

## Chapter 2

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

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

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

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

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

Therefore the quadratic fields are each distinct.

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

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

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

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

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

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

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

$2r$  being an integer requires that  $r = \frac{a}{2}$ , where  $a$  is an integer. Substituting  $r = \frac{a}{2}$  into the second equation, we see that  $a^2 - 4ms^2$  is an integer divisible by 4. In order for the quantity to be an integer,  $s = \frac{b}{2}$ , where  $b$  is an

integer. Therefore  $\alpha$  is an algebraic integer of the form  $\frac{a+b\sqrt{m}}{2}$  if and only if  $a^2 - mb^2 \equiv 0 \pmod{4}$ .

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

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

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

For each  $a_i$  let  $k_i$  be the degree of the algebraic integer  $a_i$  over  $\mathbb{Q}$ : therefore for any power  $k \geq k_i$ , it can be written as a linear combination of powers of  $a_i$  less than  $k_i$ . Additionally any power of  $\alpha^k$  where  $k \geq n$  can be written as a linear combination of powers of  $\alpha$  multiplied by each of the  $a_i$ . Therefore only a finite number of powers of  $a_0^{m_0} \dots a_{n-1}^{m_{n-1}} \alpha^m$  are needed; the  $a_i$  terms are capped to be lower than  $k_i$  and the  $\alpha$  term is capped to be lower than  $n$ .

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

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

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

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

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

This is the required result.

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

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

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

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

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

Therefore

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

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

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

We expand the product:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11. (c) (TODO)

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

The field  $\mathbb{Q}[\omega]$  has Galois group  $\simeq \mathbb{Z}_p^\times$ , which has cardinality  $p-1$  and so has an element of order 2 (complex conjugation). Therefore  $u$  has  $p-1$  conjugates, which consist of  $(p-1)/2$  elements along with their complex conjugates. Enumerate the conjugates of  $u$  as  $a_1, \dots, a_n, \bar{a}_1, \dots, \bar{a}_n$ .

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

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

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

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

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

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

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

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

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

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

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

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

If  $1 + \sqrt{2}$  were a root of 1, we would have  $(1 + \sqrt{2})^k = 1$  for some  $k$ . However by the Binomial Theorem,  $(1 + \sqrt{2})^k = \sum_{i=0}^k \binom{k}{i} (\sqrt{2})^i$ , which will always

contains a term  $\sqrt{2}$  multiplied by a positive number. Therefore  $1 + \sqrt{2}$  is not a root of 1.

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

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

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

15. (a) Let  $a + b\sqrt{-5}$  be an element of  $\mathbb{Z}[\sqrt{-5}]$ . Then the norm of  $a + b\sqrt{-5}$  is  $(a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$ , where  $a, b \in \mathbb{Z}$ . Since there are no integer solutions  $a, b$  such that  $a^2 + 5b^2 = 2$  or  $a^2 + 5b^2 = 3$ , there can be no element of  $\mathbb{Z}[\sqrt{-5}]$  with a norm of 2 or 3.
15. (b) In  $\mathbb{Z}[\sqrt{-5}]$ ,  $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ . If unique factorization held in  $\mathbb{Z}[\sqrt{-5}]$ , there would be elements  $a, b, c, d \in \mathbb{Z}[\sqrt{-5}]$  such that  $a \cdot b = 2$ ,  $c \cdot d = 3$ ,  $a \cdot d = 1 + \sqrt{-5}$ ,  $b \cdot c = 1 - \sqrt{-5}$ . However by (a), 2 and 3 are irreducible in  $\mathbb{Z}[\sqrt{-5}]$ , meaning they are irreducible elements, and so no  $a, b, c, d$  can exist.
16. We argue in the style of K. Conrad: Trace and Norm, Section 4. Suppose  $\sqrt[4]{3} \in \mathbb{Q}[\alpha]$  where  $\alpha = \sqrt[4]{2}$ ; therefore  $\sqrt{3} = a + b\alpha + c\alpha^2 + d\alpha^3$ . We have the following traces:

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

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

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

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

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

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

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

17 - TODO

18 - TODO

19 - TODO

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

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

$$N(f'(\alpha)) = N(g'(\alpha))N(h(\alpha))$$

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

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

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

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

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

is an integral basis for  $KL$ .

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

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

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

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

**First prove the result for  $n = 1$ .**

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

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

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

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

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

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

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

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

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

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

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

Since  $G$  and  $H$  are free abelian subgroups of rank  $n$ ,  $G \simeq \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$  and since  $H$  is a subgroup of  $G$ , then  $H \simeq I_1 \oplus \dots \oplus I_n$ , where each  $I_i \subseteq \mathbb{Z}$  is an additive subgroup of  $\mathbb{Z}$ . Each  $\mathbb{Z}/I_i$  is finite, having cardinality equal to the generating element of  $I_i$ . Therefore  $G/H$  is finite, having cardinality  $\prod_{i=1}^n |\mathbb{Z}/I_i|$ .

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

Let  $\beta_i$  be 1 projected to the  $i$ th-factor and 0 elsewhere. Then the set of  $\{\beta_i\}$  generate  $G$ . Let  $d_i$  be the minimum element of  $I_i$ , an additive subgroup of  $\mathbb{Z}$ : we show  $\{d_i \beta_i\}$  generates  $H$ . Take  $a \in H$ , and let  $\iota_i(a)$  be the  $i$ th factor of  $a$ , so  $\iota_i(a) \in I_i$ . By choice of  $d_i$ ,  $\iota_i(a) = d_i m$  for some



integer  $m$ , and  $a = \iota_1(a) \oplus \cdots \oplus \iota_n(a) = d_1\beta_1 + \cdots + d_n\beta_n$ . Since  $a$  was chosen arbitrarily, the  $\{d_i\beta_i\}$  generates  $H$ .

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

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

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

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

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

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

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

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

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

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

Reducing terms gives us

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

28. (c) By Theorem 8,  $\text{disc}(a) = -N(f'(\alpha))$  (the negative sign holds since  $n = 3 \neq 0, 1, 4$ ).

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

We now compute the discriminant of  $\alpha$ :

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

This is the required result.

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

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

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

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

29. (a)  $m, n \equiv 1 \pmod{4}$ : The corresponding rings of integers for  $\mathbb{Q}[\sqrt{m}]$  and  $\mathbb{Q}[\sqrt{n}]$  are  $\mathbb{Z}[(1 + \sqrt{m})/2]$  and  $\mathbb{Z}[(1 + \sqrt{n})/2]$  with discriminants  $m$  and  $n$ . By assumption, these discriminants are relatively prime, so Theorem 12, Corollary 1 applies. The field  $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$  thus has an integral basis  $\{1, (\sqrt{m} + 1)/2, (\sqrt{n} + 1)/2, (1 + \sqrt{m} + \sqrt{n} + \sqrt{nm})/4\}$ . By Exercise 23 (c), the discriminant for this basis is  $m^2n^2$ .
29. (b) The rings of integers for  $\mathbb{Q}[\sqrt{m}]$  and  $\mathbb{Q}[\sqrt{n}]$  are  $\mathbb{Z}[(1 + \sqrt{m})/2]$  and  $\mathbb{Z}[\sqrt{n}]$ , with discriminants  $m$  and  $4n$ . Since  $m$  was assumed to be square-free,  $(m, 4n) = 1$ , so Theorem 12, Corollary 1 applies again. The field  $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$  thus has an integral basis  $\{1, (\sqrt{m} + 1)/2, \sqrt{n}, (\sqrt{mn} + \sqrt{n})/2\}$ . By Exercise 23 (c), the discriminant for this basis is  $m^2(4n)^2 = 16m^2n^2$ .
30. Let  $f$  be the monic irreducible polynomial for  $\alpha$  over  $\mathbb{Z}$  and for each  $g \in \mathbb{Z}[x]$ , let  $\bar{g}$  denote the polynomial in  $\mathbb{Z}_3[x]$  obtained by reducing the coefficients mod 3.
30. (a) Show that  $g(\alpha)$  is divisible by 3 in  $\mathbb{Z}[\alpha]$  if and only if  $\bar{g}$  is divisible by  $\bar{f}$  in  $\mathbb{Z}_3[x]$ .
- Suppose  $g(\alpha)$  is divisible by 3. Then  $g(\alpha) = 3m$  for some  $m$  and so  $(g - 3m)(\alpha) = 0$ . Since this is a polynomial in  $\alpha$  and  $f$  is the minimum polynomial,  $f \mid g - 3m$ . Therefore  $\bar{f} \mid \overline{g - 3m} = \bar{g}$ .

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

30. (b) Consider the four algebraic integers:

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

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

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

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

30. (c) Let  $\alpha_i$  from (b) be defined by  $f_i(\alpha)$  (for any fixed  $\alpha$ ). Because  $\alpha_i\alpha_j$  is divisible by 3, by (a),  $\bar{f} \mid \overline{f_i f_j}$ . However,  $\bar{f} \nmid \overline{f_i}^n$  for any power of  $n$  (or else 3 would divide  $\overline{f_i}^n$  which is not the case by (b)), so  $\overline{f_i f_j} \neq \overline{f_i}^n$  for any  $n$ . Therefore, since  $\mathbb{Z}_3[x]$  is a UFD,  $\bar{f}$  has an irreducible factor that does not divide  $\overline{f_i}$  but does divide  $\overline{f_j}$  for all  $j \neq i$ .
30. (d) The result of (c) is that  $\bar{f}$  has at least 4 irreducible factors in  $\mathbb{Z}_3[x]$ . However,  $\bar{f}$  is of degree at most 4, since  $\alpha \in \mathbb{Q}[\sqrt{7}, \sqrt{10}]$ . For there to be at least 4 irreducible factors of  $\bar{f}$  it would imply each are of degree 1, but there are only 3 monic polynomials of degree 1 in  $\mathbb{Z}_3[x]$ :  $x$ ,  $x - 1$ ,  $x - 2$ . Therefore  $\mathbb{A} \cap \mathbb{Q}[\sqrt{7}, \sqrt{10}] \neq \mathbb{Z}[\alpha]$  for any  $\alpha$ .

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

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

32. The fields  $\mathbb{Q}[\sqrt[3]{2}]$  and  $\mathbb{Q}[\omega\sqrt[3]{2}]$  where  $\omega = e^{2\pi i/3}$  both have degree 3 over  $\mathbb{Q}$ , but their composition  $\mathbb{Q}[\omega, \sqrt[3]{2}]$  has degree 6 over  $\mathbb{Q}$ .
33. Let  $\omega = e^{2\pi i/m}$ , where  $m \geq 3$ . We know that  $N(\omega) = \pm 1$  because  $\omega$  is a unit. Show the + sign holds.

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

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

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

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

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

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

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

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

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

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

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

$$N(1 - \omega) = u(1 - \omega)^n$$

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

35. (a) Let  $\omega = e^{2\pi i/m}$  and  $\theta = \omega + \omega^{-1}$ . Then  $\omega^2 - (\omega + \omega^{-1})(\omega) + 1 = 0$  and so  $\omega$  is a root of the polynomial  $x^2 + \theta x + 1$ .  $\omega \notin \mathbb{Q}[\theta]$ , therefore  $\mathbb{Q}[\omega] : \mathbb{Q}[\theta]$  has degree 2.
35. (b) Since  $\theta = \omega + \omega^{-1} \in \mathbb{R}$ , clearly  $\mathbb{Q}[\theta] \subseteq \mathbb{Q}[\omega] \cap \mathbb{R}$ . We therefore have the tower of field extensions  $\mathbb{Q}[\theta] \subseteq \mathbb{Q}[\omega] \cap \mathbb{R} \subsetneq \mathbb{Q}[\omega]$ . By (a),  $[\mathbb{Q}[\omega] : \mathbb{Q}[\theta]] = 2$ . By the Tower Law,  $[\mathbb{R} \cap \mathbb{Q}[\omega] : \mathbb{Q}[\theta]]$  must be a divisor of 2 by distinct from 2 (since  $\omega \notin \mathbb{R}$ ). Therefore the degree must be 1 and so  $\mathbb{R} \cap \mathbb{Q}[\omega] = \mathbb{Q}[\theta]$ .
35. (c) Let  $\sigma$  be the automorphism defined by  $\sigma(\omega) = \omega^{-1}$ . Then  $\sigma(\theta) = \theta$ , and so  $\mathbb{Q}[\theta]$  is in the fixed field of the automorphism  $\sigma$ . As the degree of  $\mathbb{Q}[\omega]$  over  $\mathbb{Q}[\theta]$  is 2, there can be no distinct intermediate field between  $\mathbb{Q}[\omega]$  and  $\mathbb{Q}[\theta]$ .  $\mathbb{Q}[\omega]$  is not in the fixed field of  $\sigma$  and so  $\mathbb{Q}[\theta]$  must be the fixed field of this automorphism.
35. (d) Show that  $\mathbb{A} \cap \mathbb{Q}[\theta] = \mathbb{R} \cap \mathbb{Z}[\theta]$ .

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

This is the required result.

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

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

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

$$\{1, \omega, \omega^{-1}, \omega^2, \omega^{-2}, \omega^3, \dots, \omega^n\} \quad (1)$$

$$\{1, \omega, \theta, \theta\omega, \theta^2, \theta^2\omega, \dots, \theta^{n-1}\omega\} \quad (2)$$

We evaluate the expression  $\theta^k$  using the Binomial Theorem:

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

Therefore

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

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

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

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

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

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

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

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

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

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

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

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

By Exercise 23,

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

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

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

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

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

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

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

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

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

Proceeding in this way we have

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

Finally, we have

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

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

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

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

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

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

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

Since  $f_i(\alpha)/d_i$  and  $f_j(\alpha)/d_j$  are members of the ring  $R$ ,  $f_i(\alpha)f_j(\alpha)/d_i d_j$  must also be a member of the ring  $R$ .  $f_i(\alpha)f_j(\alpha)$  has order  $i + j$ . Since

this is  $< n$ , this element by be generated by the basis elements of order  $\leq i + j$ . Let  $a_k$  be the integers that generate this element. Then

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

$$\begin{aligned}\text{Tr}(\alpha) &= \alpha + \omega\alpha + \omega^2\alpha = \alpha(\omega^2 + \omega + 1) = 0 \\ \text{Tr}(\alpha^2) &= \alpha^2 + \omega^2\alpha^2 + \omega\alpha^2 = \alpha^2(\omega^2 + \omega + 1) = 0\end{aligned}$$

With these in hand we now have

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

By the additive linearity of trace, we have

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

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

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

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

41. (c) Write  $m$  as  $hk^2$ . Then  $(\alpha^2/k)^3 = m^2/k^3 = (h^2k^4)(k^3) = h^2k$ , and so  $\alpha^2/k$  is the root of the polynomial  $f(x) = x^3 - h^2k$ , and so  $\alpha^2/k \in R$ .
41. (d) Suppose  $m \equiv \pm 1 \pmod{9}$ . Let  $\beta = (\alpha \mp 1)^2/3$ . Show that

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

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

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

Moving the terms around, we have the required result:

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

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

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

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

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

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

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

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

Next we have

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

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

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

This is the required result.

