathrm{disc}(\theta))^2 = \sqrt{\mathrm{disc}(\theta)}^4 \geq 0$, so $(\mathrm{disc}(\theta))^2 = p^{p-3}, \mathrm{disc}(\theta) = \pm p^{(p-3)/2}$. But $\mathrm{disc}(\theta) = \sqrt{\mathrm{disc}(\theta)}^2 \geq 0$, thus $\mathrm{disc}(\theta) = p^{(p-3)/2}$.

36. For simplicity, write $\alpha_1 = 1, \alpha_2 = f_1(\alpha), \ldots, \alpha_k = f_{k-1}(\alpha)/d_{k-1}$. We first show that $\{\alpha_1, \ldots, \alpha_k, \beta\}$ is a linearly independent set. Since we have $\pi(\alpha^k) = \alpha^k \neq 0$, $\pi(\beta) \neq 0$ (since $\pi(\alpha^k)$ is integer multiple of $\pi(\beta)$ by assumption). Now suppose

$$a_1\alpha_1 + \cdots + a_k\alpha_k + b\beta = 0$$

with $a_1, \ldots, a_k, b \in \mathbb{Z}$. Because $\pi(\alpha_i) = 0$, this implies

$$0 = \pi(a_1\alpha_1 + \cdots + a_k\alpha_k + b\beta) = b\pi(\beta),$$

so $b = 0$. But $\{\alpha_1, \ldots, \alpha_k\}$ is a linearly independent set, so

$$a_1\alpha_1 + \cdots + a_k\alpha_k = 0$$

implies $a_1 = \cdots = a_k = 0$, proving linear independence of $\{\alpha_1, \ldots, \alpha_k, \beta\}$.

Now we show this set generates R_{k+1}. Let $\gamma \in R_{k+1}$. Then, by choice of β, $\pi(\gamma) = b\pi(\beta)$ for some $b \in \mathbb{Z}$, so that $\pi(\gamma - b\beta) = 0$, thus $\gamma - b\beta \in R_k$. By choice of $\alpha_1, \ldots, \alpha_k$, we can write

$$\gamma - b\beta = a_1\alpha_1 + \cdots + a_k\alpha_k$$

for $a_1, \ldots, a_k \in \mathbb{Z}$, hence

$$\gamma = a_1\alpha_1 + \cdots + a_k\alpha_k + b\beta,$$

thus $\{\alpha_1, \ldots, \alpha_k, \beta\}$ indeed generates R_{k+1} and so is an integral basis.

37. Suppose $f(\alpha) = g(\alpha)$. Then α is a root of the polynomial $f - g$, which is in $\mathbb{Q}[x]$ and has degree smaller than n. Since α has degree n, this means $f - g$ must be the zero polynomial, so $f = g$.

38. Clearly $1, f_1(\alpha)/d_1, \ldots, f_{k-1}(\alpha)/d_{k-1}$ are linearly independent, as a subset of certain basis. Let $\gamma \in R_k$, we may assume it's nonzero. Express it using the given basis for R. Let i be the largest such that $f_i(\alpha)/d_i$ has nonzero coefficient in this expression. Rewritting this expression now using the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ of $\mathbb{Q}[\alpha]$, we see γ has a nonzero coefficient of α^i. By definition of R_k, this means $i < k$. Hence R_k is generated by $1, f_1(\alpha)/d_1, \ldots, f_{k-1}(\alpha)/d_{k-1}$, meaning it is an integral basis.

Now suppose $mR_k \subseteq \mathbb{Z}[\alpha]$ for m a positive integer. Then in particular $m \cdot f_{k-1}(\alpha)/d_{k-1} \in \mathbb{Z}[\alpha]$, thus coefficient of α^{k-1} in this last number must be an integer. Since f_{k-1} is monic of degree $k-1$, this coefficient is m/d_{k-1}, showing $m \geq d_{k-1}$. On the other hand, we have $d_{k-1} \cdot f_i(\alpha)/d_i = f_i(\alpha) \cdot d_{k-1}/d_i \in \mathbb{Z}[\alpha]$ because $d_i \mid d_{k-1}$. Since by above 1 and $f_i(\alpha)/d_i, 0 < i < k$ form an integral basis for R_k, this implies $d_{k-1}R_k \subseteq \mathbb{Z}[\alpha]$.

39. We will show, by induction on k, that

$$1, g_1(\alpha)/d_1, \ldots, g_{k-1}(\alpha)/d_{k-1}$$

is an integral basis of R_k. For that, it's enough to show we can express $1, f_1(\alpha)/d_1, \ldots, f_{k-1}(\alpha)/d_{k-1}$ in terms of this new basis. This is clear for $k = 1$, so assume the result for a given $k < n - 1$, we will show it for $k + 1$. We therefore know that $1, f_1(\alpha)/d_1, \ldots, f_{k-1}(\alpha)/d_{k-1}$ can be expressed using this basis. To express $f_k(\alpha)/d_k$, note that $f_k(\alpha)/d_k - g_k(\alpha)/d_k$ has zero

coefficient of α^k (both f_k, g_k are monic of degree k) and are in R (as both $f_k(\alpha)/d_k, g_k(\alpha)/d_k$ are, by assumption), so it is an element of R_k. By our assumption, $f_k(\alpha)/d_k - g_k(\alpha)/d_k$ can be expressed as an integer linear combination of $\{1, g_1(\alpha)/d_1, \ldots, g_{k-1}(\alpha)/d_{k-1}\}$, so $f_k(\alpha)/d_k$ is an integer linear combination of $\{1, g_1(\alpha)/d_1, \ldots, g_k(\alpha)/d_k\}$, so the latter is a basis of R_{k+1}.

40.(a) We have $\mathrm{disc}(\alpha) = \mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{disc}(\mathbb{Z}[\alpha])$.