41. (f) We have  $\text{disc}(\alpha) = -27m^2$ . By Exercise 40(a),  $d_2^2 \text{disc}(R) = \text{disc}(\alpha) = -27m^2 = -27h^2k^4$ . We know  $k \mid d_2$  so write  $d_2 = jk$ , thus  $j^2k^2 \text{disc}(R) = -27h^2k^4$  and so  $j^2 \text{disc}(R) = -27h^2k^2 = -27mh$ . By assumption  $h$  is square-free, so  $j^2 \mid -27m$ , implying either  $j \mid 3$  or  $j \mid m$ . Therefore  $j \mid 3m$ .
41. (g) Letting  $p$  be a prime such that  $p \neq 3$ ,  $p \mid m$ ,  $p^2 \mid m$ . Let  $p \mid d_2$ , and write  $d_2 = pj$ . Therefore if  $(\alpha^2 + a\alpha + b)/d_2 \in R$ , then

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Therefore if  $3 \nmid m$  and  $m \not\equiv \pm 1 \pmod{9}$ ,  $3 \nmid d_2$ .

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

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

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

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

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

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

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

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

Therefore,

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

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

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

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

43. (c) Let  $a$  be squarefree and not equal to  $\pm 1$ . Let  $\alpha$  be a root and  $d_1, d_2, d_3, d_4$  be as in Theorem 13. Prove that if  $4^4a + 5^5$  is squarefree then  $d_1 = d_2 = 1$  and  $d_3d_4 \mid a^2$ .

By exercise 40,

$$\text{disc}(\alpha) = 5^5a^4 + 4^4a^5 = a^4(5^5 + 4^4a) = (d_1d_2d_3d_4)^2\text{disc}(R)$$

Here  $d_1d_2 \mid d_3$ ,  $d_1d_2 \mid d_4$ , and  $d_1d_3 \mid d_4$ . Therefore  $d_1$  and  $d_2$  both have 6 factors represented in the  $\text{disc}(\alpha)$  expression which is impossible unless they are both 1. Since  $5^5 + 4^4a$  is squarefree,  $(d_3d_4)^2$  must divide  $a^4$  and so  $d_3d_4 \mid a^2$ .

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

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

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

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

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

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

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

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

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

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

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

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

44. (b) TODO

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

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

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

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

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

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

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

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

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

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

Plugging values in gives:

$$\begin{aligned} n = 2 &= -(2^2b - a^2) = a^2 - 4b \\ n = 3 &= -(27b^2) + a^32^2 = -27b^2 + 4a^3 \\ n = 4 &= b^34^4 - a^43^3 = 256b^3 - 27a^4 \\ n = 5 &= b^45^5 + a^54^4 \end{aligned}$$

These agree with the known values of these polynomials.

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

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

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

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

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

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

Multiplying through by  $n^n$  gives us:

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

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

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

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

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



## Chapter 3

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

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

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

Since  $G$  is a free abelian group of rank  $n$ ,

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

Therefore

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

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

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

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

7. If  $I + J = 1$  then there exist  $\alpha \in I, \beta \in J$  such that  $\alpha + \beta = 1$ . Raising both powers to the  $m + n$ th power, we have  $(\alpha + \beta)^{m+n} = 1^{m+n} = 1$ . By the binomial theorem,  $(\alpha + \beta)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n-k}{k} \alpha^{m+n-k} \beta^k$ . If  $k < n$ , this element is a member of  $I^m$  (as  $\alpha^{n+\text{positive}} \in I^m$ ); otherwise this element is a member of  $J^n$ . Therefore  $(\alpha + \beta)^{m+n} \in I^m + J^n$ .
8. (a) Suppose  $I = (2, x)$  was generated by some  $\alpha \in I$ . Therefore there are  $\beta, \gamma \in \mathbb{Z}[x]$  such that  $\alpha\beta = 2$  and  $\alpha\gamma = x$ . Since  $\alpha\beta = 2$ , the rank of  $\alpha$  must be 0;  $\alpha \in \mathbb{Z}$ . The only option is  $\alpha = 2$  (since  $1 \notin I$ ). However 2 is not a factor of  $x$  in  $\mathbb{Z}[x]$ . Therefore the ideal  $(2, x)$  is not principal in  $\mathbb{Z}[x]$ .
8. (b) Let  $f, g \in \mathbb{Z}[x]$  and let  $m, n$  be the gcd of the coefficients of  $f$  and  $g$  respectively. Prove  $mn$  is the gcd of the coefficients of  $fg$ .

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

$$f = m(a_0 + a_1x + \dots + a_jx^j) \tag{3}$$

$$g = n(b_0 + b_1x + \dots + b_kx^k) \tag{4}$$

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

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

we know that  $mn \mid d$ .

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

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

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

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

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

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

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

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

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

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

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

$$5^2 \quad (1)$$

$$5(\alpha^2 + 3\alpha - 1) \quad (2)$$

$$5(\alpha + 2) \quad (3)$$

$$(\alpha + 2)(\alpha^2 + 3\alpha - 1) = \alpha^3 + (3 + 2)\alpha^2 + (-1 + 6)\alpha - 2 = 5(\alpha^2 + \alpha) \quad (4)$$

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

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

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

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

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

The ring homomorphism  $\psi$  from  $\mathbb{Z}[x] \rightarrow S$  defined by  $\psi(x) = \alpha$  is a surjective. Let  $\beta \in S$ ;  $\beta = m_0 + m_1\alpha + m_2\alpha^2$  for integers  $m_0, m_1, m_2$ , so  $f(m_0 + m_1x + m_2x^2) = \beta$ . Therefore the surjective  $\psi$  induces a surjection  $\hat{\psi}$  on the quotient rings:

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

This utilizes the following lemma on ring homomorphisms:

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

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

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

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

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

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

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

12. (e) Suppose  $(5, \alpha^2 + 3\alpha - 1) = S$ . Then by (a),  $5S = (5, \alpha + 2)S$ ; however,  $\alpha + 2 \notin 5$ , so  $S/(5, \alpha^2 + 3\alpha - 1)$  must be a field of order 25.
13. (a) Let  $S = \mathbb{Z}[\alpha]$ ,  $\alpha^3 = \alpha + 1$ . Verify  $23S = (23, \alpha - 10)^2(23, \alpha - 3)$ .  
Let  $I = (23, \alpha - 10)^2(23, \alpha - 3)$ . The generators of  $I$  are:

$$23^3 \tag{1}$$

$$23^2(\alpha - 3) \tag{2}$$

$$23^2(\alpha - 10) \tag{3}$$

$$(\alpha - 10)^2(\alpha - 3) = -23(\alpha^2 - 7\alpha + 13) \tag{4}$$

$$23(\alpha - 10)^2 = 23(\alpha^2 - 20\alpha + 100) \tag{5}$$

$$23(\alpha - 10)(\alpha - 3) = 23(\alpha^2 - 13\alpha + 30) \tag{6}$$

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

$$(4) + (5) = 23(-13\alpha + 87) \tag{7}$$

$$2 \cdot (6) - (5) + (4) = 23\alpha + 53 \cdot 23 \tag{8}$$

$$13 \cdot (8) - (7) = 23 \cdot 602 \tag{9}$$

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

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

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

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

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

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

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

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

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

$$\begin{aligned} N_K^L(I) &= R \cap (Q_1^{ef} \cdots Q_r^{ef})S \\ &= R \cap (Q_1 \cdots Q_r)^{ef}S \\ &= R \cap P^f S \\ &= P^f \end{aligned}$$

□

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

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

14. (d)

$$\begin{aligned}
N_K^L(IJ) &= R \cap \prod_{\sigma \in G} \sigma(IJ) \\
&= R \cap \prod_{\sigma \in G} \sigma(I) \prod_{\sigma \in G} \sigma(J) \\
&= R \cap \left( \prod_{\sigma \in G} \sigma(I) \right) \left( \prod_{\sigma \in G} \sigma(J) \right) \\
&= R \cap (N_K^L(I) N_K^L(J)) \\
&= N_K^L(I) N_K^L(J)
\end{aligned}$$

The final equality holds since  $N_K^L(I)$  and  $N_K^L(J)$  are ideals in  $R$ .

14. (e) If  $\beta \in N_K^L((\alpha))$ , then  $\beta = \sigma_1(\alpha) \cdots \sigma_k(\alpha) \gamma = N_K^L(\alpha) \gamma$ ; since  $\beta \in R$  and  $N_K^L(\alpha) \in R$ ,  $\gamma$  must also be in  $R$ . Thus  $N_K^L((\alpha))$  is the ideal generated by  $N_K^L(\alpha)$ .
15. (a) Show for three fields  $K \subset L \subset M$ , that  $N_K^M(I) = N_K^L N_L^M(I)$  for an ideal  $I \subset \mathbb{A} \cap M$ .

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

$$N_K^M(U) = P^{f(U|P)} = P^{f(U|S)f(S|P)} = N_K^L N_L^M(U)$$

If  $I = U_1 \cdots U_r$ , then

$$N_K^M(I) = \prod_{i=1}^r N_K^M(U_i) = \prod_{i=1}^r N_K^L N_L^M(U_i) = N_K^L N_L^M(I)$$

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

$$\begin{aligned}
N_K^M((\alpha)) &= (N_K^M(\alpha)) && \text{(exercise 14. (e))} \\
&= (N_K^L(N_L^M(\alpha))) && \text{Definition of relative norm} \\
&= (N_K^L(\alpha^n)) && \alpha \in L \text{ and } L \subset M \\
&= (N_K^L(\alpha))^n && \text{Factorization of ideals}
\end{aligned}$$

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

$$\begin{aligned}
N_K^M((\alpha)) &= N_K^L N_L^M((\alpha)) && \text{part (a)} \\
&= N_K^L((\alpha^n)) && \text{Exercise 14. (e), } M \text{ is normal over } L \\
&= N_K^L((\alpha))^n && \text{Factorization of ideals} \\
&= N_K^L((\alpha))^n && \text{Exercise 14. (d)}
\end{aligned}$$

We therefore have

$$(N_K^L(\alpha))^n = N_K^L((\alpha))^n$$

and conclude that  $N_K^L(\alpha) = N_K^L((\alpha))$ .

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

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

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

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

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

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

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

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

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

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

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

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

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

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

and

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

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

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

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

17. (c) By 16. (b), the order of  $P$  divides the order of  $Q$  multiplied by  $f(Q|P)$ ; therefore  $3 \mid d_Q 11$  and so  $3 \mid d_Q$ . Therefore  $Q$  must also not be a principal ideal.
17. (d) Suppose  $2 = \alpha\beta$  in  $\mathbb{Z}[\omega]$  and neither  $\alpha$  nor  $\beta$  is a unit, therefore  $2\mathbb{Z}[\omega] = (\alpha)(\beta) = (2, \theta)(2, \bar{\theta})$ . By the uniqueness of ideal factorization,  $(2, \theta)$  must be principal; however, we have seen that this is not the case in part (c). This is a contradiction; therefore either  $\alpha$  or  $\beta$  must be a unit.
18. (a) Show  $\text{disc}(r\alpha_1, \alpha_2, \dots, \alpha_n) = r^2 \text{disc}(\alpha_1, \dots, \alpha_n)$ .

Writing the discriminant as the determinant of each of the  $\sigma_j$  conjugates of  $\alpha_n$ , we have:

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

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

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



18. (b) Let  $\beta$  be a linear combination of  $\alpha_2, \dots, \alpha_n$  with coefficients in  $\mathbb{Q}$ . Show  $\text{disc}(\alpha_1 + \beta, \alpha_2, \dots, \alpha_n) = \text{disc}(\alpha_1, \dots, \alpha_n)$ .
- For all  $\sigma_k$ ,  $\sigma_k(\alpha_1 + \beta) = \sigma_k(\alpha_1) + \sigma_k(\beta)$ . If  $\beta = p_2\alpha_2 + \dots + p_n\alpha_n$ , then  $\sigma_k(\beta) = p_2\sigma_k(\alpha_2) + \dots + p_n\sigma_k(\alpha_n)$  for  $p_i \in \mathbb{Q}$ . Writing  $\text{disc}(\alpha_1 + \beta, \alpha_2, \dots, \alpha_n)$  in matrix form, the  $k$ -th row of the first column has the form  $\sigma_k(\alpha_1) + p_2\sigma_k(\alpha_2) + \dots + p_n\sigma_k(\alpha_n)$ .
- Subtracting a column times a linear factor has no effect on the determinant of the matrix, so by subtracting  $p_i$  multiplied by column  $i$  from the first column for each  $i$ , we see  $\text{disc}(\alpha_1 + \beta, \alpha_2, \dots, \alpha_n) = \text{disc}(\alpha_1, \dots, \alpha_n)$ .
19. Let  $K$  and  $L$  be number fields,  $K \subset L$ , and let  $R = \mathbb{A} \cap K$ ,  $S = \mathbb{A} \cap L$ . Let  $P$  be a prime of  $R$ .
19. (a) Show that if  $\alpha \in S$ ,  $\beta \in R$ , and  $\alpha\beta \in PS$ , then either  $\alpha \in PS$  or  $\beta \in P$ .
- Let  $\psi : S/PS \rightarrow P/R$  be the homomorphism defined by taking a coset in  $S/PS$  to the corresponding coset in  $P/R$ . If  $\alpha\beta \in PS$ , then  $\psi(\alpha\beta) = 0$ . Since  $P$  is maximal,  $R/P$  is an integral domain, so as  $\psi$  is a homomorphism into  $R/P$  either  $\psi(\alpha) = 0$ , or  $\psi(\beta) = 0$ ; equivalently,  $\alpha \in PS$  or  $\beta \in P$ .
22. ( $\alpha^5 = 2\alpha + 2$ ) Let  $\alpha^5 = 2\alpha + 2$  and  $R = \mathbb{A} \cap \mathbb{Z}[\alpha]$ . By Exercise 43,  $\text{disc}(\alpha) = 4^4 \cdot (-2)^5 + 5^5 2^4 = 2^4 \cdot 3 \cdot 13 \cdot 67$ .
- As 2 is the prime with power greater than 1 dividing  $\text{disc}(\alpha)$ , we focus on its factorization. (If  $\text{disc}(\alpha)$  were not the whole ring of integers, the order  $|R/\mathbb{Z}[\alpha]|$  would be divisible by a power of 2.)
- By 43 (d),  $\alpha + 1$  is a unit, so we can determine the factorization of 2 by factoring the minimum polynomial of  $\alpha + 1$  over  $\mathbb{Q} \bmod 2$ . Sage gives this as  $x^5 - 5x^4 + 10x^3 - 10x^2 + 3x - 1$ ; mod 2 this is  $x^5 + x^4 + x + 1 = (x - 1)^5$ ; therefore the prime 2 has the factorization  $2R = (2, \alpha)^5$  and the inertial degree of the primes lying over 2 is 1. Using the improvement of Theorem 24,  $2^4 \mid \text{disc}(R)$ ; therefore  $\text{disc}(R) = \text{disc}(\alpha)$  and  $\mathbb{A} \cap \mathbb{Z}[\alpha] = \mathbb{Z}[\alpha]$ .
22. ( $\alpha^5 = 2\alpha^4 + 2$ ) We proceed in a similar method to the previous case: we calculate the discriminant of  $\alpha$ , take the prime factors that have square terms, and factor the minimum polynomial of  $\alpha^4 + 1$  (a unit by 44 (d)) modulo those prime factors.
- By 44 (a),  $\text{disc}(\alpha) = (-2)^3(4^4(-2)^5 + 5^5(-2)) = 2^4 \cdot 3 \cdot 29 \cdot 83$ , so again we only need to focus on  $p = 2$ . Sage gives the minimum polynomial of  $\alpha^4 + 1$  as  $x^5 - 21x^4 + 10x^3 - 10x^2 + 5x - 1$ ; mod 2 this is  $x^5 + x^4 + x + 1 = (x - 1)^5$ , so  $2R = (2, \alpha^4)^5$  and so  $\sum f_i = 1$  and by the improvement of Theorem 24,  $2^4 \mid \text{disc}(R)$ . Therefore  $\text{disc}(\alpha) = \text{disc}(R)$  and  $\mathbb{A} \cap \mathbb{Z}[\alpha] = \mathbb{Z}[\alpha]$ .
24. Let  $R, K, S, L$  be as usual. A prime  $P \subset R$  is *totally ramified* if  $PS = Q^n$ ,  $n = [L : K]$ .
24. (a) Suppose  $P$  is totally ramified in  $S$ ; then  $PS = Q^n$ . Let  $M$  be an extension field such that  $K \subset M \subset L$  with  $\mathbb{A} \cap M = T$ . and  $U$  be a prime of  $M$

lying over  $P$ . Then  $U \subset Q$  and  $US = Q^{[M:L]}$ . Since the ramification degree is multiplicative in towers,  $[L : K] = e(Q|P) = e(Q|U)e(U|P) = [L : M]e(U|P)$ ; therefore  $e(U|P) = [M : K]$  and so  $P$  is totally ramified in  $M$ .