Claim. *$\{1, f_1(\alpha), \ldots, f_{n-1}(\alpha)\}$ is an integral basis for $\mathbb{Z}[\alpha]$.*

Proof. These elements are necessarily linearly independent and they are contained in $\mathbb{Z}[\alpha]$. By induction on i we show $\alpha^i, 0 \leq i < n$ is in the subgroup generated by them, so that whole $\mathbb{Z}[\alpha]$ is. This is clear for $i = 0$. If all powers of α below the ith are in the subgroup, then so is $\alpha^i - f_i(\alpha)$ (recall f_i is monic of degree i), hence so is α_i. Thus $1, f_1(\alpha), \ldots, f_{n-1}(\alpha)$ is an integral basis of $\mathbb{Z}[\alpha]$. □

This implies $\mathrm{disc}(\alpha) = \mathrm{disc}(1, f_1(\alpha), \ldots, f_{n-1}(\alpha))$. From the definition of discriminant and properties of determinants it's clear multiplying one of the elements of the n-tuple by a constant c changes discriminant by a factor of c^2. Hence

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

so $\mathrm{disc}(\alpha) = (d_1 \ldots d_{n-1})^2 \mathrm{disc}(R)$.

40.(b) By exercise 27.(c),

$$(d_1 \ldots d_{n-1})^2 \mathrm{disc}(R) = \mathrm{disc}(\mathbb{Z}[\alpha]) = |R/\mathbb{Z}[\alpha]|^2 \mathrm{disc}(R),$$

hence $|R/\mathbb{Z}[\alpha]| = d_1 \ldots d_{n-1}$.

40.(c) Since elements $f_i(\alpha)/d_i, f_j(\alpha)/d_j$ are in R, so must be their product $f_i(\alpha) f_j(\alpha)/d_i d_j$. Indeed, as $f_i f_j$ has degree $i+j$, this last element lies in R_{i+j+1}, so it is a linear combination of $1, f_1(\alpha)/d_1, \ldots, f_{i+j}(\alpha)/d_{i+j}$. This element has coefficient of α^{i+j} equal to $1/d_i d_j$, which must then be a multiple of $1/d_{i+j}$, hence $d_{i+j} \mid d_i d_j$.

40.(d) By induction we show $d_1^i \mid d_i$ for $i < n$: clear for $i = 1$, and if $d_1^{i-1} \mid d_{i-1}$, then $d_1^i \mid d_1 d_{i-1} \mid d_i$ by (c).

It follows that

$$d_1^{n(n-1)} = (d_1^1 d_2^2 \ldots d_1^{n-1})^2 \mid (d_1 d_2 \ldots d_{n-1})^2 \mid \mathrm{disc}(\alpha),$$

the last divisibility being clear from (a).

41.(a) By Theorem 8, $\text{disc}(\alpha) = -N(f'(\alpha))$, where $f(x) = x^3 - m$ is the minimal polynomial of α. We have $f'(\alpha) = 3\alpha^2$ so $N(f'(\alpha)) = 27N(\alpha)^2$. By looking at f, we see $N(\alpha) = m$. Hence $\text{disc}(\alpha) = -27m^2$.

Exercise 40.(d) tells is $d_1^6 \mid 27m^2$. If d_1 is divisible by a prime $p \neq 3$, then $p^6 \mid m^2, p^3 \mid m$, contradicting the fact m is cubefree. So d_1 is a power of 3. But if $9 \mid d_1$, then $3^{12} \mid 27m^2, 3^9 \mid m^2, 3^5 \mid m$, again contradicting m being cubefree. So $d_1 = 1$ or 3. If $d_1 = 3$, then $3^6 \mid 27m^2, 3^3 \mid m^2, 3^2 \mid m$.

41.(b) If $9 \mid m$ and $d_1 = 3$, then for some monic linear $f_1 = x + a \in \mathbb{Z}[x]$ we have $f_1(\alpha)/3 \in R$, i.e. $(\alpha + a)/3$. Cubing we get

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

Trace of α, α^2 is zero, so trace of this number is $\frac{a+m}{9} \in \mathbb{Z}, 9 \mid a + m$. Since $9 \mid m$, this implies $\frac{a}{3} \in \mathbb{Z} \subseteq R$, hence $\frac{\alpha}{3} \in R$. Cubing this, we get $\frac{m}{27} \in R$, hence $27 \mid m$. But m is cubefree, so this can't be. Thus $d_1 = 3$ cannot hold.

41.(c) $\frac{\alpha^2}{k} = \sqrt[3]{\frac{h^2k^4}{k^3}} = \sqrt[3]{h^2k}$ is a root of monic polynomial $x^3 - h^2k$, so is an algebraic integer.

41.(d) On one hand, we have

$$\left(\beta - \frac{1}{3}\right)^3 = \beta^3 - \beta^2 + \frac{1}{3}\beta - \frac{1}{27}.$$

On the other hand,

$$\begin{aligned}\left(\beta - \frac{1}{3}\right)^3 &= \left(\frac{\alpha^2 \mp 2\alpha}{3}\right)^3 = \frac{\alpha^6 \mp 6\alpha^5 + 12\alpha^4 \mp 8\alpha^3}{27} \\ &= \frac{m^2 \mp 6m\alpha^2 + 12m\alpha \mp 8m}{27} = \frac{m^2 \mp 2m}{27} \mp \frac{6m\alpha^2 \mp 12m\alpha + 6m}{27} \\ &= \frac{(m \mp 1)^2}{27} - \frac{1}{27} \mp \frac{2m}{3}\beta.\end{aligned}$$

Equating the two gives us

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

Because $m \equiv \pm 1 \pmod 9$, all the coefficients of β above are in $\mathbb{Z}$. Hence β is a root of monic cubic polynomial from $\mathbb{Z}[x]$, showing β is an algebraic integer.

41.(e) From (c) we know k divides α^2, so it clearly divides $\alpha^2 \pm k^2\alpha + k^2$. Also, by (d), 3 divides $\alpha^2 \mp 2\alpha + 1$, but it also divides $k^2 - 1, k^2 + 2$ (as $k \in \mathbb{Z}, 3 \nmid k$), so 3 also divides $\alpha^2 \pm k^2\alpha + k^2$. Say $\gamma = \alpha^2 \pm k^2\alpha + k^2$, $\frac{\gamma}{k} = \gamma_1$, $\frac{\gamma}{3} = \gamma_2, \gamma_1, \gamma_2 \in R$. As $3, k$ are relatively prime, $3a + kb = 1$ for some $a, b \in \mathbb{Z}$. But then

$$3\gamma a + k\gamma b = \gamma.$$

Since $k \mid \gamma, 3 \mid \gamma$, the above shows $3k \mid 3\gamma a + k\gamma b = \gamma$, so $\frac{\gamma}{3k} \in R$.

41.(f) By exercise 40.(a), $d_2^2 \mid 27m^2 = 3 \cdot (3m)^2$, so $d_2 \mid 3m$

41.(g) Since $(\alpha^2 + a\alpha + b)/d_2 \in R$, under these assumptions $(\alpha^2 + a\alpha + b)/p = d_2/p \cdot (\alpha^2 + a\alpha + b)/d_2 \in R$. Trace of this number is $3b/p$, so, being an integer, $p \mid 3b, p \mid b$ (as $p \neq 3$). Hence $(\alpha^2 + a\alpha)/p \in R$. Cubing gives

$$\frac{\alpha^6 + 3a\alpha^5 + 3a^2\alpha^4 + a^3\alpha^3}{p^3} = \frac{3am\alpha^2 + 3a^2m\alpha + m^2 + a^3m}{p^3}.$$

Trace gives $p^3 \mid 3m(m + a^3)$. Since $p \nmid 3, p^2 \nmid m$ we have $p^2 \mid m + a^3$. Since $p \mid m$, this gives $p \mid a^3, p \mid a, p^2 \mid a^3, p^2 \mid m$, contradicting our assumptions. So $p \nmid d_2$.

41.(h) Suppose $p^2 \mid d_2$. Just as in (g), we then find $p^6 \mid m(m + a^3)$. Since $p^3 \nmid m, p^4 \mid m + a^3$. As $p \mid m, p \mid a^3, p^3 \mid a^3$ giving $p^3 \mid m$, which contradicts m being cubefree.

41.(i) We compute

$$\begin{aligned}\left(\frac{\alpha^2 + a\alpha + b}{d_2}\right)^2 &= \frac{\alpha^4 + 2a\alpha^3 + (a^2 + 2b)\alpha^2 + 2ab\alpha + b^2}{d_2^2} \\ &= \frac{(2b + a^2)\alpha^2 + (m + 2ab)\alpha + b^2 + 2am}{d_2^2}.\end{aligned}$$

Exercise 38 implies, as this element is in R, that

$$\frac{(2b + a^2)\alpha^2 + (m + 2ab)\alpha + b^2 + 2am}{d_2} \in \mathbb{Z}[\alpha],$$

thus d_2 divides $2b + a^2, m + 2ab, b^2 + am$.

41.(j) Suppose $3 \nmid m, m \not\equiv \pm 1 \pmod 9$, and also $3 \mid d_2$. (i) implies all three numbers there are divisible by 3. In particular, $3 \mid m + 2ab$. Since $3 \nmid m, 3 \nmid a, b$. So $0 \equiv 2b + a^2 \equiv 2b + 1 \pmod 3, b \equiv 1 \pmod 3$. From there $0 \equiv m + 2ab \equiv m + 2a \equiv m - a \pmod 3$, so $m \equiv a \pmod 3$.

As $3 \mid d_2$, $3 \mid \alpha^2 + a\alpha + b$, hence, by above, $3 \mid \alpha^2 + m\alpha + 1$. If $m \equiv \pm 1 \pmod 3$, then $3 \mid \alpha^2 \mp 2\alpha + 1 = (\alpha \mp 1)^2$, so $(\alpha \mp 1)^2/3 \in R$. Its fourth power is $(\alpha \mp 1)^8/81$. The only terms of the numerator which will contribute anything

to the trace are $\binom{8}{2}\alpha^6 = 28m^2, \mp\binom{8}{5}\alpha^3 = \mp 56m, 1$. Hence the trace will be $(28m^2 \mp 56m + 1)/27$, so $27 \mid 28m^2 \mp 56m + 1$. But now

$$28m^2 \mp 56m + 1 \equiv 28m^2 \mp 56m + 28 \equiv 28(m \mp 1)^2 \equiv (m \mp 1)^2 \pmod{27},$$

so $27 \mid (m \mp 1)^2, 9 \mid m \mp 1$ and so $m \equiv \pm 1 \pmod 9$, contradicting our assumption.

41.(k) If $3 \mid m, 9 \nmid m$ and $3 \mid d_2$, (i) implies that $3 \mid b^2 + am, 3 \mid b$, and since $3 \mid 2b + a^2, 3 \mid a$.

$3 \mid d_2$ implies $3 \mid \alpha^2 + a\alpha + b$, so by above $3 \mid \alpha^2$, i.e. $\alpha^2/3 \in R$. But taking cube of this element, we get $27 \mid m^2, 9 \mid m$ contradicting out assumption. So $3 \nmid d_2$.

41.(l) Suppose $9 \mid m$ and $9 \mid d_2$. Then (i) implies $9 \mid 2ab$. If $3 \nmid a$, then this implies $9 \mid b$. If $3 \mid a$, then $9 \mid b$ follows from $9 \mid 2b + a^2$.

Since $9 \mid \alpha^2 + a\alpha + b, 9 \mid \alpha^2 + a\alpha$. Cubing $(\alpha^2 + a\alpha)/9$ and taking trace implies $3^5 \mid m(m + a^3)$. As $3^3 \nmid m, 3^3 \mid m + a^3$. But then $3 \mid a, 3^3 \mid a^3, 3^3 \mid m$ giving us a contradiction. Hence $9 \nmid d_2$.