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

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

26. Let  $\alpha = \sqrt[3]{m}$  where  $m$  is a cubefree integers,  $K = \mathbb{Q}[\alpha]$ ,  $R = \mathbb{A} \cap K$ .

26. (a) Let  $p$  be a prime  $\neq 3$  and  $p^2 \nmid m$ . By Exercise 2.41,  $\text{disc}(\alpha) = -27m^2$ , so  $p \nmid \text{disc}(\alpha)$ . Therefore  $p \nmid |R/R[\alpha]|$  and so the prime decomposition of  $p$  in  $R$  is determined by factoring the polynomial  $x^3 - m \pmod{p}$ .

26. (b) Let  $p \neq 3$  and suppose  $p^2 \mid m$  and write  $m = hk^2$ . We set  $\gamma = \alpha^2/k$ . Note  $\gamma^2 = h\alpha$ .

By Exercise 2.41, There are two possible integral bases for  $R$ : either  $\{1, \alpha, \alpha^2/k\}$  ( $m \not\equiv \pm 1 \pmod{9}$ ) or  $\{1, \alpha, (\alpha^2 \pm k^2 + k^2)/3k\}$  ( $m \equiv \pm 1 \pmod{9}$ ).

$|R/R[\gamma]| = h$  in the first scenario,  $|R/R[\gamma]| = 3h$  in the second.  $h$  is squarefree and so  $p \nmid |R/R[\gamma]|$  and so the prime decomposition of  $p$  is determined by factoring the minimal polynomial for  $\gamma \pmod{p}$ .  $\gamma^3 = \alpha^6/k^3 = m^2/k^3 = h^2k$  so the minimal polynomial for  $\gamma$  is  $x^3 - h^2k$ .

Since  $p \mid k$ , this reduces to factoring the equation  $x^3 \pmod{p}$  and so there is one prime lying over  $p$  with a ramification degree of 3; therefore  $pR = (p, \gamma)^3 = (p, \alpha^2/k)^3$ .

26. (c) If  $m \not\equiv \pm 1 \pmod{9}$ , the integral basis for  $R$  is  $\{1, \alpha, \alpha^2/k\}$  and so  $|R/R[\gamma]| = h$ . We split into two cases, one where  $3 \mid k$ , one where  $3 \nmid k$ .

**Case 1:**  $3 \mid h$ : If  $3 \mid h$  then  $(3, \alpha)^3$  has generators  $(27, 3\alpha^2, 9\alpha, m)$ . Because  $m$  is cubefree,  $9 \nmid m$ , so  $\text{gcd}(m, 27) = 3 \in (3, \alpha)$ . Therefore  $3R = (3, \alpha)^3$ .

**Case 2:**  $3 \nmid h$ : By Theorem 27, the prime decomposition of  $3R$  can be determined by factoring  $x^3 - h^2k \pmod{3}$ ;  $\pmod{3}$ ,  $x^3 - h^2k \equiv (x - h^2k)^3 \pmod{3}$  and so 3 is totally ramified in  $R$  with  $3R = (3, \gamma - h^2k)^3$ .

26. (d) If  $m = 10$ , then the integral basis for  $R$  is  $\{1, \alpha, (\alpha^2 + \alpha + 1)/3\}$ . Taking  $\beta = (\alpha - 1)^2/3$  we note  $(\alpha^2 + \alpha + 1)/3 - \alpha = \beta$  and  $\beta^2 = 2(\alpha^2 + \alpha + 1)/3 - 5$ . Therefore, we have the series of equivalences (using the transformations

developed in Exercise 3.18):

$$\begin{aligned}
\text{disc}(R) &= \text{disc}\left(1, \alpha, \frac{\alpha^2 + \alpha + 1}{3}\right) \\
&= \text{disc}\left(1, \frac{\alpha^2 + \alpha + 1}{3} - \alpha, \frac{\alpha^2 + \alpha + 1}{3}\right) \\
&= \frac{1}{4} \text{disc}\left(1, \beta, \frac{2(\alpha^2 + \alpha + 1)}{3}\right) \\
4\text{disc}(R) &= \text{disc}\left(1, \beta, \frac{2(\alpha^2 + \alpha + 1)}{3} - 5\right) \\
&= \text{disc}(1, \beta, \beta^2)
\end{aligned}$$

By Exercise 2.27,  $\text{disc}(\beta) = |R/R[\beta]|^2 \text{disc}(R)$  so we conclude that  $|R/R[\beta]| = 2$  and so can apply Theorem 27.

By Exercise 2.41, the minimal polynomial for  $\beta$  if  $m = 10$  is  $x^3 - x^2 + 7x - 3$ ; mod 3, this reduces to  $x(x^2 - 2x + 1) = x(x - 1)^2$ . Therefore by Theorem 27, the prime decomposition of  $3R = (3, \beta)(3, \beta - 1)^2$ .

(Not done: consider for general  $m \equiv \pm 1 \pmod{9}$ .)

26. (e) When  $m \equiv \pm 1 \pmod{9}$ , an integral basis of  $R$  is  $\{1, \alpha, (\alpha^2 \pm k^2 \alpha + k)/3k\}$ ; we have  $|R/R[\alpha]| = 3h$  and by Exercise 2.27 and 2.41,  $\text{disc}(\alpha) = |R/R[\alpha]|^2 \text{disc}(R) = -27m^2$ , so  $\text{disc}(R) = -3h^2k^2$ . Since  $m \equiv \pm 1 \pmod{9}$ ,  $3 \nmid h$  (otherwise  $m \equiv 0, 3, 6 \pmod{9}$ ) and  $3 \nmid k$  (otherwise  $m \equiv 0 \pmod{9}$ ).

By exercise 21,  $p^{n-\sum f_i} \mid \text{disc}(R)$  and so  $\sum f_i = 2$ . Since  $\sum f_i e_i = 3$  we must have at least 2 prime ideals lying over 3. Since  $3 \mid \text{disc}(R)$ , by the converse to Theorem 24,  $3R$  must be ramified with degree greater than 1. Since the sum of the inertial degrees is also greater than 1, the only possibility satisfying both conditions is that  $3R = P^2Q$  for prime ideals  $P$  and  $Q$ , with both  $P$  and  $Q$  having inertial degree 1.

27. Let  $\alpha^5 = 5(\alpha + 1)$ . From Exercise 2.43, we know  $\text{disc}(\alpha) = 4^4(-5)^5 + 5^5(-5)^4 = 5^5(5^4 - 4^4) = 5^5 \cdot 3^2 \cdot 41$ . This polynomial has the form in exercise 28 ( $p = 5, r = 1$ ), and so by Exercise 3.28 (c),  $5^4 \mid \text{disc}(R)$ , therefore 3 is the only square prime dividing  $|\text{disc}(R)/\text{disc}(R[\alpha])|$  and for all other primes, Theorem 27 applies.

$x^5 - 5x - 5 \equiv x^5 + x + 1 \equiv (x^2 + x + 1)(x^3 + x^2 + 1) \pmod{2}$ , so by Theorem 27,  $2R = (2, \alpha^2 + \alpha + 1)(2, \alpha^3 + \alpha^2 + 1)$ .

I also worked this problem out using the fact that  $\alpha + 1$  as a unit; its minimum polynomial over  $\mathbb{Q}$  is  $x^5 - 5x^4 + 10x^3 - 10x^2 + 1$  and works for any prime (including  $p = 3$ ). In particular for  $p = 2$ ,  $x^5 - 5x^4 + 10x^3 - 10x^2 + 1 \equiv x^5 + x^4 + 1 \pmod{2}$ . This polynomial splits into two factors  $x^2 + x + 1$  and  $x^3 + x + 1$  over  $\mathbb{Z}_2$ ; therefore  $2R = (2, (\alpha + 1)^2 + \alpha)(2, (\alpha + 1)^3 + \alpha) = (2, \alpha^2 + \alpha + 1)(2, \alpha^3 + \alpha^2 + 1)$  which matches the other solution.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**44 (d):**  $\text{disc}(\alpha) = a^4[(4a)^4 + 5^5] = (d_3 d_4)^2 \text{disc}(R)$ . As in the previous case,  $p^6 \mid (d_3 d_4)^2 \text{disc}(R)$  and so  $a^2 \mid (4a)^4 + 5^5$ , contradicting the assumption that this quantity is squarefree.

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

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

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

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

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

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

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

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

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

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

Taking  $r = 4$  and  $p = 5$ , we see  $4^5 + 2 \cdot 4 - 2 = 130 \equiv 0 \pmod{5}$ . Letting  $\psi$  be the homomorphism from (a), we observe that if there were  $x, y, z$  such that  $x^4 + y^4 + z^4 = \alpha$ , we would have  $\psi(x^4 + y^4 + z^4) = \psi(\alpha) = 4$ . However in  $\mathbb{Z}_5$ ,  $x^4 \equiv 1$  for all  $x$  so  $\psi(x^4 + y^4 + z^4) = \psi(x)^4 + \psi(y)^4 + \psi(z)^4 = 3 \not\equiv 4$ . Therefore there are no  $x, y, z \in \mathbb{Q}[\alpha]$  such that  $x^4 + y^4 + z^4 = \alpha$ .

30. (a) Let  $f$  a nonconstant polynomial  $f(x)$  over  $\mathbb{Z}$  with  $f(0) = 1$ . Suppose there are only a finite number of primes such that  $f(x) \equiv 0 \pmod{p}$  has a root; then there must be some largest prime  $P'$  for which a root exists. Consider the prime divisors of  $f(P'!)$ : for every prime  $p$ ,  $f(P'!) \equiv 1 \pmod{p}$ , so it must have a prime divisor  $q > P'$ . However, then  $f(P'!) \equiv 0 \pmod{q}$  contradicting that there were only a finite number of primes such that  $f$  had a root.

Next, suppose  $f(x)$  is a nonconstant polynomial over  $\mathbb{Z}$ . If  $f(0) = 0$  then  $f(0) = 0$  and so  $f$  has a root for all primes  $p$ . Suppose  $f(0)$  is nonzero, then the polynomial  $g(x) = f(f(0)x)/f(0)$  is also in  $\mathbb{Z}$  (as  $f(0)$  must divide each coefficient).  $g(x)f(0) \equiv f(f(0)x) \pmod{p}$ ; as  $\mathbb{Z}[x]$  is an integral domain,  $g(x)$  has a root mod  $p$  if and only if  $f(x)$  has a root. As  $g(0) = 1$  it has a root for infinitely many primes and so does  $f(x)$ .

30. (b) Let  $K = \mathbb{Q}[\alpha]$  be a number field and take  $f(x)$  be the minimal polynomial for  $\alpha$ . Let  $R = \mathbb{A} \cap K$  and consider the value  $|R : \mathbb{Z}[\alpha]|$ . For any prime  $p \nmid |R : \mathbb{Z}[\alpha]|$  such that  $f(x)$  has a root  $r \pmod{p}$ , by Theorem 27, there is a prime ideal of the form  $(p, \alpha - r)$  lying above  $P$ . The inertial degree of this prime ideal is 1 (as  $x - r$  has degree one). As  $|R : \mathbb{Z}[\alpha]|$  is a finite value, only finitely many primes divide it. However  $f$  has a root for infinitely many primes  $p$ . Therefore there are infinitely many primes  $p$  such that  $f(P|p) = 1$ .

30. (c) Take the polynomial  $x^m - 1$ . If for any prime  $x^m - 1 \equiv 0 \pmod{p}$  has a solution, then  $x^m \equiv 1 \pmod{p}$  and so  $m \mid p - 1$ ; thus there exists  $k$  such that  $km = p - 1$  and so  $1 \equiv p \pmod{m}$ . By (a) the polynomial  $x^m - 1$  has roots for infinitely many primes  $p$ , so for any  $m$ , an infinite number of primes  $p$  exist such that  $p \equiv 1 \pmod{m}$ .

30. (d) Let  $L$  and  $K$  be number fields. Take  $M$  the normal closure of  $K$ . Only finitely many primes are ramify in  $M$ ; however by (b) there are an infinite number of primes  $p$  such that  $f(Q|p) = 1$  for  $Q$  a prime ideal lying over  $p$ . Taking away the primes that ramify, in  $M$  these primes have inertial degree 1 and ramification index 1, so they must split completely. As  $L$  is an intermediate field and inertial degree/ramification index is multiplicative, these primes must also have inertial degree/ramification index equal to 1 in  $L$ . Therefore there are an infinite number of primes  $p$  that split into  $[L : K]$  distinct factors in the intermediate field  $L$ .

30. (e) TODO

31. (a) For fractional ideals  $A, B$ , let  $A = \alpha I$  and  $B = \beta I$ . For  $r \in A, s \in B$ , then  $r = \alpha i$  and  $s = \beta j$  where  $i \in I, j \in J$ . Therefore  $rs = \alpha i \beta j = \alpha \beta i j \in \alpha \beta I J$ . Conversely assume  $c \in \alpha \beta I J$  then  $c = \alpha \beta c'$  where  $c' \in I J$ , so  $c'$  has the form  $r s$  for  $i \in I, j \in J$ . Therefore  $c = \alpha i \beta j$  and so is a member of  $\alpha I \beta J = AB$ . Therefore the product of fractional ideals is independent of the representation of its factors.

31. (b) Let  $A = \alpha I$  for  $\alpha \in K, I \subset R$ ; we will show  $A^{-1}A = R$ . By Theorem 15 there is some  $J$  such that  $IJ$  is principal, generated by some  $\beta \in R$ .

**Claim:**  $A^{-1} = \alpha^{-1} \beta^{-1} J$

Take  $a \in A^{-1}$ . We have the following series of inclusions:

$$\begin{aligned} aA = a\alpha I &\subset R \\ a\alpha I J &\subset R J = J \\ a\alpha(\beta) &\subset J \\ (a) &\subset \alpha^{-1} \beta^{-1} J \end{aligned}$$

Therefore  $a \in \alpha^{-1} \beta^{-1} J$ . Conversely  $\alpha^{-1} \beta^{-1} J \subset A^{-1}$  as  $\alpha^{-1} \beta^{-1} I J = (1) \subset R$ . This proves the claim.

Using the claim,  $AA^{-1} = \alpha^{-1} \alpha \beta^{-1} I J = \beta^{-1}(\beta) = (1) = R$ .

31. (c) Let  $A$  be a fractional ideal of the form  $\alpha I$  for  $\alpha \in K, I \subset R$ . As  $K$  is the field of fractions of  $R$ ,  $\alpha = r/s$  for some  $r \in R, s \in S$ .