42.(a) Let α' be the conjugate element of α with respect to base field $\mathbb{Q}[\sqrt{m}]$ (if $\alpha \in \mathbb{Q}[\sqrt{m}]$, then $\alpha' = \alpha$). Then $T^K_{\mathbb{Q}[\sqrt{m}]}(\alpha) = \alpha + \alpha', N^K_{\mathbb{Q}[\sqrt{m}]} = \alpha\alpha'$. If both these are algebraic integers, then α is as well, as a root of a monic polynomial $x^2 - (\alpha + \alpha')x + \alpha\alpha'$ with algebraic integer coefficients (see exercise 4). Conversely, if α is a root of a monic integer polynomial, then α' is a root of the same polynomial. Then both $T^K_{\mathbb{Q}[\sqrt{m}]}(\alpha), N^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ are algebraic integers.

42.(b) Let $\alpha = w + x\sqrt{m} + y\sqrt{n} + z\sqrt{k}, w, x, y, z \in \mathbb{Q}$. Taking $T^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ we find that $2w + 2z\sqrt{m} \in \mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$ which is generated by $1, \sqrt{m}$ as $m \equiv 3 \pmod 4$. This implies $2w, 2x \in \mathbb{Z}$. By considering other two relative traces, we also get $2y, 2z \in \mathbb{Z}$. Writing $2w = a, 2x = b, 2y = c, 2z = d$ we get

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2}.$$

By (a), $\alpha \in R$ then its relative norm is an algebraic integer. We have

$$\begin{aligned} N^K_{\mathbb{Q}[\sqrt{m}]}(\alpha) &= \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2} \frac{a + b\sqrt{m} - (c\sqrt{n} + d\sqrt{k})}{2} \\ &= \frac{a^2 + 2ab\sqrt{m} + b^2m - c^2n - 2cd\sqrt{nk} - d^2k}{4}. \end{aligned}$$

We have $\sqrt{nk} = \frac{n}{(n,m)}\sqrt{m}$. The fraction is an even integer, so $2cd\sqrt{nk} \equiv 0 \pmod 4$. Hence the coefficient of $\sqrt{m}$ in this norm is $\frac{2ab}{4}$. For this to be integer, one of a, b must be even. We will see in fact both are even.

Coefficient of 1 in the numerator is

$$a^2 + b^2 m - c^2 n - d^2 k \equiv a^2 - b^2 - 2(c^2 + d^2) \pmod 4.$$

For this to be divisible by 4, we need $a^2 - b^2$ to be even. But since one of the terms in this difference is even, the other has to be as well. So both a, b are even, so $c^2 + d^2 \equiv 0 \pmod 2$. This means c, d have the same parity. Therefore

$$\alpha = p + q\sqrt{m} + \frac{c\sqrt{n} + d\sqrt{m}}{2} = p + q\sqrt{m} + \frac{d-c}{2}\sqrt{n} + c\frac{\sqrt{n} + \sqrt{m}}{2}$$

with $p, q, c, \frac{d-c}{2}$ integers. So R is contained in the subgroup generated by

$$1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n} + \sqrt{k}}{2}.$$

But it's straightforward to verify all these are algebraic integers. So this is an integral basis for R.

42.(c) Write $\alpha = w + x\sqrt{m} + y\sqrt{n} + z\sqrt{k}, w, x, y, z \in \mathbb{Q}$. Taking trace relative to $\mathbb{Q}[\sqrt{n}]$ gives $2w + 2y\sqrt{n}$ is an algebraic integer, so $a = 2w, c = 2y$ are integers. Similarly $d = 2z$ is an integer. Taking trace relative to $\mathbb{Q}[\sqrt{m}]$ shows that $2w + 2z\sqrt{m}$ is an algebraic integer, so it must be of the form $\frac{p+q\sqrt{m}}{2}$ with p, q of the same parity. But since $2q$ is an integer, p is even, hence so is q and $b = 2x$ is an integer. So

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2}.$$

By (a), if $\alpha \in R$ then its relative norm is an algebraic integer. Taking norm relative $\mathbb{Q}[\sqrt{n}]$ we get

$$\begin{aligned} N^K_{\mathbb{Q}[\sqrt{n}]}(\alpha) &= \frac{a + c\sqrt{n} + b\sqrt{m} + d\sqrt{k}}{2} \frac{a + c\sqrt{n} - (b\sqrt{m} + d\sqrt{k})}{2} \\ &= \frac{a^2 + 2ac\sqrt{n} + c^2 n - b^2 m - 2bd\sqrt{mk} - d^2 k}{4}. \end{aligned}$$

Coefficient of 1 in the numerator is $a^2 + c^2 n - b^2 m - d^2 k \equiv a^2 - b^2 + n(c^2 - d^2) \pmod 4$ (recall $n \equiv k \pmod 4$), which has to be divisible by 4. If $n \equiv 2 \pmod 4$, then this implies that $a^2 - b^2$ is even, so that $a \equiv b \pmod 2$ and $a^2 - b^2 \equiv 0 \pmod 4$, and hence $c^2 - d^2$ has to be even, which means $c \equiv d \pmod 4$. If $n \equiv 3 \pmod 4$, this gives $a^2 - b^2 - c^2 + d^2 \pmod 4$. For this to be even, an even number out of a, b, c, d must be odd.