Let  $I$  have the factorization into prime ideals  $P_1^{e_1} \dots P_k^{e_k}$ ,  $(r)$  have factorization  $P_{k+1}^{e_{k+1}} \dots P_m^{e_m}$ , and  $(s)$  have factorization  $P_{m+1}^{e_{m+1}} \dots P_r^{e_r}$ ; combining the terms and removing the primes raised to the 0th power, gives the prime factorization of  $A$  as

$$A = P_1^{e_1} \dots P_k^{e_k} P_{k+1}^{e_{k+1}} \dots P_m^{e_m} P_{m+1}^{-e_{m+1}} \dots P_r^{-e_r}$$

Given two different factorizations of  $A$ ,  $A = P_1^{e_1} \dots P_k^{e_k} = Q_1^{e'_1} \dots Q_j^{e'_j}$ , we have  $R = (P_1^{e_1} \dots P_k^{e_k})^{-1} Q_1^{e'_1} \dots Q_j^{e'_j} = (P_1^{-e_1} \dots P_k^{-e_k}) Q_1^{e'_1} \dots Q_j^{e'_j}$ . Since this product is equal to  $R$ , the  $P_i$  and  $Q_i$  terms must all cancel showing that the factorizations were identical.

31. (d-f) TODO

33. Let  $A$  be an additive subgroup of  $L$ . Define

$$A^{-1} = \{\alpha \in L : \alpha A \subset S\}$$

and

$$A^* = \{\alpha \in L : \text{Tr}_K^L(\alpha A) \subset R\}$$

33. (a) Show  $A^{-1}$  is an  $S$ -submodule of  $L$  and  $A^*$  is an  $R$ -submodule.

First note  $A^{-1}$  is an additive subgroup of  $L$ : if  $\alpha, \beta \in A^{-1}$ ,  $\alpha A \subset S$  and  $\beta A \subset S$  so  $(\alpha + \beta)A \subset S$ . To show  $A^{-1}$  is an  $S$ -submodule of  $L$ , take  $\alpha \in A^{-1}$ ,  $s \in S$ ,  $a \in A$ ; as  $\alpha a \in S$  then  $\alpha as \in S$  so  $\alpha sA \subset S$  and so  $A^{-1}$  is an  $S$ -submodule.

As the trace property is additive,  $A^*$  is an additive subgroup of  $L$ . To show  $A^*$  is an  $R$ -submodule take  $\alpha \in A^*$  and  $r \in R$ ; so  $\text{Tr}_K^L(\alpha A) \subset R$ . As  $\text{Tr}_K^L(r\alpha A) = r\text{Tr}_K^L(\alpha A)$ ,  $r\alpha \in A^*$  and so  $A^*$  is an  $R$ -submodule.

Finally given  $\alpha \in A^{-1}$ ; given  $a \in A$ ,  $\alpha a \in S$ . The relative trace or norm of an element in  $L$  is a member of the base field  $K$ ; as the relative trace is just the sum of the diagonal entries of the permutation matrix of  $\alpha a$ ,  $\text{Tr}_K^L(\alpha a) \in R$ .

33. (b) Let  $A$  be a fractional ideal; then from the definition in exercise 31,  $A = \alpha I$ ,  $\alpha \in L$ ,  $I$  an ideal of  $S$ . Take  $s \in S$ ; then any element of  $sA$  has the form  $s\alpha k$ , for  $k \in I$ . As  $I$  is an ideal,  $sk \in I$  and so  $s\alpha k \in A$ .  $\alpha^{-1} \in A^{-1}$  as  $\alpha^{-1}A = \alpha^{-1}\alpha I = I \subset S$ .

To prove the converse, suppose  $SA = A$  and  $A^{-1} \neq \{0\}$ . Take some  $\alpha^{-1} \neq 0 \in A^{-1}$  so that  $\alpha^{-1}A \subset S$ . Given  $a \in A$ ,  $\alpha^{-1}a \in S \implies a \in \alpha S$ ; therefore  $a = \alpha s$  for  $s \in S$ . Let  $I = \{x : \alpha x \in A\}$ . Take  $a, b \in A$ ; then  $a = \alpha x_0$ ,  $b = \alpha x_1$  ( $x_0, x_1 \in I$ ); as  $A$  is additive  $\alpha(x_0 + x_1) \in A \implies x_0 + x_1 \in I$ ; therefore  $I$  is an additive subset of  $S$ . Finally take  $s \in S$ ,  $x \in I$ ; as  $SA = A$ , then  $s\alpha x \in A$  and so  $s\alpha x \in A$  and so  $sx \in I$ .  $I$  is therefore an ideal, and so  $A = \alpha I$  is a fractional ideal.

33. (c) Define  $\text{diff } A = (A^*)^{-1}$ .  $A$  and  $B$  are subgroups of  $L$  and  $I$  is a fractional ideal of  $S$ .

$A \subset B \implies A^{-1} \supset B^{-1}$ : take  $\beta^{-1} \in B^{-1}$ ; then  $\beta^{-1}A \subset \beta^{-1}B \subset S$  and so  $\beta^{-1} \in A^{-1}$ .

$A \subset B \implies A^* \supset B^*$ : take  $\beta \in B^*$ ; then  $\text{Tr}_K^L(\beta B) \subset R$ ; as  $A \subset B$  then  $\beta A \subset \beta B$  and so  $\text{Tr}_K^L(\beta A) \subset R$  as well. So  $\beta \in A^*$ .

$\text{diff } A \subset (A^{-1})^{-1}$ :  $\text{diff } A = (A^*)^{-1}$ .  $A^{-1} \subset A^*$  (by 33. (a)), so  $(A^{-1})^{-1} \supset (A^*)^{-1} = \text{diff } A \implies \text{diff } A \subset (A^{-1})^{-1}$ .

$(I^{-1})^{-1} = I$ : By 31 (b), the fractional ideals form a group under multiplication and  $II^{-1} = S$ ; therefore  $(I^{-1})^{-1} = I$ .

$\text{diff } I \subset I$ :  $\text{diff } I \subset (I^{-1})^{-1} = I$  by the two previous steps.

$\text{diff } I$  is a fractional ideal:  $I^*$  is an additive subgroup of  $L$ , by 33 (a), the inverse of  $I^*$  is an  $S$ -module and so  $S(\text{diff } I) = \text{diff } I$ .  $\text{diff } I^{-1} \supset I^{-1}$  and as  $\gamma^{-1} \in I^{-1}$ ,  $\gamma^{-1} \in \text{diff } I^{-1}$  and so  $\text{diff } I$  has a non-empty inverse. Therefore  $I$  is a fractional ideal by 33 (b).

$A \subset I \implies \text{diff } A$  is a fractional ideal: As  $A^*$  is an additive subgroup,  $\text{diff } A$  is an  $S$ -module. Similarly  $\text{diff } A^{-1} \supset A^{-1}$  and  $\gamma \in A^{-1}$  (as  $A \subset I$ ,  $\gamma I \subset S \implies \gamma A \subset S$ ), so  $\text{diff } A$  is also a fractional ideal by 33 (b).



$I^*$  is an  $S$ -submodule of  $L$ : By the additive property of the trace,  $I^*$  is an additive subgroup. Take  $s \in S$ : as  $\text{Tr}(\alpha I) \subset R \implies \text{Tr}(\alpha \gamma J) \subset R$ ; as  $J$  is an  $S$ -ideal,  $sJ \subset J$ , so  $\text{Tr}(s\alpha \gamma J) = \text{Tr}(\alpha \gamma J) \subset R$ , so  $I^*$  is an  $S$ -submodule.  $I^*$  is a fractional ideal:  $I^* = ((I^*)^{-1})^{-1} = (\text{diff } I)^{-1}$ ;  $\text{diff } I$  is a fractional ideal by previous and as the fractional ideals form a multiplicative group so is its inverse.

34. Let  $\{\alpha_1, \dots, \alpha_n\}$  be a basis for  $L$  over  $K$ .

34. (a) Since the  $\alpha_i$ s form a basis for  $L$  over  $K$  their discriminant is nonzero and so the matrix  $M$  corresponding to the trace product has nonzero determinant. Take  $\beta_i = \sum_{k=1}^n \alpha_k M_{ik}^{-1}$ . Then  $\text{Tr}(\beta_i \alpha_j) = \sum_{k=1}^n \alpha_j \alpha_k M_{ik}^{-1} = \sum_{k=1}^n M_{ki} M_{ik}^{-1} = \delta_{ij}$  where  $\delta_{ij}$  is the Kronecker delta function. Therefore the  $\beta_i$  form a dual basis to the  $\alpha_i$ .

34. (b) Let  $A = R\alpha_1 \oplus \dots \oplus R\alpha_n$ . Show that  $A^* = B$  where  $B$  is the  $R$ -module generated by the  $\beta_i$ .

As the  $\beta_i$  were written as linear combinations of the  $\alpha_i$ s, we know  $B \subset A^*$ ; it remains to show the opposite direction.

Let  $\gamma \in A^*$ , define  $m_i = \text{Tr}_L^K(\gamma \alpha_i)$ ; by assumption  $m_i \in R$ . Take  $\beta = \sum_{i=1}^n m_i \beta_i$ . For any  $\alpha \in A$ ,  $\alpha = r_1 \alpha_1 \oplus \dots \oplus r_n \alpha_n$  so  $\text{Tr}_K^L(\gamma \alpha) = \sum_{i=0}^n r_i m_i = \text{Tr}_K^L(\beta \alpha)$ . Therefore  $\text{Tr}_L^K((\gamma - \beta)A) = 0$ .

We claim  $\gamma - \beta = 0$ . Since  $A$  is a free  $R$ -module generated by the  $\alpha_i$ , each  $\alpha_i \in A$ . If  $(\gamma - \beta)^{-1} \neq 0 \in L$ , it can be written as a sum of the  $\alpha_i$  with coefficients in  $K$ . As  $K$  is the field of fractions of  $R$  there is some  $r \neq 0$  such that  $r$  clears the denominators of the coefficients of the  $\alpha_i$  and so  $r(\gamma - \beta)^{-1} \in A$ . Then  $\text{Tr}_K^L(r(\gamma - \beta)(\gamma - \beta)^{-1}) = \text{Tr}_K^L(r) = rn$  where  $n = [L : K]$ . However  $\text{Tr}_K^L((\gamma - \beta)\alpha) = 0$  for all  $\alpha \in A$ . Therefore  $\gamma - \beta = 0$  and so  $A^* \subset B$ . We conclude  $A^* = B$ .

35. Let  $\alpha \in L$ ,  $L = K[\alpha]$ . Let  $f$  be the monic irreducible polynomial for  $\alpha$  over  $K$ , and write  $f(x) = (x - a)g(x)$ . Then we have

$$g(x) = \gamma_0 + \gamma_1 x + \dots + \gamma_{n-1} x^{n-1}$$

We claim that

$$\left\{ \frac{\gamma_0}{f'(\alpha)}, \dots, \frac{\gamma_{n-1}}{f'(\alpha)} \right\}$$

is the dual basis to  $\{1, \alpha, \dots, \alpha^{n-1}\}$ .

35. (a) Let  $\sigma_1, \dots, \sigma_n$  be the embeddings of  $L$  in  $\mathbb{C}$  fixing  $K$  pointwise. Then the  $\sigma_i(\alpha)$  are the roots of  $f$ . Applying  $\sigma_i$  to  $f(x)$  gives

$$\sigma_i(f(x)) = \sigma_i(x - \alpha)\sigma_i(g(x)) = (x - \alpha_i)g_i(x)$$

where  $g_i(x)$  is  $g(x)$  with  $\sigma_i$  applied to each coefficient and  $\alpha_i$  is the conjugate  $\sigma_i(\alpha)$ .

35. (b) By the chain rule, we have

$$f'(x) = (x - \alpha_i)g'_i(x) + g_i(x)$$

So rearranging terms gives

$$g_i(\alpha_j) = f'(\alpha_j) - (\alpha_j - \alpha_i)g'_i(\alpha_j)$$

Clearly  $g_i(\alpha_i) = f'(\alpha_i)$ . If  $i \neq j$ ,  $f'(\alpha_j) = (\alpha_j - \alpha_i)g'_i(\alpha_j) + g_i(\alpha_j)$ ;  $g_i(\alpha_j) = 0$  since  $g_i$  is a root of all conjugates of  $\alpha$  except for  $\alpha_i$ . Therefore  $g_i(\alpha_j) = 0$ .

35. (c) Let  $M$  be the matrix formed by  $[\alpha_j^{i-1}]$  where  $i$  is the row and  $j$  is the column. Let  $N$  be the matrix  $[\sigma_i(\gamma_{j-1}/f'(\alpha))]$ .

Take  $NM_{ij}$  as the  $i$ th row and  $j$ th column of the matrix product  $NM$ . Then  $NM_{ij} = \sum_{k=1}^n \alpha_j^{k-1} \sigma_i(\gamma_{k-1}/f'(\alpha)) = \frac{1}{f'(\alpha)} g'_i(\alpha)$ . By (b) this value is 1 when  $i = j$  and 0 otherwise; therefore  $NM$  is the identity matrix.

Since  $\alpha$  is the root of a monic polynomial over  $K$  it must be such that  $\alpha \notin K$  and  $\text{disc}(\alpha) \neq 0$ ; therefore the matrix  $M$  is invertible and so  $NM = I$  implies  $N = M^{-1}$ ; so  $MN = I$ .  $MN_{ij} = \sum_{k=1}^n \sigma_k(\alpha^{i-1} \gamma_{j-1}/f'(\alpha)) = \text{Tr}(\alpha^{i-1} \gamma_{j-1}/f'(\alpha))$ .

Since  $MN$  is also the identity element the set  $\{\frac{\gamma_0}{f'(\alpha)}, \dots, \frac{\gamma_{n-1}}{f'(\alpha)}\}$  is therefore the dual basis to  $\{1, \alpha, \dots, \alpha^{n-1}\}$ .

35. (d) Let  $a_i$  be the coefficient of the  $i$ th power of  $f(x)$ . Multiplying out  $f(x) = (x - \alpha)g(x)$ ,

$$-\gamma_0\alpha + (\gamma_0 - \gamma_1\alpha)x + (\gamma_1 - \gamma_2\alpha)x^2 + \dots \gamma_{n-1}x^n$$

To show the  $\gamma_i$  as an  $R$ -module generate  $R[\alpha]$  we prove the following lemma by induction:

**Lemma 2.** For  $i \neq n-1$ ,  $\gamma_i = \sum \alpha^{n-i-1} + a_{n-i-1}\alpha^{n-i-2} + \dots + a_{i+1}$ .

*Proof.* From the above multiplication,  $-\gamma_0\alpha = a_0 = -(\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha)$  and so  $\gamma_0 = \alpha^{n-1} + a_{n-1}\alpha^{n-2} + \dots + a_1$ . This is a sum of powers with leading coefficient 1 and constant term equal to  $a_i$ . Therefore the base case is satisfied.

Next, assume  $\gamma_i = \alpha^{n-i-1} + a_{n-i-1}\alpha^{n-i-2} + \dots + a_{i+1}$ . From the above expansion we have  $a_{i+1} = (\gamma_i - \alpha\gamma_{i+1})$ , so  $a_{i+1} = a_{i+1} + a_{i+2}\alpha + \dots + \alpha^{n-i-1} - \alpha\gamma_{i+1}$  and so  $\alpha\gamma_{i+1} = \alpha(\alpha^{n-i-2} + \dots + a_{i+2})$ . Therefore  $\gamma_{i+1}$  can also be written in the appropriate form.  $\square$

For  $i = n-1$ ,  $\gamma_{n-1} = 1$  since  $f(x)$  is a monic polynomial. There is then a translation matrix between the powers of  $\alpha$  and the  $\gamma_i$ s with 1s on the diagonal. This translation matrix is upper triangular since the power of  $\alpha$  in row  $i$  is  $i-1$ . This matrix is invertible over  $\mathbb{Z}$  and the powers of  $\alpha$  must also be writable in terms of the  $\gamma_i$ s. Therefore the  $\gamma_i$ s generate  $R[\alpha]$  as an the  $R$ -module.

35. (e) We have the following:

$$\begin{aligned}
 (R[\alpha])^* &= \left\{ \frac{\gamma_0}{f'(\alpha)}, \dots, \frac{\gamma_{n-1}}{f'(\alpha)} \right\} && \text{By 34. (b)} \\
 &= \frac{1}{f'(\alpha)} \{\gamma_0, \dots, \gamma_{n-1}\} \\
 &= \frac{1}{f'(\alpha)} R[\alpha] && \text{By 35. (d)}
 \end{aligned}$$

35. (f) Let  $\beta \in \text{diff } R[\alpha]$ ; then  $\beta(R[\alpha])^* \subset S$ . By (e),  $\beta(\frac{1}{f'(\alpha)})R[\alpha] \subset S$  so  $\beta R[\alpha] \subset f'(\alpha)S$ . Therefore  $\beta \in f'(\alpha)S$ . Therefore  $\text{diff } R[\alpha] \subset f'(\alpha)S$ . The reverse inclusion is straightforward. Therefore  $\text{diff } R[\alpha] = f'(\alpha)S$ .
35. (g) Let  $R[\alpha] \subset S$  so  $\text{diff } R[\alpha] = R[\alpha] \text{ diff } S \subset \text{diff } S$  by the final equality of Exercise 33. By (f),  $\text{diff } R[\alpha] = f'(\alpha)S$ . Since  $f'(\alpha) \in \text{diff } f'(\alpha)S$  therefore  $f'(\alpha) \in \text{diff } S$ .

## Chapter 4

1. Prove from the definitions that  $E(Q|P) \triangleleft D(Q|P)$ .

Let  $\sigma \in E(Q|P)$  and  $\tau \in D(Q|P)$ . We have the following series of equivalences:

$$\begin{aligned}
 \alpha &\equiv \alpha \pmod{Q} \\
 \tau(\alpha) &\equiv \tau(\alpha) \pmod{Q} \\
 \sigma(\tau(\alpha)) &\equiv \tau(\alpha) \pmod{Q} \\
 \tau^{-1}(\sigma(\tau(\alpha))) &\equiv \tau^{-1}\tau(\alpha) \equiv \alpha \pmod{Q}
 \end{aligned}$$

Therefore  $E$  is normal in  $D$ .

3. (a) Let  $p$  be an odd prime. Since the multiplicative group of any prime is cyclic, it must have a generator  $g$  with order  $p-1$ . As  $g^{p-1} \equiv 1 \pmod{p}$ ,  $g^{(p-1)/2} \equiv -1 \pmod{p}$ . Therefore if  $p \equiv 1 \pmod{4}$  then  $g^{(p-1)/4} \equiv \pm 1 \pmod{p}$  and  $\left(\frac{-1}{p}\right) = 1$ . Conversely, if  $\left(\frac{-1}{p}\right) = -1$ , let  $a$  be such that  $a^2 \equiv -1 \pmod{p}$ ; therefore  $a^4 \equiv 1 \pmod{p}$  and so  $4 \mid p-1$ .
5. Let  $K$  and  $L$  be number fields,  $L$  a normal extension of  $K$  with Galois group  $G$ , and  $P$  a prime of  $K$ . By "intermediate field" we mean "intermediate field distinct from  $K$  and  $L$ ".
5. (a) If  $P$  is inert in  $L$ , then as  $\text{ref} = n$ ,  $f = n$ . The decomposition group  $D(Q|P)$  is thus all of  $G$ . As  $G$  is normal in itself, Corollary 1 to Theorem 28 gives us that  $G$  is cyclic of order  $n$ .

5. (b) Suppose  $P$  is totally ramified in every intermediate field, but not totally ramified in  $L$ . Take  $L_E$  to be the inertia field of  $P$ ; by Theorem 28, the ramification index of  $L_E$  is 1. By assumption  $L_E$  is totally ramified and so  $[L_E : K] = 1$ ; therefore  $L_E = K$  and so  $f(Q|P) = 1$  and  $r(Q|P) = 1$ ; therefore  $P$  must be totally ramified in  $L$  also, contradicting our assumption. Therefore no intermediate fields distinct from  $K$  and  $L$  must exist.

Since no intermediate fields exist,  $G$  must have no proper subgroups and so be of prime order for some prime  $p$ , and so must also be cyclic.

5. (c) Suppose every intermediate field contains a unique prime lying over  $P$  but  $L$  does not. We argue in similar style to (b). Take  $L_D$  to be the decomposition field of  $P$ . By Theorem 28, there must only be 1 unique prime lying over  $L_D$  and so  $[L_D : K] = 1$  and therefore  $r = 1$ . Therefore  $n = ef$  and so there is one unique prime lying over  $P$  in  $L$ , contradicting our assumption, and so no intermediate fields distinct from  $K$  and  $L$  exist. Therefore  $G$  is cyclic of prime order as in (b).
5. (d) If  $P$  is unramified in every intermediate field but ramified in  $L$ , then in particular  $P$  is unramified in  $L_E$ . Let  $H \subset G$ , then as  $L_H$  is unramified,  $L_H \subset L_E$  and so  $E \triangleleft H$ . As  $L_E$  is also an intermediate field and is unramified,  $[L : L_E] \neq 1$  and so  $E$  is nontrivial. Therefore  $E$  is the unique smallest nontrivial subgroup of  $G$ .

Since  $E$  has no subgroups, it must be of prime order for some prime  $p$ . As it is the unique subgroup of order  $p$ , it must be normal in  $G$ , as it is the sole element of its conjugacy class. Since  $Z(G) \neq \emptyset$  in a group of prime power order and is a normal subgroup of  $G$ ,  $E$  must also be contained in  $Z(G)$ .

Because every subgroup of  $G$  contains  $E$ , by the Sylow theorems, every subgroup of  $G$  must have prime power order, including  $G$  itself. (Otherwise there would be a  $q$ -subgroup  $H$  with  $H \cap E \neq \emptyset$  which would give an element of  $H$  with order  $p$ , a contradiction.)

5. (e) If  $P$  splits completely in every intermediate field but not in  $L$ , then  $P$  must split completely in  $L_D$  and so  $L_D \neq K$ .

Let  $M$  be an intermediate field of  $L$ ; then  $r_M = [L : M]$ ; but  $r_M \leq r$ . Therefore any intermediate field of  $L$  must be a subfield of  $L_D$  and there are no intermediate fields between  $L_D$  and  $L$ .

Therefore, for any nontrivial subgroup  $H \subset G$ ,  $D \subset H$ , and  $D$  has no proper subgroups. Therefore it must be of prime order for some  $p$  and so cyclic. As in (d),  $G$  must be a group of order  $p^k$ ,  $D \triangleleft G$ , and  $D \subset Z(G)$ .

**An example over  $\mathbb{Q}$ :** Let  $L$  be the cyclotomic field  $\mathbb{Q}[\zeta_5]$ . The Galois group of  $L$  has order 4 and is cyclic with generator  $\sigma$ .

Let  $p = 19$ ;  $19 \equiv -1 \pmod{5}$  so  $19^2 \equiv 1 \pmod{5}$  and so 19 has multiplicative order 2 mod 5. By Theorem 26, its inertial degree in  $\mathbb{Z}[\zeta_5]$  is 2 and as

$\gcd(5, 19) = 1$ , its ramification index is 1; since  $\text{ref} = 4$ , 19 must split into 2 primes in  $\mathbb{Z}[\zeta_5]$ .

Because there are 2 primes lying over 19 in  $\mathbb{Z}[\zeta_5]$ , and  $\sigma$  generates the Galois group,  $\sigma$  must permute the primes lying over 19, meaning its decomposition group  $D = \{e, \sigma^2\}$ . This is a normal subgroup in  $G$  and so Corollary 2 to Theorem 28 applies.

As there are no other subgroups of  $G$ , 19 splits completely in every proper subfield of  $\mathbb{Q}[\zeta_5]$  but not in  $\mathbb{Q}[\zeta_5]$ , where it has inertial degree 2.

5. (f) Let  $P$  be inert in every intermediate field but not inert in  $L$ . By (b), for there to be an intermediate field,  $P$  must be ramified in  $L$  with degree  $e$ . By (d),  $G$  is a group of prime power order.

Let  $E$  be the inertia subgroup of  $P$ : since  $P$  remains inert in every subgroup, there  $E$  is a maximal subgroup in  $G$ . Applying (a) to  $L_E$  we have that  $E$  is cyclic; as  $E$  is a unique maximal subgroup,  $G$  is therefore also cyclic.

7. (a) Let  $p = 3$ ,  $K = \mathbb{Q}[\sqrt{-3}]$ ,  $L = \mathbb{Q}[\sqrt{3}]$ . Since  $\mathbb{Q}[i] \subset KL$  and  $p$  is inert in  $\mathbb{Q}[i]$ ,  $p$  is not totally ramified in  $KL$  despite being totally ramified in  $K$  and  $L$ .

7. (b) Let  $p = 2$ . By Theorem 25,  $p$  ramifies in any quadratic field  $\mathbb{Q}[\sqrt{m}]$  with  $m \equiv 3 \pmod{4}$ ; however,  $p$  splits in any quadratic field  $1 \equiv 3 \pmod{4}$ . Since  $3^2 \equiv 1 \pmod{4}$ , any two extensions of  $\mathbb{Q}$   $m, n \equiv 3 \pmod{4}$ ,  $\gcd(m, n) = 1$ , and  $mn \not\equiv 5 \pmod{8}$  will contain a subfield where  $p = 2$  splits into 2 distinct primes. Let  $K = \mathbb{Q}[\sqrt{7}]$ ,  $L = \mathbb{Q}[\sqrt{15}]$ : then  $7 \cdot 15 \equiv 1 \pmod{8}$  and so 2 does not remain inert and splits into two primes in its subfield  $\mathbb{Q}[\sqrt{105}]$ . Therefore 2 splits into two ramified prime ideals in  $KL$ .

7. (c) Let  $p = 2$ . By Theorem 25,  $p$  is inert in any quadratic field  $\mathbb{Q}[\sqrt{m}]$  where  $m \equiv 5 \pmod{8}$ . Therefore  $p$  is inert in both  $K = \mathbb{Q}[\sqrt{5}]$  and  $L = \mathbb{Q}[\sqrt{13}]$ . However, the composite field  $KL$  contains the subfield  $\mathbb{Q}[\sqrt{65}]$  and  $65 \equiv 1 \pmod{8}$ , and by Theorem 25, 2 splits into two primes in  $\mathbb{Q}[\sqrt{65}]$ . Therefore 2 also splits into two primes in  $KL$  each with inertial degree 2.

7. (d) Let  $p = 2$ . We reverse the procedure we used in (b) and look for any two relatively prime integers  $m, n$  such that  $mn \equiv 5 \pmod{8}$ . Take  $m = 3, n = 15$ ; then  $p$  is ramified in both  $K = \mathbb{Q}[\sqrt{3}]$  and  $L = \mathbb{Q}[\sqrt{15}]$  but remains inert in the subfield  $\mathbb{Q}[\sqrt{5}] \subset KL$ . Therefore  $p$  has a residue field extension of degree 2 in  $KL$ .

8. Let  $r, e, f$  be positive integers. I will assume Dirichlet's Theorem on primes in arithmetic progression: given integers  $a$  and  $d$  such that  $\gcd(a, d) = 1$ , there exists a prime  $p$  such that  $p = a + nd$ .

8. (a) The  $q$ th cyclotomic field has degree  $q - 1$  over  $\mathbb{Q}$ . Since  $q$  is the only prime dividing  $\text{disc}(\mathbb{Z}[\zeta_q])$ , no distinct prime  $p$  will ramify in  $\mathbb{Q}[\zeta_q]$ ; therefore,

by Theorem 26, if  $p$  has multiplicative order  $f \bmod q$ , it will split into  $(q-1)/f$  distinct primes in  $\mathbb{Q}[\zeta_q]$ .

For any given  $r$ , take  $q$  a prime such that  $q \equiv 1 \pmod{r}$ ; by Exercise 30 (c), there are an infinite number of primes that satisfy this property.

Since  $q$  is a prime, it has a primitive root  $g$  and  $g^r$  has order  $f$  in  $q$ . It remains to find a prime  $p$  such that  $p \equiv g^r \pmod{q}$ . Such a prime  $p$  always exists by Dirichlet's Theorem on primes in arithmetic progression.

- (b) Take  $q$  to be a prime such that  $q \equiv rf \pmod{1}$ ; then there exists some  $k$  such that  $krf + 1 = q$ . Let  $g$  be a primitive root for  $q$ : then  $q^r$  is an element of order  $fk$ , so using Dirichlet's Theorem we find  $p$  such that  $p \equiv g^r \pmod{q}$ . Since  $p$  has order  $fk \bmod q$ , the prime ideal  $(p)$  in  $\mathbb{Z}$  splits into  $r$  distinct prime ideals in  $\mathbb{Q}[\zeta_q]$ .

As  $\text{Gal}(\mathbb{Q}[\zeta_q])$  is cyclic, the comment after Theorem 28 applies and  $\mathbb{Q}[\zeta_q]$  splits into  $r$  distinct prime ideals in every subfield containing the decomposition field, which is of order  $r$ . Therefore  $p$  also splits into  $r$  distinct prime ideals in the subfield  $K'$  of degree  $rf$ .

- (c) When choosing  $p$ , we apply the Chinese Remainder Theorem to the system of equivalences  $g^{kr} \equiv p \pmod{q}$  and  $p \equiv 1 \pmod{e}$  (choosing a  $q$  such that  $\gcd(q, e) = 1$ ). This gives an integer  $M$ , possibly composite, such that  $M \equiv 1 \pmod{e}$  and  $M \equiv g^{kr} \pmod{q}$ . We know that  $M \not\equiv 1 \pmod{q}$  since  $g$  was chosen to be a primitive root of  $q$ . Therefore  $\gcd(M, qe) = 1$ , and we can apply Dirichlet's Theorem on primes in arithmetic progression to find a prime  $p$  such that  $p = M + nqe$  for some  $n$ ; therefore  $p \equiv 1 \pmod{e}$  and  $p \equiv g^{kr} \pmod{q}$ .
- (d) In the  $p$ th cyclotomic field,  $p$  is totally ramified. Since  $\mathbb{Q}[\zeta_p]$  is normal over  $\mathbb{Q}$ ,  $p$  is totally ramified in every intermediate field. Finally,  $\text{Gal}(\mathbb{Q}[\zeta_p])$  is cyclic so it has a normal subgroup of order  $d$  for each divisor of  $p-1$ . As  $p$  was chosen such that  $p \equiv 1 \pmod{e}$ . It follows that  $\mathbb{Q}[\zeta_p]$  has a subfield  $K''$  such that  $[K'' : \mathbb{Q}] = e$ .

The composition field  $K'K'' \subset \mathbb{Q}[\zeta_q]$  and has degree  $ref$  over  $\mathbb{Q}$ . Since  $p$  splits into  $r$  distinct factors in  $K'$  and is ramified in  $K''$ , it splits into  $r$  distinct factors, each with ramification index  $e$ .