If a, b have different parity, then c, d have different parity as well. By looking at this expression, we see that either a and c are odd or b and d are. We see the coefficient of $\sqrt{n}$ in the numerator is $2ac + 2bd \cdot \frac{m}{(m,n)} \equiv 2ac + 2bd \pmod 4$ since $\frac{m}{(m,n)}$ is odd. But if a, c are odd or b, d are odd, then this coefficient is not

divisible by 4. Hence if this norm is an algebraic integer, $a \equiv b, c \equiv d \pmod 2$. Thus every element of R can be written as

$$a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}2 = \frac{a-b}{2} + b\frac{1+\sqrt{m}}{2} + \frac{c-d}{2}\sqrt{n} + d\frac{\sqrt{n}+\sqrt{k}}{2}$$

with $a, b, c, d \in \mathbb{Z}, a \equiv b, c \equiv d \pmod 2$, or, equivalently, with $\frac{a-b}{2}, b, \frac{c-d}{2}, d$ integers. It follows that the subgroup generated by

$$1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}$$

contains R, so, since these are easily seen to be algebraic integers, they are an integral basis for R.

42.(d) Writing $\alpha = w + x\sqrt{m} + y\sqrt{n} + z\sqrt{k}, w, x, y, z \in \mathbb{Q}$ and taking trace relative to $\mathbb{Q}[\sqrt{m}]$ we see $2w + 2x\sqrt{m}$ is an algebraic integer, so it is of the form $\frac{a+b\sqrt{m}}{2}, a \equiv b \pmod 2$, so $w = \frac{a}{4}, x = \frac{b}{4}$. Similarly, $y = \frac{c}{4}, z = \frac{d}{4}$ with $a \equiv c, a \equiv d \pmod 2$. Hence

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{4}$$

with $a \equiv b \equiv c \equiv d \pmod 2$. Subtracting from this $d\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)$ and noting $\sqrt{mk}$ is an integer multiple of $\sqrt{n}$, we get an element of R of the form

$$\frac{a' + b'\sqrt{m} + c'\sqrt{n}}{4}$$

with (by above) $a' \equiv b' \equiv c' \equiv 0 \pmod 2$. Writing $a' = 2r, b' = 2s, c' = 2t$, it is equal to

$$\frac{r + s\sqrt{m} + t\sqrt{n}}{2}.$$

. Taking norm of this element relative to $\mathbb{Q}[\sqrt{n}]$ we get

$$\frac{r + s\sqrt{m} + t\sqrt{n}}{2}\frac{r + s\sqrt{m} - t\sqrt{n}}{2} = \frac{r^2 + 2rs\sqrt{m} + s^2m - t^2n}{4}.$$

This must be an algebraic integer, so the coefficient of 1 in this must be divisible by 2. This coefficient is equal to $r^2+s^2m-t^2n \equiv r-s-t \equiv 0 \pmod 2$. Therefore

$$\frac{r + s\sqrt{m} + t\sqrt{n}}{2} = \frac{r-s-t}{2} + s\frac{1+\sqrt{m}}{2} + t\frac{1+\sqrt{n}}{2}$$

with all three coefficients integral, thus

$$\alpha = \frac{r-s-t}{2} + s\frac{1+\sqrt{m}}{2} + t\frac{1+\sqrt{n}}{2} + d\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right).$$

It's clear

$$1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)$$

are algebraic integers, so by above they form an integral basis for R.

42.(e) Since m, n are squarefree, we see so is k. Thus none of these numbers is divisible by 4. Moreover, $mn = (m,n)^2 k$. If both $m \equiv n \equiv 2 \pmod 4$, we have $2 \nmid k$, so $k \equiv 1$ or $3 \pmod 4$. These two possibilities, with reordered terms, are covered in (c) and (b), respectively. Now if m, n are not both even, $(m,n)^2 \equiv 1 \pmod 4$, so $mn \equiv k \pmod 4$. If one of m, n, say n, is even, then $k \equiv 2 \pmod 4$, so we get cases covered in (b) and (c), this time without reordering. Otherwise, all m, n, k are odd, and either all or exactly one of them is $1 \pmod 4$. These are covered in (d) and (c), respectively.

42.(f)

Claim. *In all cases,* $\mathrm{disc}(1, \sqrt{m}, \sqrt{n}, \sqrt{k}) = 256mnk$.

Proof. By again using properties of determinants,

$$\mathrm{disc}(1, \sqrt{m}, \sqrt{n}, \sqrt{k}) = \frac{k}{mn}\mathrm{disc}(1, \sqrt{m}, \sqrt{n}, \sqrt{mn}).$$

To find the latter, we use exercise 23.(b) with $K = \mathbb{Q}, L = \mathbb{Q}[\sqrt{m}], M = \mathbb{Q}[\sqrt{n}, \sqrt{m}]$ (which is denoted K in this exercise) and the bases $1, \sqrt{m}$ and $1, \sqrt{n}$. We then get

$$\mathrm{disc}^M(1, \sqrt{m}, \sqrt{n}, \sqrt{mn}) = (\mathrm{disc}^L(1, \sqrt{m}))^2 N_L^M(\mathrm{disc}_L^M(1, \sqrt{n})).$$

We have $\mathrm{disc}^L(1, \sqrt{m}) = 4m$ and $\mathrm{disc}_L^M(1, \sqrt{n}) = 4n$, which has relative norm $16n^2$. This gives

$$\begin{aligned} \mathrm{disc}(1, \sqrt{m}, \sqrt{n}, \sqrt{mn}) &= (4m)^2 16n^2 = 256(mn)^2, \\ \mathrm{disc}(1, \sqrt{m}, \sqrt{n}, \sqrt{k}) &= 256mnk. \end{aligned}$$

□

In (b), from basic properties of determinants we see

$$\begin{aligned} \mathrm{disc}(R) &= \mathrm{disc}\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right) = \frac{1}{4}\mathrm{disc}(1, \sqrt{m}, \sqrt{n}, \sqrt{n}+\sqrt{k}) \\ &= \frac{1}{4}\mathrm{disc}(1, \sqrt{m}, \sqrt{n}, \sqrt{k}) = 64mnk. \end{aligned}$$

At the same time, the discriminants of four quadratic subfields are $4m, 4n, 4k$ since $m, n, k \not\equiv 1 \pmod 4$, and $4m \cdot 4n \cdot 4k = \mathrm{disc}(R)$.