- (e) Take  $e = 2, f = 3, r = 5$ . We start by finding a prime  $q$  such that  $q \equiv 1 \pmod{fr}$ ;  $q = 31$  works (here  $k = 2$ ). 31 has several primitive roots - we want to choose one such that  $g^r = g^5$  is smallest as this will make our search for a prime easiest. In particular 13 is a primitive root of 31 and  $13^5 \equiv 6 \pmod{31}$ , so we choose  $p = 37$ .

The  $31 \cdot 37 = 1147$ th cyclotomic field therefore has a subfield of degree  $ref = 30$  over  $\mathbb{Q}$  (by (d)) where the prime ideal  $(5)$  splits into 5 distinct primes, each with ramification index 2.

9. Let  $L$  be a normal extension of  $K$ ,  $P$  a prime of  $K$ , and  $Q$  and  $Q'$  of  $L$  lying over  $P$ . Since  $L$  is normal there is some  $\sigma$  such that  $Q' = \sigma Q$ . Let  $D$

and  $E$  be the decomposition and inertia groups for  $Q$  over  $P$  and  $D'$  and  $E'$  the corresponding things for  $Q'$  over  $P$ .

9. (a) Prove that  $D' = \sigma D \sigma^{-1}$  and  $E' = \sigma E \sigma^{-1}$ .

$D' = \sigma D \sigma^{-1}$ : Suppose  $\tau \in D$ ; then  $\tau(Q) = Q$ . As  $Q' = \sigma Q$ ,  $\sigma^{-1}(Q') = Q$ . Then  $\sigma(\tau(\sigma^{-1}))(Q') = Q'$ ,  $\sigma\tau\sigma^{-1} \in D'$ , so  $\sigma D \sigma^{-1} \subseteq D'$ .

Conversely assume  $\tau' \in D'$ , so  $\tau'(Q') = Q'$  and  $\tau'(\sigma(Q)) = Q'$ . Thus  $\sigma^{-1}\tau'(\sigma(Q)) = Q$ , so  $\sigma^{-1}\tau'\sigma \in D$  and  $\tau' \in \sigma D \sigma^{-1}$ . Therefore  $D' \subseteq \sigma D \sigma^{-1}$ ; we conclude  $D' = \sigma D \sigma^{-1}$ .

$E' = \sigma E \sigma^{-1}$ : Let  $\tau \in E$ ; then  $\alpha \equiv \tau(\alpha) \pmod{Q}$  for all  $\alpha \in S$ , so  $\alpha - \tau(\alpha) \in Q$ . In particular  $\sigma^{-1}(\alpha) - \tau(\sigma^{-1}(\alpha)) \in Q$ , and so  $\alpha - \sigma(\tau(\sigma^{-1}(\alpha))) \in \sigma Q = Q'$ . Therefore  $\sigma\tau\sigma^{-1} \in E'$  and  $\sigma E \sigma^{-1} \subseteq E'$ .

Conversely assume  $\tau' \in E'$ ; then  $\alpha - \tau'(\alpha) \in Q'$  for any  $\alpha \in S$ . So  $\sigma(\alpha) - \tau'(\sigma(\alpha)) \in Q'$  and  $\alpha - \sigma^{-1}(\tau'(\sigma(\alpha))) \in \sigma^{-1}Q' = Q$ . Therefore  $\sigma^{-1}E'\sigma \subseteq E$  and so  $E' \subseteq \sigma E \sigma^{-1}$ ; we conclude  $E' = \sigma E \sigma^{-1}$ .

9. (b) Let  $\psi(\alpha) \equiv \alpha^{\|P\|} \pmod{Q}$ ; then  $\psi(\alpha) - \alpha^{\|P\|} \in Q$  for any  $\alpha \in S$ . In particular  $\psi(\sigma(\alpha)) - \sigma(\alpha)^{\|P\|} \in Q$  and so  $\sigma^{-1}\psi(\sigma(\alpha)) - \alpha^{\|P\|} \in \sigma^{-1}Q = Q'$ . Therefore  $\psi' = \sigma^{-1}\psi\sigma$ .

- 12 (a) Let  $\omega = e^{2\pi i/m}$ , let  $G = \text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \simeq \mathbb{Z}_m^\times$ ,  $K$  be any subfield of  $\mathbb{Q}[\omega]$  and  $H$  the subgroup of  $G$  fixing  $K$ . Let  $p \in \mathbb{Z}$  such that  $p \nmid m$ , and let  $f$  denote the least integer such that  $p^f \in H$ . Show  $f$  is the inertial degree  $f(P|p)$  for any  $P$  of  $K$  lying over  $p$ .

Since  $p$  is unramified,  $\phi(P|p)$  exists and corresponds to some  $b \in G$ . A permutation in  $G$  corresponds to taking  $\omega \mapsto \omega^b$ . However the Frobenius automorphism has the property  $b(\omega) = \omega^b \equiv \omega^p \pmod{P}$ , so we have  $b \equiv p \pmod{n}$ .

Let  $H\bar{a}_1, \dots, H\bar{a}_n$  be the cosets of  $H$  (with  $\bar{a}_1$  being the permutation that takes  $\omega \mapsto \omega^{a_1}$ ).

Let the cyclic group  $\{1, p, p^2, \dots, p^{f-1}\}$  (with  $p^f = 1$ ) act on the right cosets of  $H$ . For any coset  $Hx$ ,  $p^a(Hx) = Hxp^a$ ; if  $xp^a = x$  then  $\omega^{xp^a} = \omega^x$  and so  $xp^a \equiv x \pmod{m}$ . Therefore  $p^a \equiv 1 \pmod{m}$ ; as  $p \nmid m$ ,  $a = 0$ . By the orbit stabilizer theorem, the size of an orbit of  $Hx$  is the size of the whole group, i.e.  $f$ , by Theorem 33 the inertial degree of any prime  $P$  of  $K$  lying over  $p$  is  $f$ .

12. (b) Let  $\mathbb{Q}[\omega + \omega^{-1}]$  be a subfield of  $\mathbb{Q}$ . The subgroup of  $G$  that fixes  $\mathbb{Q}[\omega + \omega^{-1}]$  is the subgroup of order 2 consisting of the identity and complex conjugation  $\tau$  that takes  $\omega \mapsto \omega^{-1}$ . This  $\tau$  is identified with the permutation  $m-1 \in \mathbb{Z}_m^\times$ , so the subgroup  $H$  consists of  $\{1, m-1\} = \{1, -1\}$ .

Let  $K = \mathbb{Q}[\omega + \omega^{-1}]$ . By the tower law,  $\phi(m) = [\mathbb{Q}[\omega] : \mathbb{Q}] = [\mathbb{Q}[\omega] : K][K : \mathbb{Q}] = 2 \cdot [K : \mathbb{Q}]$ , so  $[K : \mathbb{Q}] = \phi(m)/2$ . For any odd prime  $p$  such that  $p \nmid m$ ,  $p$  is unramified in  $\mathbb{Q}[\omega]$  and so also in  $K$ . By (a),  $p$  will split into  $\phi(m)/2f$  primes in  $K$ , where  $f$  is the smallest integer such that  $p^f \equiv \pm 1 \pmod{m}$ .

12. (c) Letting  $p$  be a prime not dividing  $m$ , and take  $K$  to be any quadratic subfield  $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\omega]$ . Let  $H$  be the subgroup fixing  $K$ . Since  $p \nmid m$ ,  $p$  is unramified in  $\mathbb{Q}[\omega]$  and so also unramified in  $\mathbb{Q}[\sqrt{d}]$ . Therefore either  $p$  remains inert or splits into two primes in  $\mathbb{Q}[\omega]$ .

Let  $p$  be odd. We will show that  $\bar{p} \in H$  iff  $d$  is a square mod  $p$ ; this is equivalent to  $f = 1$  iff  $d$  is a square mod  $p$ . As  $p$  is unramified, Theorem 25 gives that  $f = 1$  iff  $d$  is a square mod  $p$ .

Now let  $p = 2$ . We will show that  $\bar{p} \in H$  iff  $d \equiv 1 \pmod{8}$ . This is equivalent to  $f = 1$  iff  $d \equiv 1 \pmod{8}$ . As  $p$  is unramified, Theorem 25 gives the only possibility where  $f = 1$  is  $d \equiv 1 \pmod{8}$ .

13. Let  $m \in \mathbb{Z}$ . Assume  $m$  is not square and  $m \neq -1$ . Let  $K = \mathbb{Q}[\sqrt[4]{m}]$  and  $L = \mathbb{Q}[\sqrt[4]{m}, i]$ ; then  $L$  is a normal extension of  $\mathbb{Q}$  such that  $K \subset L$ . Denote the roots  $\alpha, i\alpha, -\alpha, -i\alpha$  as 1, 2, 3, and 4.

13. (a)  $[K : \mathbb{Q}] = 4$  and  $[L : K] = 2$  so  $L$  is a degree 8 extension of  $\mathbb{Q}$  where  $f(x) = x^4 - m$  splits. Let  $G = \text{Gal}(L/K)$ ; so  $|G| = 8$ . Letting the roots of  $f$  be  $\alpha, i\alpha, -\alpha, -i\alpha$ ,  $G \subset S_4$  and so  $G \simeq D_8$  (the dihedral group on 4 objects) as this is the only subgroup of  $S_4$  of order 8. Therefore  $G = \{1, \tau, \sigma, \tau\sigma, \sigma^2, \tau\sigma^2, \sigma^3, \tau\sigma^3\}$ . In  $D_8$ ,  $\tau^2 = 1$  and  $\sigma^4 = 1$ , with  $\tau\sigma = \sigma^{-1}\tau$ . Note  $\tau$  corresponds to complex conjugation (switching  $i\alpha$  with  $-i\alpha$ ).

13. (b) Let  $p$  be an odd prime not dividing  $m$ . Prove  $p$  is unramified in  $L$ .

Let  $S = \mathbb{A} \cap L$  and consider  $\text{disc}(\alpha)$ .  $\text{disc}(\alpha) = N(f'(\alpha)) = \pm N(4\alpha^3) = \pm 4^8 N(\alpha)^3 = \pm 4^8 (-m)^3$ ; therefore  $p \nmid \text{disc}(\alpha)$ . Because  $\text{disc}(R) \mid \text{disc}(\alpha)$ ,  $p \nmid \text{disc}(R)$  also, so  $p$  is unramified in  $L$ .

13. (c) Let  $Q$  be a prime lying over  $p$ . Since  $p$  is unramified in  $L$ , the Frobenius automorphism  $\phi(Q|p)$  exists. The subgroup  $H$  of  $G$  that fixes  $K$  is the subgroup corresponding to complex conjugation:  $\{1, \tau\}$ . The right cosets of  $H$  are  $H, H\sigma, H\sigma^2, H\sigma^3$ .

Suppose  $\phi(Q|p) = \tau$ . Since  $H\sigma\tau = H\tau\sigma^3 = H\sigma^3$ , these two cosets are in the same partition.  $H\tau = H$  and  $H\sigma^2\tau = H\tau\sigma^2\tau = H\sigma^2$ . Therefore we have three partitions of cosets:  $\{H\}, \{H\sigma, H\sigma^3\}, \{H\sigma^2\}$ , and by Theorem 32,  $Q$  splits into 3 primes in  $K$ .

13. (d) For each permutation of  $G$ , we follow a similar process to (c) to give how  $Q$  splits. The subgroup  $H$  fixing  $K$  remains the same as in (c).

The partitions are straightforward to calculate since right-multiplication of any  $H\sigma^n$  by any permutation gives another coset of the form  $H\sigma^m$ . This is straightforward for permutations  $\sigma^a$ , whereas for permutations  $\sigma^a\tau$ ,

$$H\sigma^n(\sigma^a\tau) = H\sigma^{n+a}\tau = H\tau\sigma^{-(n+a)} = H\sigma^{-(n+a)}$$



$\psi(Q p)$	Partitions	Number of Primes
1	$\{H\}, \{H\sigma\}, \{H\sigma^2\}, \{H\sigma^3\}$	4
$\sigma, \sigma^3$	$\{H, H\sigma, H\sigma^2, H\sigma^3\}$	1
$\sigma^2$	$\{H, H\sigma^2\}, \{H\sigma, H\sigma^3\}$	2
$\tau$	$\{H\}, \{H\sigma, H\sigma^3\}, \{H\sigma^2\}$	3
$\sigma\tau$	$\{H, H\sigma^3\}, \{H\sigma, H\sigma^2\}$	2
$\sigma^2\tau$	$\{H, H\sigma^2\}, \{H\sigma\}, \{H\sigma^3\}$	3
$\sigma^3\tau$	$\{H, H\sigma\}, \{H\sigma^2, H\sigma^3\}$	2

18. (a) TODO

18. (b) Suppose  $\sigma \in \cap V_m$ , then for any  $\alpha \in S$ ,  $\sigma(\alpha) - \alpha \in \cap Q^m = 0$ . Since  $\alpha$  was chosen arbitrarily  $\sigma$  must be the identity permutation. Therefore the descending chain of subgroups eventually stabilizes at the identity.

19. Let  $\sigma \in V_{m-1}$ ,  $\pi \in Q - Q^2$ , and  $\sigma(\pi) \equiv \sigma (Q^{m+1})$ .

19. (a) Suppose  $\alpha \in \pi S$ , so it must have form  $\alpha = \pi\beta$  for  $\beta \in S$ . By the definition of  $\sigma$ ,  $\sigma(\beta) \equiv \beta (Q^m)$ . As  $\pi \in Q - Q^2$ ,  $\pi\sigma(\beta) \equiv \pi(\beta) (Q^{m+1})$ . Since  $\pi \equiv \sigma(\pi) (Q^{m+1})$ ,  $\sigma(\pi)\sigma(\beta) = \sigma(\pi\beta) = \sigma(\alpha) \equiv \alpha (Q^{m+1})$ .

19. (b) Since  $\pi \notin Q^2$ , the principal ideal  $(\pi)$  has a decomposition  $JQ$  where  $J \not\subset Q$ . If the ideal  $(\alpha)$  has a decomposition  $IQ^n$  where  $I \not\subset Q$ , then  $IJQ \subset \pi S$  and  $IJ \not\subset Q$ .

$IJ$  also contains an integer  $m$  ( $m = \|IJ\|$ ), take  $\beta = m$ . Then  $\sigma(\beta) = \beta$  and  $\beta\alpha \in \pi S$ .

Given  $\alpha \in Q$ ,  $\beta\alpha \in \beta Q = \pi S$ . By (a),  $\sigma(\beta\alpha) \equiv \beta\alpha (Q^{m+1})$ . As  $\sigma(\beta) = \beta$ ,  $\beta\sigma(\alpha) \equiv \beta\alpha (Q^{m+1})$ . Since  $\beta \notin Q$  we can cancel both sides and so  $\sigma(\alpha) \equiv \alpha (Q^{m+1})$ .

19. (c) Following the hint,  $S = S_E + Q$ ; so every  $\alpha \in S$  can be written as a sum of an element of the number ring of the fixed field of  $E$  and an element of  $Q$ . Let  $\alpha = \beta + \gamma$  where  $\beta \in S_E$  and  $\gamma \in Q$ . By (b),  $\sigma(\gamma) \equiv \gamma (Q^{m+1})$ , so  $\sigma(\gamma) + \beta \equiv \gamma + \beta (Q^{m+1})$ . Since  $\beta \in S_E$ ,  $\sigma(\beta) = \beta$  and so,  $\sigma(\gamma + \beta) \equiv \gamma + \beta (Q^{m+1})$ . This is the required result.