In (c) we find

$$\begin{aligned}\mathrm{disc}R &= \mathrm{disc}\left(1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right) = \frac{1}{16}\mathrm{disc}(1, 1+\sqrt{m}, \sqrt{n}, \sqrt{n}+\sqrt{k}) \\ &= \frac{1}{16}\mathrm{disc}(1, \sqrt{m}, \sqrt{n}, \sqrt{k}) = 16mnk.\end{aligned}$$

The quadratic subfields have discriminants $m, 4n, 4k$, so the product formula holds.

In (d)

$$\begin{aligned}\mathrm{disc}R &= \mathrm{disc}\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{(1+\sqrt{m})(1+\sqrt{k})}{4}\right) \\ &= \frac{1}{256}\mathrm{disc}(1, 1+\sqrt{m}, 1+\sqrt{n}, 1+\sqrt{m}+\sqrt{mk}+\sqrt{k}) \\ &= \frac{1}{256}\mathrm{disc}(1, \sqrt{m}, \sqrt{n}, \sqrt{k}) = mnk\end{aligned}$$

(recall $\sqrt{mk}$ is an integer multiple of $\sqrt{n}$). Product formula again holds, as quadratic subfields have discriminants m, n, k.

43.(a) By Theorem 8 $\mathrm{disc}(\alpha) = N(f'(\alpha)) = N(\alpha f'(\alpha))/N(\alpha)$. We have $\alpha f'(\alpha) = 5\alpha^5 + a\alpha = 5(-a\alpha - b) + a\alpha = -4a\alpha - 5b$. We see $4a\alpha + 5b$ is a root of $\left(\frac{x-5b}{4a}\right)^5 + a\left(\frac{x-5b}{4a}\right) + b$, from where we find

$$\begin{aligned}N(\alpha f'(\alpha)) &= -N(4a\alpha + 5b) = \frac{\left(-5^5b^5/4a^5 - 5b/4 + b\right)}{1/(4a)^5} \\ &= -5^5b^5 - 5\cdot 4^4a^5b + 4^5a^5b = -5^5b^5 - 4^4a^5b.\end{aligned}$$

Thus

$$\mathrm{disc}(\alpha) = \frac{N(\alpha f'(\alpha))}{N(\alpha)} = \frac{-5^5b^5 - 4^4a^5b}{-b} = 5^5b^4 + 4^4a^5.$$

43.(b) If $\alpha^5 = \alpha + 1$, then we have $a = b = -1$. Then $\mathrm{disc}(\alpha) = 5^5 - 4^4 = 19\cdot 151$ is squarefree. By exercise 27.(e) $1, \alpha, \ldots, \alpha^4$ is a basis for $\mathbb{A}\cap\mathbb{Q}[\alpha]$, so $\mathbb{A}\cap\mathbb{Q}[\alpha] = \mathbb{Z}[\alpha]$.

43.(c) By exercise 40.(a), $(d_1d_2d_3d_4)^2 \mid \mathrm{disc}(\alpha) = a^4(4^4a + 5^5)$. If we assume $4^4a + 5^5$ is squarefree, then, as can be seen by looking at factorizations, $(d_1d_2d_3d_4)^2 \mid a^4, d_1d_2d_3d_4 \mid a^2$. However $d_2 \mid d_3, d_4$, so $d_2^3 \mid a^2$. Since a is squarefree, this can only be if $d_2 = 1$. Hence also $d_1 = 1$ and $d_3d_4 \mid a^2$.

For given a, $4^4a + 5^5$ have prime factorizations

$$3\cdot 13\cdot 67, 2357, 7\cdot 227, 31\cdot 43, 5\cdot 113, 3\cdot 103, -7\cdot 29, -5\cdot 11\cdot 13.$$

Some more examples of such squarefree $4^4a + 5^5$ are given by

$$-17, -19, -21, -22, -26, -29, -30, \ldots$$

43.(d) We have $\alpha^5 = -a\alpha - a = -a(\alpha+1)$, and

$$N(\alpha+1) = \frac{N(\alpha)^5}{N(-a)} = \frac{(-a)^5}{(-a)^5} = 1,$$

so $\alpha+1$ is a unit.

44.(a) By Theorem 8

$$\operatorname{disc}(\alpha) = N(f'(\alpha)) = N(5\alpha^4 + 4a\alpha^3) = N(\alpha)^3 N(5\alpha+4a) = -b^3 N(5\alpha+4a).$$

Clearly $5\alpha+4a$ is a root of $\left(\frac{x-4a}{5}\right)^5 + a\left(\frac{x-4a}{5}\right)^4 + b$. From there we see

$$\begin{aligned} N(5\alpha+4a) &= -\frac{(-4a/5)^5 + a(4a/5)^4 + b}{1/5^5} = -(-4^5a^5 + 5\cdot 4^4a^5 + 5^5b) \\ &= -(4^4a^5 + 5^5b), \end{aligned}$$

thus $\operatorname{disc}(\alpha) = b^3(4^4a^5 + 5^5b)$.

44.(b) First we show b^3 and $4^4a + 5^5b$ are relatively prime. Indeed, if prime p divides both of these numbers, then it also divides b and hence also 4^4a, thus it either divides a or is 2. But this contradicts assumption that $b, 2a$ are relatively prime.

By exercise 40.(a) we have $d_3^4 = (d_3d_4)^2 \mid \operatorname{disc}(\alpha) = b^3(4^4a^5 + 5^5b)$. If $4^4a^5 + 5^5b$ is squarefree, this implies $d_3^4 \mid b^3$, which, if b is squarefree, is only possible if $d_3 = 1$. Hence also $d_1 = d_2 = 1$.

Moreover, $d_4^2 \mid \operatorname{disc}(\alpha) = b^3(4^4a^5 + 5^5b)$, so $d_4^2 \mid b^3$. Looking at prime factorizations and recalling b is squarefree, this implies $d_4 \mid b$.