20. Take  $\pi \in Q - Q^2$ . We first show the suggested statement. Given  $\sigma \in V_i - V_{i+1}$ , by exercise 19 we know  $\sigma(\pi) \equiv \pi (Q^i)$  if and only if  $\sigma \in V_{i+1}$ . As  $V_i \subset V_m$  for  $m \leq i$ , then  $\sigma(\pi) - \pi \in Q^{i+1}$  if and only if  $\sigma \in V_i$ .  $\sigma \in V_i$  implies  $\sigma \in V_m$  for  $m \leq i$  (ramification subgroups are a descending sequence) and  $Q^{i+1} \subset Q^{m+1}$  for  $m \leq i$ ; therefore  $\sigma(\pi) - \pi \in Q^{m+1}$  if and only if  $\sigma \in V_m$ .

Take  $\sigma \in E$ . Since the  $V_i$  are a descending sequence of subgroups of  $E$ , there is some  $k \geq 0$  so that  $\sigma \in V_k - V_{k+1}$ . Applying the suggested statement to this, we see  $\sigma \in V_k \iff \sigma(\pi) \equiv \pi (Q^{k+1})$ .

(What's left here? This feels incomplete.)

21. (a) Take  $\pi \in Q - Q^2$  and  $\sigma \in E$ .

TODO: add case where  $Q = (\pi)$ .

Let  $(\pi) = QI$ . As  $Q, I$  are relatively prime, we take  $x$  be the solution to the system of congruences

$$\begin{array}{rcl} x & \equiv & \sigma(\pi) \pmod{Q^2} \\ x & \equiv & 0 \pmod{I} \end{array}$$

Claim:  $x \in Q$ . Proof of claim: As  $\sigma(\pi) - x \in Q^2$ ,  $\pi(\sigma(\pi) - x) \in Q^2$ . Because  $\sigma \in E$ ,  $\pi\sigma(\pi) \in Q^2$ , subtracting this shows that  $\pi x \in Q^2$ . Because  $\pi \notin Q^2$ ,  $x \in Q$ .

Now  $x \in Q, I$ . Since  $Q, I$  are coprime ideals,  $Q \cap I = QI$  and so  $x \in QI = (\pi)$ . Therefore  $x = \alpha\pi$  for some  $\alpha \in S$  and  $\sigma(\pi) \equiv \alpha\pi \pmod{Q^2}$ , the required result.

21. (b) By (a),  $\tau(\pi) \equiv \alpha_\tau \pi \pmod{Q^2}$ ,  $\sigma\tau(\pi) \equiv \alpha_\sigma \alpha_\tau \pi \pmod{Q^2}$ , thus  $\sigma\tau(\pi) \equiv \alpha_\sigma \alpha_\tau \pi \pmod{Q^2}$  as required.

21. (c) Let  $\psi : E \rightarrow (S/Q)^* = \sigma \rightarrow \alpha_\sigma$ . TODO (basic)

- 22 . Take  $m \geq 2$ . Our goal is to embed  $V^{m-1}/V^m$  in the additive group of  $S/Q$ .

22. (a) Show that for each  $\sigma \in V^{m-1}$ , there exists an  $\alpha \in S$  depending on  $\sigma$  so

$$\sigma(\pi) \equiv \pi + \alpha\pi^m \pmod{Q^{m+1}}$$

TODO: add case where  $Q = (\pi)$ .

We proceed as in 21. (a). Let  $(\pi) = QI$  and take  $x$  be a solution to the system of congruences

$$\begin{array}{rcl} x & \equiv & \sigma(\pi) \pmod{Q^{m+1}} \\ x & \equiv & \pi \pmod{I^m} \end{array}$$

Claim:  $x - \pi \in Q^m$ . Proof of claim: since  $\sigma \in V_{m-1}$ ,  $\sigma(\pi) - \pi \in Q^m$ ; therefore  $\pi\sigma(\pi) - \pi^2 \in Q^{m+1}$ . As  $\sigma(\pi) - x \in Q^{m+1}$ ,  $\pi\sigma(\pi) - \pi x \in Q^{m+1}$ : subtracting this from  $\pi\sigma(\pi) - \pi^2$  shows  $\pi x - \pi^2 = \pi(x - \pi) \in Q^{m+1}$ . Since  $\pi \notin Q^2$ ,  $x - \pi \in Q^m$ .

As  $x - \pi \in Q^m \cap I^m = Q^m I^m = (\pi)^m$ ,  $x - \pi = \alpha\pi^m$  for some  $\alpha$ . Therefore  $\sigma(\pi) \equiv \pi + \alpha\pi^m \pmod{Q^{m+1}}$  as required.

## Chapter 5

6. Show that  $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$  is principal for  $m = 2, 3, 5, 6, 7, 173, 293, 437$ . As each of these  $m$  is positive, these are real quadratic fields and so the

number of complex embeddings  $s = 0$ . Therefore the bound given by Minkowski's Theorem is that every ideal class contains an ideal with  $\|J\| < \frac{2!}{2^2} \cdot \sqrt{|\text{disc}(R)|}$ , where  $\text{disc}(R) = m$  if  $m \equiv 1 \pmod{4}$  and  $\text{disc}(R) = 4m$  otherwise. Therefore

$$\|J\| < \begin{cases} \frac{\sqrt{m}}{2} & m \equiv 1 \pmod{4} \\ \sqrt{m} & m \equiv 2, 3 \pmod{4} \end{cases}$$

$m = 2$ :  $\|J\| < \sqrt{2} \approx 1.4$  so every ideal class contains an ideal with norm 1. Therefore every ideal must be principal.

$m = 3$ :  $\|J\| < \sqrt{3} \approx 1.7$  so every ideal is principal.

$m = 5$ :  $\|J\| < \sqrt{5}/2 \approx 1.1$  so every ideal is principal.

$m = 6$ :  $\|J\| < \sqrt{6} \approx 2.4$  so we must check that the prime ideal containing 2 is principal. By Theorem 25, 2 factors as  $(2, \sqrt{6})^2$  in  $\mathbb{Q}[\sqrt{6}]$ .  $(2, \sqrt{6})$  is principal, generated by  $(2 + \sqrt{6})$ :  $2 = -1 \cdot (2 + \sqrt{6})(2 - \sqrt{6})$  and  $\sqrt{6} = 2 + \sqrt{6} - 2$ . Therefore every ideal is principal.

$m = 7$ :  $\|J\| < \sqrt{7} \approx 2.6$  so we must check that the prime ideal containing 2 is principal. By Theorem 25, 2 factors as  $(2, 1 + \sqrt{7})^2$ .  $(2, \sqrt{7})$  is generated by  $3 + \sqrt{7}$ ;  $2 = (3 + \sqrt{7})(3 - \sqrt{7})$  and  $1 + \sqrt{7} = 3 + \sqrt{7} - 2$ . Therefore every ideal is principal.

$m = 173$ :  $173 \equiv 1 \pmod{4}$ , so  $\|J\| < \sqrt{173}/2 \approx 6.5$ , so we must check that the prime ideals containing 2, 3, 5 are all principal. Since  $173 \equiv 5 \pmod{8}$ , 2 remains prime in  $\mathbb{Q}[\sqrt{m}]$  and so its ideal is principal. 173 is a prime number. Since  $173 \equiv 1 \pmod{4}$ , by quadratic reciprocity,  $\left(\frac{173}{p}\right) = \left(\frac{p}{173}\right)$ , so  $\left(\frac{3}{173}\right) = \left(\frac{173}{3}\right) = \left(\frac{2}{3}\right) = -1$ . Similarly  $\left(\frac{5}{173}\right) = \left(\frac{173}{5}\right) = \left(\frac{3}{5}\right) = -1$ . So both 3 and 5 remain inert in  $\mathbb{Q}[\sqrt{m}]$  and so every ideal is principal.

$m = 293$ :  $293 \equiv 1 \pmod{4}$  so  $\|J\| < \sqrt{293}/2 \approx 8.5$  so we must check the prime ideals containing 2, 3, 5, 7 are all principal.  $293 \equiv 5 \pmod{8}$  so 2 remains prime in  $\mathbb{Q}[\sqrt{293}]$  and its ideal is principal. 293 is a prime number. Calculation with Sage shows that 3, 5, 7 each are not squares mod 293, so these prime ideals remain inert in  $\mathbb{Q}[\sqrt{293}]$  and so are principal. Therefore every ideal is principal.

$m = 437$ :  $437 \equiv 1 \pmod{4}$  so  $\|J\| < \sqrt{437}/2 \approx 10.4$  so we must check that the prime ideals 2, 3, 5, 7 are all principal.  $437 \equiv 5 \pmod{8}$  so 2 remains prime in  $\mathbb{Q}[\sqrt{437}]$ .  $437 = 19 \cdot 23$  so none of 3, 5, 7 ramify in  $\sqrt{437}$ . Using Sage we can calculate the Jacobi symbol  $\left(\frac{3, 5, 7}{437}\right) = -1$ . As the Jacobi symbol is -1 each of these are nonresidues mod 437 and so by Theorem 25 remain prime in  $\mathbb{Q}[\sqrt{437}]$ . Therefore every ideal is principal.

10. (b) First, the problem in the book has a typo (both editions). The problem statement should be "Suppose  $p$  is an odd prime such that  $4p < -m$ . Show  $m$  is a non-square mod  $p$ ."

Since  $m \equiv 5 \pmod{8}$ ,  $m \equiv 1 \pmod{4}$ . Let  $R = \mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$ . If  $m$  is a square mod  $p$ , then  $pR = (p, \frac{n+\sqrt{m}}{2})(p, \frac{n-\sqrt{m}}{2})$  (by Theorem 25). Suppose  $R$

is a PID; therefore the ideal  $(p, \frac{n+\sqrt{m}}{2})$  is generated by  $\frac{n+\sqrt{m}}{2}$  with  $p = (\frac{n+\sqrt{m}}{2})(\frac{n-\sqrt{m}}{2})$ . Therefore

$$n^2 - m = 4p \implies n^2 - m < -m \implies n^2 < 0$$

This contradicts  $n^2 \equiv m \pmod{p}$ , so  $p$  must be inert in  $R$ , meaning  $m$  is a nonsquare mod  $p$ .

10. (c) From (a) we know  $m \equiv 5 \pmod{8}$ , and so  $m \equiv 1 \pmod{4}$ . If  $m$  is to be a principal ideal domain, it must be prime: otherwise any prime  $p \mid m$  would ramify in  $\mathbb{Q}[\sqrt{m}]$  as the ideal  $(p, \sqrt{m})$  which is nonprincipal if  $\sqrt{m}$  has a norm  $\neq p$ .

The first prime above 19 such that  $m \equiv 5 \pmod{8}$  is 29; therefore by (b) any  $m < -19$  such that  $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$  is a principal ideal domain must have 3, 5, and 7 be inert.

For an odd prime  $p$  to be inert,  $m$  must be a non-residue modulo  $p$ . We already know that 2 is inert if  $m \equiv 5 \pmod{8}$ . For 3 to be inert,  $m \equiv 2 \pmod{3}$ . For 5 to be inert,  $m \equiv \pm 2 \pmod{5}$ . For 7 to be inert,  $m \equiv 3, 5, 6 \pmod{7}$ . Using the Chinese Remainder Theorem on each of these combinations we have

$$m \equiv -403, -163, -43, -67, -667, -547 \pmod{840}$$

Relevant computation with Sage:

```
sage: modulae_list = [( [2], 3), ([2, 3], 5),
...                  ([3, 5, 6], 7), ([5], 8)]
sage: prime_list = [a[1] for a in modulae_list]
sage: residues = [a[0] for a in modulae_list]
sage: [-(840-CRT_list(list(rs),prime_list))
...     for rs in itertools.product(*residues)]
[-403, -163, -43, -67, -667, -547]
```

10. (d) TODO (base off (c))

11. The Minkowski bound for  $\mathbb{Z}[\sqrt{-6}]$  is  $\frac{2!}{2^2} \left(\frac{4}{\pi}\right) \sqrt{24} \approx 3.11$ . Both 2 and 3 ramify in  $\mathbb{Z}[\sqrt{-6}]$  as they divide the discriminant;  $(2, \sqrt{-6})^2 = (2)$  and  $(3, \sqrt{-6})^2 = (3)$ . Neither of these ideals is principal as  $x^2 + 6y^2 = \{2, 3\}$  has no integer solutions.  $(2, \sqrt{-6}) = \frac{\sqrt{-6}}{3}(3, \sqrt{-6})$ , so they are in the same ideal class element. Therefore the ideal class group of  $\mathbb{Z}[\sqrt{-6}]$  has order 2.

The Minkowski bound for  $\mathbb{Z}[\sqrt{-10}]$  is  $\frac{2!}{2^2} \left(\frac{4}{\pi}\right) \sqrt{40} \approx 4.02$ , so again we only need to consider 2 and 3. 2 ramifies as  $(2, \sqrt{-10})^2$ ; as in the previous case this is not a principal ideal due to  $x^2 + 10y^2 = 2$  having no integer solutions. 3 remains inert;  $-10 \equiv 2 \pmod{3}$  and  $\left(\frac{2}{3}\right) = -1$ , so 3 does not factor in  $\mathbb{Z}[\sqrt{-10}]$ .

12. The Minkowski bound for  $\mathbb{Z}[\sqrt{-23}]$  is 3.053, so only 2 and 3 need to be considered. As  $\left(\frac{2}{-23}\right) = 1$ , 2 factors as  $2 = \left(2, \frac{\sqrt{-23}-1}{2}\right)\left(2, \frac{\sqrt{-23}+1}{2}\right)$ .  $x^2 + 23y^2 = 8$  has no integer solutions, so this must be a non-principal ideal.  $\left(2, \frac{\sqrt{-23}-1}{2}\right)^2 = (4, \sqrt{-23}-1, \frac{\sqrt{-23}-11}{2}) = (4, \frac{\sqrt{-23}+3}{2})$ . This is also not a principal ideal since  $x^2 + 23y^2 = 16$  has no solutions with  $y \neq 0$  (since  $\frac{\sqrt{-23}+3}{2}$  is in the ideal it can't just be generated by an integer). However,  $\left(2, \frac{\sqrt{-23}-1}{2}\right)^3 = (8, \sqrt{-23}-1, \sqrt{-23}+3, \frac{\sqrt{-23}-13}{2})$ . First observe  $\frac{\sqrt{-23}+3}{2}$  is in this ideal. Next, observe  $8 = N(\frac{\sqrt{-23}+3}{2})$ , so the ideal is principal. Therefore there are 3 elements in the ideal class group.

I am (for now) omitting the part of the exercise which asks that we do the same for  $-31, -83, -139$ .

(Skip a bunch of quadratic field exercises.)

17. Let  $\omega = e^{2\pi i/7}$ .  $\text{disc}(\mathbb{Z}[\omega]) = -7^5$ , and  $\mathbb{Z}[\omega]$  has degree 6 over  $\mathbb{Q}$ . There are 6 embeddings from  $\mathbb{Z}[\omega]$  into  $\mathbb{Q}$ ; each taking  $\omega$  to a different root of unity. Therefore the Minkowski bound is  $\frac{6!}{6^6} \left(\left(\frac{4}{\pi}\right)^3 \sqrt{7^5}\right) = \frac{720 \cdot 64 \cdot 49 \sqrt{7}}{\pi^3 6^6} = \frac{3920 \sqrt{7}}{81 \pi^3} \approx 4.12$ . So the only prime ideals we need to examine contain 2 or 3.