For $b = 5, a = -2$, clearly b is squarefree, b and $2a = -4$ are relatively prime, and also $4^4a^5 + 5^5b = 7433$ is prime, thus squarefree.

44.(c) If $a = \pm b$, then $\operatorname{disc}(\alpha) = a^3(4^4a^5 \pm 5^5a) = a^4((4a)^4 \pm 5^5)$. By exercise 40.(a), $d_2^6 \mid (d_2d_3d_4)^2 \mid \operatorname{disc}(\alpha) = a^4((4a)^4 \pm 5^5)$, so, assuming the latter factor is squarefree, it follows that $d_2^6 \mid a^4$. Since a is squarefree, this means $d_2 = 1$ hence also $d_1 = 1$. Additionally, $(d_3d_4)^2 \mid a^4((4a)^4 \pm 5^5)$, so $(d_3d_4)^2 \mid a^4, d_3d_4 \mid a^2$.

44.(d) If we have $\alpha^5 + a\alpha^4 \pm a$, i.e. $\alpha^5 = -a\alpha^4 \mp a = -a(\alpha^4 \pm 1)$, then

$$N(\alpha^4 \pm 1) = \frac{N(\alpha)^5}{N(-a)} = \frac{(\mp a)^5}{(-a)^5} = \pm 1,$$

so $N(\alpha^4 \pm 1)$ is a unit.

45. Assume first α is a root of irreducible $x^n + ax + b = 0$. Then $N(\alpha) = (-1)^n b$. We also have

$$N(f'(\alpha)) = \frac{N(\alpha f'(\alpha))}{N(\alpha)} = (-1)^n \frac{N(n\alpha^n + a\alpha)}{b} = (-1)^n \frac{N(-na\alpha - nb + a\alpha)}{b}$$
$$= (-1)^n \frac{N(-(n-1)a\alpha - nb)}{b} = \frac{N((n-1)a\alpha + nb)}{b}.$$

It's clear $(n-1)a\alpha + nb$ is a root of

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

It follows that

$$N((n-1)a\alpha + nb) = \frac{(-nb/(n-1)a)^n - nb/(n-1) + b}{1/((n-1)a)^n}$$
$$= (-nb)^n - (n-1)^{n-1}na^n b + (n-1)^n a^n b$$
$$= (-1)^n n^n b^n - (n-1)^{n-1}a^n b,$$

thus

$$N'(f'(\alpha)) = (-1)^n n^n b^{n-1} - (n-1)^{n-1}a^n,$$
$$\text{disc}(\alpha) = \pm((-1)^n n^n b^{n-1} - (n-1)^{n-1}a^n)$$

by Theorem 8, with + sign iff $n \equiv 0, 1 \pmod 4$.

If α is a root of irreducible $x^n + ax^{n-1} + b$. Then

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

(for the last equality, n is even iff $n(n-2)$ is). $n\alpha - a(n-1)$ is a root of

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

from which we see

$$N(n\alpha + a(n-1)) = (-1)^n \frac{(-a(n-1)/n)^n + a(-a(n-1)/n)^{n-1} + b}{1/n^n}$$
$$= (n-1)^n a^n - (n-1)^{n-1}na^n + (-1)^n n^n b$$
$$= -(n-1)^{n-1}a^n + (-1)^n n^n b,$$

thus

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

with + sign iff $n \equiv 0, 1 \pmod 4$.

46.(a) Note f' is a polynomial integer coefficients and an integer root r.

Claim. *$f'(x)$ can be written as $(x-r)g(x)$ with $g \in \mathbb{Z}[x]$.*

Proof. We provide a simple proof avoiding exercise 8.(c), chapter 3. Consider polynomial $f'(x+r)$. It has integer coefficients and is zero at $x=0$, so it's constant term is zero. Factoring it out, we have $f'(x+r) = xh(x)$ for $h \in \mathbb{Z}[x]$. Plugging in $x-r$ in place of x we recover $f'(x) = (x-r)g(x)$ for $g(x) = h(x-r) \in \mathbb{Z}[x]$. □

Let $\alpha_1, \ldots, \alpha_n$ be conjugates of α. By Theorem 8

$$\begin{aligned}\operatorname{disc}(\alpha) &= \pm N(f'(\alpha)) = \pm \prod_{i=1}^{n} f'(\alpha_i) = \pm \prod_{i=1}^{n} (\alpha_i - r) g(\alpha_i) \\ &= \pm(-1)^n \prod_{i=1}^{n} (r - \alpha_i) \prod_{i=1}^{n} g(\alpha_i) = \pm(-1)^n f(r) \prod_{i=1}^{n} g(\alpha_i),\end{aligned}$$

hence $f(r) \mid \operatorname{disc}(\alpha)$ in algebraic integers, thus the divisibility also holds in integers.

46.(b) Suppose f' has a root r, s with $\gcd(r,s) = 1$.

Claim. *$f'(x) = (sx-r)g(x)$ with $g \in \mathbb{Z}[x]$.*

Proof. $sx - r$ is an integer polynomials coefficients of which have gcd 1. We know $f'(x) = (sx-r)g(x)$ with $g \in \mathbb{Q}[x]$, possibly with noninteger coefficients. Let $c \in \mathbb{Z}$ be such that cg has integer coefficients. Then $sx - r$ divides $c \cdot f'$ in $\mathbb{Z}[x]$. Thus, by exercise 8.(d) of chapter 3, $sx - r$ either divides c or f' in $\mathbb{Z}[x]$. But c is a constant polynomial, so $sx - r$ divides $f'(x)$. □

Let $\alpha_1, \ldots, \alpha_n$ be conjugates of α. By Theorem 8

$$\begin{aligned}\operatorname{disc}(\alpha) &= \pm N(f'(\alpha)) = \pm \prod_{i=1}^{n} f'(\alpha_i) = \pm \prod_{i=1}^{n} (s\alpha_i - r) g(\alpha_i) \\ &= \pm(-1)^n s^n \prod_{i=1}^{n} \left(\frac{r}{s} - \alpha_i\right) \prod_{i=1}^{n} g(\alpha_i) = \pm(-1)^n s^n f\left(\frac{r}{s}\right) \prod_{i=1}^{n} g(\alpha_i),\end{aligned}$$

so $s^n f\left(\frac{r}{s}\right)$ (easily seen to be an integer) divides $\operatorname{disc}(\alpha)$.