By the Corollary to Theorem 26, 2 splits into  $\frac{\varphi(7)}{3} = 2$  ideals mod 7 ( $2^3 \equiv 1 \pmod{7}$ ), while 3 remains inert. Mod 2,  $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$  factors as  $(x^3 + x + 1)(x^3 + x^2 + 1)$ , so  $2 = (2, \omega^3 + \omega + 1)(2, \omega^3 + \omega^2 + 1)$ . As  $(\omega^3 + \omega + 1)(\omega^3 + \omega^2 + 1)(\omega^4) = 2$ , so both of these ideals is principal. Therefore  $\mathbb{Z}[\omega]$  is a PID.

Next, let  $\mathbb{Z}[\omega + \omega^{-1}]$ . By Exercise 35, Chapter 2, the discriminant over this number field is  $7^2 = 49$ . This is a real subfield of order 3 over  $\mathbb{Q}$  (no embeddings in  $\mathbb{C}$ ) so its Minkowski bound is  $\frac{3!}{3^3} \sqrt{49} = \frac{14}{9} < 2$ , so  $\mathbb{Z}[\omega + \omega^{-1}]$  is a PID.

18. Let  $\omega = e^{2\pi i/11}$ . This is a real subfield of degree 5 over  $\mathbb{Q}$  with discriminant  $11^4$ , so its Minkowski bound is  $\frac{5!}{5^5} \cdot 11^2 = \frac{2904}{625} \approx 4.6$ . So we must investigate the prime ideals 2 and 3.

By Exercise 12 Chapter 4 primes in  $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$  for  $\zeta_p$  a  $p$ th root of unity split into  $\frac{p-1}{2f}$  ideals, where  $f$  the smallest integer so that  $p^f \equiv \pm 1 \pmod{p}$ . Letting  $p = 11$  and looking at 2 and 3, we have both  $2^5 \equiv -1 \pmod{11}$  and  $3^5 \equiv 1 \pmod{11}$ , so both 2 and 3 remain inert in  $\mathbb{Z}[\omega]$ . Therefore  $\mathbb{Z}[\omega]$  is a PID.

We repeating the same process for  $\omega = e^{2\pi i/13}$ . In this case the discriminant of  $\mathbb{Z}[\omega + \omega^{-1}] = 13^5$  so the Minkowski bound is  $\frac{6!169\sqrt{13}}{6^6} = \frac{845\sqrt{13}}{324} \approx 9.403$ . We must examine the primes 2, 3, 5, 7. Here the ideal splitting formula that a prime splits into  $\frac{6}{f}$  ideals.

2 and 7 remain inert in  $\mathbb{Z}[\omega + \omega^{-1}]$  ( $2^6, 7^6 \equiv -1 \pmod{13}$ ), but 3 splits into 2 ideals ( $3^3 \equiv 1 \pmod{13}$ ) and 5 splits into 3 ideals ( $5^2 \equiv -1 \pmod{13}$ ). Computation

via Sage shows each of these ideals is principal. Therefore  $\mathbb{Z}[\omega + \omega^{-1}]$  is a PID.

19. Let  $K = \mathbb{Q}[\sqrt[3]{2}]$ .  $\mathbb{A} \cap K = \mathbb{Z}[\sqrt[3]{2}]$  by Exercise 41 of Chapter 2 ( $2 \not\equiv \pm 1 \pmod{9}$ ), and  $\text{disc}(\mathbb{Z}[\sqrt[3]{2}]) = -27(2)^2$ . There are 2 complex embeddings for  $K$  so the Minkowski bound of  $K$  is  $\frac{3!}{3^3} \left(\frac{4}{\pi}\right) \sqrt{|-27 \cdot 2^2|} = \frac{16\sqrt{3}}{3\pi} \approx 2.94$ . The only prime ideal class we must investigate is the one lying over (2); however, 2 is fully ramified in  $\mathbb{A} \cap K$ , and so its ideal is  $(2, \sqrt[3]{2})^3 = (\sqrt[3]{2})^3$  is principal. Therefore  $\mathbb{Z}[\sqrt[3]{2}]$  is a PID.

Let  $\alpha$  be a root of  $\alpha^3 - \alpha - 1$ . By Exercise 28 of Chapter 2  $\mathbb{A} \cap \mathbb{Q}[\alpha] = \mathbb{Z}[\alpha]$ , and  $\text{disc}(\alpha) = -(-4 + 27) = -23$ . This field also has 2 complex embeddings (there is only 1 real root), so the Minkowski bound is  $\frac{8\sqrt{23}}{9\pi} \approx 1.356$ . There are no primes within this bound so every ideal of  $\mathbb{Z}[\alpha]$  is a principal ideal.

20. Let  $\alpha$  be a root of  $\alpha^3 - \alpha - 7$ . By Exercise 28 of Chapter 2,  $\text{disc}(\alpha) = (-4 + 27 \cdot 7^2) = -1319$ . This is prime (so squarefree) and so  $\mathbb{A} \cap \mathbb{Q}[\alpha] = \mathbb{Z}[\alpha]$  by Exercise 27 of Chapter 2. This field has 2 complex embeddings (only 1 real root) so the Minkowski bound is  $\frac{8\sqrt{1319}}{9\pi} \approx 10.27$ . We must investigate the primes 2, 3, 5, and 7. Since  $\text{disc}(\alpha)$  is prime each of these factors in the Dedekind way, e.g. by seeing how the polynomial  $\alpha^3 - \alpha - 7$  factors mod  $p$ . Additionally, since the minimum polynomial has degree 3 the prime remains inert if there is no root mod  $p$ .

- $p = 2$ :  $x^3 - x - 7 \equiv x^3 + x + 1 \pmod{2}$ . This has a root if there is an  $x$  so that  $x(x^2 + 1) = 1$  (clearly not), so 2 remains inert.
- $p = 3$ :  $x^3 - x - 7 \equiv x^3 + 2x + 2 \pmod{3}$ . This has a root if  $x(x^2 + 2) = 1$ ; however no options work. 3 remains inert.
- $p = 5$ :  $x^3 - x - 7 \equiv x^3 + 4x + 3 \pmod{5}$ . This has a root if  $x(x^2 + 4) = 2$ ; again no options work.
- $p = 7$ : as per the hint,  $7 = \alpha^3 - \alpha = \alpha(\alpha + 1)(\alpha - 1)$ , so  $(7) = (7, \alpha)(7, \alpha + 1)(7, \alpha - 1)$ . Since  $N(\alpha) = 7$  it is a principal ideal.  $\alpha + 1$  is the root of the polynomial  $x^3 - 3x^2 + 2x - 7$  (determined via Sage) so  $N(\alpha + 1) = 7$  and  $(\alpha + 1)$  is also principal. Similarly  $N(\alpha - 1) = 7$  and so  $(7, \alpha - 1)$  is principal.

We have considered all ideals below the Minkowski bound; each of these are principal, so  $\mathbb{Z}[\alpha]$  must be a PID.

21. By the binomial theorem,  $(\sqrt[3]{m} + a)^3 = m + 3a(\sqrt[3]{m})^2 + 3a^2(\sqrt[3]{m}) + a^3$ . Therefore the minimum polynomial for  $\sqrt[3]{m} + a$  is  $x^3 - \text{something} \cdot x^2 - \text{something} \cdot x - (m + a^3)$ , so  $N(\sqrt[3]{m} + a) = m + a^3$ .
22. Any purely cubic field has 2 complex embeddings, so the Minkowski bound is  $\frac{3!}{3^3} \left(\frac{4}{\pi}\right) \sqrt{|-27m^2|} = \frac{8m\sqrt{3}}{3\pi}$ . By Exercise 41 of Chapter 2, if  $m \not\equiv \pm 1 \pmod{9}$ ,  $\mathbb{A} \cap K = \mathbb{Z}[\sqrt[3]{m}]$  (this is the case for  $m = 3, 5, 6$ ). A real cubic field has

degree 3 over  $\mathbb{Q}$ , so it has no non-trivial subfields and if a prime ramifies, it is totally ramified.

$m = 3$ : the Minkowski bound is  $\approx 4.4$  and 3 ramifies as  $(\sqrt[3]{3})^3$  (principal).  $(\sqrt[3]{3}^2 + \sqrt[3]{3} + 1)(\sqrt[3]{3} - 1) = (2)$ ; by Exercise 21,  $N(\sqrt[3]{3} - 1) = 3 + (-1)^3 = 2$  and so both the ideals lying over 2 are principal. Therefore  $\mathbb{Q}[\sqrt[3]{3}]$  is a PID.

$m = 5$ : the Minkowski bound is  $\approx 7.3$ . Since 5 ramifies as  $(\sqrt[3]{5})^3$  (principal) we need to examine the ideal classes of 2, 3, and 7. Let  $\alpha = \sqrt[3]{5}$ .

The polynomial  $x^3 - 5 \equiv x^3 + 1 \pmod{2}$  factors as  $(x + 1)(x^2 + x + 1)$ , so by Dedekind factoring (Theorem 25) 2 splits into two factors,  $(2, \alpha + 1)(2, \alpha^2 + \alpha + 1)$ . Sage indicates that these are principal ideals and equal to  $(\alpha^2 - \alpha - 1)(\alpha^2 + 2\alpha + 3)$ . [Not sure how to see this without a computer algebra program]

$\alpha - 2$  has norm  $-3$  and so the ideal  $(\alpha - 2)$  that lies over 3 is principal (in fact this ideal ramifies over 3).

Considering the ideal class of (7):  $x^3 - 5$  is irreducible mod 7; if it were reducible it would have a root, but 5 is not a cubic residue mod 7. Therefore 7 remains inert. Therefore  $\mathbb{Q}[\sqrt[3]{5}]$  is a PID.

$m = 6$ : the Minkowski bound is  $\approx 8.8$ , so we again must consider the ideal class groups of 2, 3, 5, and 7. Let  $\alpha = \sqrt[3]{6}$ .

By Exercise 21,  $N(\alpha - 2) = -2$ ; as 2 is ramified, 2 factors as  $(\alpha - 2)^3$ . 3, 5, and 7 are seen as principal via Sage computation. 3 is ramified as  $(\alpha^2 + 2\alpha + 3)^3$ , 5 has the principal ideals  $(\alpha - 1)$  and  $(\alpha^2 + \alpha + 1)$  both with norm 5 lying over it, and 7 factors as  $(7) = (\alpha + 1)(2\alpha^2 + 4\alpha + 7)(\alpha^2 + \alpha - 5)$ . Therefore  $\mathbb{Z}[\alpha]$  is a PID.

23. (a) We let  $K = \mathbb{Q}[\sqrt[3]{m}]$  and take  $\alpha = \sqrt[3]{m}$ . By Exercise 17, Chapter 2, the norm of  $\alpha + b\alpha + c\alpha^2$  is the determinant of multiplying this element by each of the  $K$  basis  $\{1, \alpha, \alpha^2\}$ . Therefore:

$$N(a + b\alpha + c\alpha^2) = \det \begin{pmatrix} a & cm & bm \\ b & a & cm \\ c & b & a \end{pmatrix} = a^3 + c^3m^2 + b^3m - 3abcm$$

23. (b) If  $m$  is squarefree then  $\{1, \alpha, \alpha^2\}$  is an integral basis (Exercise 41, Chapter 2). Therefore for all  $\beta \in \mathbb{A} \cap K$ ,  $\beta$  has the form  $a + b\alpha + c\alpha^2$  and so by (a),  $N(\beta) \equiv a^3 \pmod{m}$ .
24. Let  $K = \mathbb{Z}[\sqrt[3]{7}]$  and  $\alpha = \sqrt[3]{7}$ . The Minkowski bound  $\approx 10.29$  so we must examine the ideals (2), (3), (5), (7). (7) ramifies as the principal ideal  $(\alpha)^3 = 7$ . (2) and (5) factor as per Dedekind.
- $x^3 - 7 \equiv x^3 + 1 \pmod{2}$  so mod 2,  $(2) = (2, \alpha + 1)(2, \alpha^2 + \alpha + 1)$ . By Exercise 23,  $N(\alpha + 1) = 1 + 7 = 8$ , so  $(2, \alpha + 1)$  is not principal. Similarly,  $N(\alpha^2 + \alpha + 1) = 1 + 7^2 + 7 - 21 = 36$ , and so  $(2, \alpha^2 + \alpha + 1)$  is also not principal.

$(2, \alpha + 1)^2 = (4, 2\alpha + 2, \alpha^2 + 2\alpha + 1) = (4, \alpha + 1)$ .  $(2, \alpha + 1)^3 = (\alpha + 1)$  which is principal. There are thus at least 3 ideal classes.

TODO: 5

## Chapter 7

1. (a)

$$\begin{aligned} 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \dots &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots - 2\left(\frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \dots\right) \\ &= \zeta(s) - 2\left(2^{-s} + \frac{2^{-s}}{2} + \frac{2^{-s}}{3} + \dots\right) \\ &= \zeta(s) - 2^{1-s}\zeta(s) = \zeta(s)(1 - 2^{1-s}) \end{aligned}$$

1. (b)  $\frac{d}{ds}(1 - 2^{1-s}) = 2^{1-s} \ln(2)$  has the value  $\ln(2)$  at  $s = 1$  so it has a simple zero (order 1).

3.

$$\zeta_{K, A \cup B}(s) = \prod_{P \in A, B} \left(1 - \frac{1}{\|P\|^s}\right) = \prod_{P \in A} \left(1 - \frac{1}{\|P\|^s}\right) \prod_{P \in B} \left(1 - \frac{1}{\|P\|^s}\right)$$

The last equality follows as  $A, B$  are disjoint. Therefore  $\zeta_{K, A \cup B} = \zeta_{K, A} \zeta_{K, B}$ .

As the quotient and the product of two non-zero analytic functions on the same region is also analytic, the relationship  $\zeta_{K, A \cup B} = \zeta_{K, A} \zeta_{K, B}$  shows that if any two of these functions are well-defined on the half plane  $x > 1/2$ , the third must also be.

Let  $\zeta_{K, A \cup B}^n$  has a pole of order  $m$  (so  $d(A \cup B) = m/n$ ). Therefore the product  $\zeta_{K, A}^n \zeta_{K, B}^n$  has a pole of order  $m$ . Letting  $k$  and  $j$  be the largest negative numbers for the Laurent expansion of  $A$  and  $B$ , we must have  $k + j = m$ . Therefore  $\zeta_{K, A}^n$  has polar density  $k/n$  and  $\zeta_{K, B}^n$  has polar density  $j/n$ , and so  $d(A \cup B) = d(A) + d(B)$ .

4. Let  $H$  be the normal subgroup of  $\{1, -1\} \in \mathbb{Z}_m^*$ . By Corollary 3 of Theorem 43, this set has density  $2/\varphi(m)$ . Similarly, the subgroup  $\{1\}$  (primes  $p \equiv 1 \pmod{m}$ ) has density  $1/\varphi(m)$ . Applying the result of Exercise 3,  $d(\text{primes } \equiv 1, -1 \pmod{m}) = d(\text{primes } \equiv 1 \pmod{m}) + d(\text{primes } \equiv -1 \pmod{m})$ , so  $2/\varphi(m) = 1/\varphi(m) + d(\text{primes } \equiv -1 \pmod{m})$ . The result follows.

5.  $\varphi(24) = 8$ , and  $\mathbb{Z}_{24}^* \simeq \mathbb{Z}_8^* \times \mathbb{Z}_3^* = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ , so every element  $a \in \mathbb{Z}_{24}^*$  has order 2. Applying Corollary 3 of Theorem 43, each subgroup  $\{1, a\}$  has polar density  $2/8$ .  $\{1\}$  has polar density  $1/8$ , so by applying Exercise 3, we see  $\{a\}$  has polar density  $1/8$  as desired.