46.(c) Write $g(x)f'(x) = h(x) + k(x)f(x)$. Plugging in α we get $g(\alpha)f'(\alpha) = h(\alpha)$. Write $g(x) = a(x-r_1)\ldots(x-r_k), h(x) = b(x-s_1)\ldots(x-s_l)$. Then

$$\begin{aligned}N(f'(\alpha)) &= \frac{N(h(\alpha))}{N(g(\alpha))} = \frac{b^n}{a^n} \frac{\prod_{j=1}^{k} N(\alpha - s_j)}{\prod_{j=1}^{l} N(\alpha - r_j)} = \frac{b^n}{a^n} \frac{\prod_{j=1}^{k} \prod_{i=1}^{n} (\alpha_i - s_j)}{\prod_{j=1}^{l} \prod_{i=1}^{n} (\alpha_i - r_j)} \\ &= (-1)^{(k+l)n} \frac{b^n}{a^n} \frac{\prod_{j=1}^{k} \prod_{i=1}^{n} (s_j - \alpha_i)}{\prod_{j=1}^{l} \prod_{i=1}^{n} (r_j - \alpha_i)} = (-1)^{(k+l)n} \frac{b^n}{a^n} \frac{\prod_{j=1}^{k} f(s_j)}{\prod_{j=1}^{l} f(r_j)}.\end{aligned}$$

Thus

$$\operatorname{disc}(\alpha) = \pm(-1)^{(k+l)n}\frac{b^n}{a^n}\frac{\prod_{j=1}^{k} f(s_j)}{\prod_{j=1}^{l} f(r_j)},$$

where, as usual, + sign holds iff $n \equiv 0, 1 \pmod 4$.

47. We have

$$\begin{aligned} xf'(x) &= 5x^5 - 2x^2 \equiv 5x^2 - 75 - 2x^2 = 3(x^2 - 25) \\ &= 3(x-5)(x+5) \pmod{f(x)}. \end{aligned}$$

Using the formula established in exercise 46.(c), with $g(x) = x, h(x) = 3(x-5)(x+5)$, hence $a = 1, r_1 = 0, b = 3, s_1 = 5, s_2 = -5$

$$\operatorname{disc}(\alpha) = -3^5\frac{f(5)f(-5)}{f(0)} = -3^5\frac{3115 \cdot (-3135)}{15} = 158201505$$

48.(a) If $a^2 - 3b = d^2$, then we quickly verify

$$f'(x) = 3\left(x - \frac{-a+d}{3}\right)\left(x - \frac{-a-d}{3}\right).$$

Using formula derived in exercise 46.(c) with $g(x) = 1, h(x) = f'(x)$ and $b = 3, s_1 = \frac{-a+d}{3}, s_2 = \frac{-a-d}{3}$ we get

$$\operatorname{disc}(\alpha) = -27f\left(x - \frac{-a+d}{3}\right)f\left(x - \frac{-a-d}{3}\right).$$

48.(b) One way to justify why this equality holds for all d is to show that the method used to show it for $d \in \mathbb{Q}$ is still valid if we replace $\mathbb{Q}$ by $\mathbb{Q}[d]$. Indeed, working through the solution of exercise 46.(c) we see that in fact at no point we have used that g, h have integer coefficients. It's not hard to verify this result holds true if we take f to be irreducible polynomial of α over $\mathbb{Q}[d]$ and g, h any polynomials over $\mathbb{Q}[d]$.

The only point to verify is that if $f(x) = x^3 + ax^2 + bx + c$ is irreducible over $\mathbb{Q}$, then it is irreducible over $\mathbb{Q}[d]$. Suppose for the contrary that it is not irreducible. Since f is cubic, it must then have a root α' in $\mathbb{Q}[d]$. Then $\mathbb{Q}[\alpha'] \subseteq \mathbb{Q}[d]$. But the former of these fields has degree 3, while the latter has degree at most 2 (as $d^2 \in \mathbb{Q}$).

48.(c) We compute

$$\begin{aligned}(3x+a)f'(x) &= (3x+a)(3x^2+2ax+b)\\ &= 9x^3+6ax^2+3bx+3ax^2+2a^2x+ab\\ &= 9(x^3+ax^2)+(2a^2+2b)x+ab\\ &\equiv 9(-bx-c)+(2a^2+3b)x+ab\\ &= (2a^2-6b)x+ab-9c\\ &= 2(a^2-3b)\left(x-\frac{9c-ab}{2a^2-6b}\right).\end{aligned}$$

Applying exercise 46.(c) with $g(x)=3x+a$, $h(x)=2(a^2-2b)\left(x-\frac{9c-ab}{2a^2-6b}\right)$ and $a=3, b=2(a^2-3b), r_1=-\frac{a}{3}, s_1=\frac{9c-ab}{2a^2-6b}$ gives

$$\operatorname{disc}(\alpha)=-\frac{8(a^2-3b)^3 f\left(\frac{9c-ab}{2a^2-6b}\right)}{27f\left(-\frac{a}{3}\right)}=\frac{8(3b-a^2)^3 f\left(\frac{9c-ab}{2a^2-6b}\right)}{27f\left(-\frac{a}{3}\right)}.$$

48.(d) Polynomials $x^3-6x^2\pm 9x+3$ are irreducible by Eisenstein criterion. Thus we can use the formula from (c). Direct substitution gives

$$\operatorname{disc}(\alpha)=-567$$

in the first case and

$$\operatorname{disc}(\alpha)=11097$$

in the second case.