PartII Number Fields Exercises

zc231

Contents

1 Chapter 1

1. We find a polynomial which is zero at the corresponding element and by standard method, show that the polynomial is irreducible or the degree of extension is equal to the degree of the polynomial we get. So (i) $x^4 + 36$ (ii) $x^4 - 4x^2 + 16$ (iii) The minimal polynomial of $y = \exp(2i\pi/19)$ is $y^6+y^5+y^4+y^3+y^2+y+1 = 0$. Then $x = y+y^{-1}$ has minimal polynomial $x^3 + x^2 - 2x - 1$ (iv) Let $x = (1 + \sqrt[3]{10} + \sqrt[3]{100})/3$ and let $y = x\sqrt[3]{10}$. Then $y = 3 + x$ and taking cube of both sides we have

$$10x^3 = x^3 + 9x^2 + 27x + 27$$

and so the minimal polynomial is $x^3 - x^2 - 3x - 3 = 0$. These are all algebraic integers.

2. Let $L = K(x)$ where $Ax^2 + Bx + B = 0$. Since $\mathrm{char}(K) \neq 2$ we can complete the square for this and so $L = K(\sqrt{a})$ for some a.

   If a/b is a square then clearly $K(\sqrt{a}) = K(\sqrt{b})$. Conversely, if $K(\sqrt{a}) = K(\sqrt{b}) = L$, then the Galois action $\sqrt{a} \mapsto -\sqrt{a}$ sends $\sqrt{b}$ to $-\sqrt{b}$. So $\sqrt{a/b}$ is fixed and so a/b is a square.

3. (i) Let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be the minimal polynomial of α over $\mathcal{O}_K$ and let $R = \mathcal{O}_K[a_0, \ldots, a_{n-1}]$. So $R[x]$ is a finitely generated R-module because x is integral over R and R is a finitely generated $\mathbb{Z}$-module because $a_0, \ldots, a_{n-1}$ are integral over $\mathbb{Z}$. So $R[x]$ is a finitely generated $\mathbb{Z}$-module and so x is integral over $\mathbb{Z}$.

   (ii) Let $g = f^n \in \mathcal{O}_K[x]$ and g is monic. α is a root of g if and only if α is a root of f. Since every root of g is integral over $\mathcal{O}_K$, so every root of f is integral over $\mathcal{O}_K$. Therefore, $f \in \mathcal{O}_K[x]$ (you can consider each irreducible factor of f, which is the minimal polynomial of some root of f).

4. Let $0 \neq x \in I$. It is integral over A so there exist $a_0, \ldots, a_{n-1} \in A$ with $a_0 \neq 0$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

   So $a_0 = -x(x^{n-1} + \cdots + a_1) \in I \cap A$.

5. All we need to check is that the embeddings are homomorpisms: Let $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = n$ and let σ be any embedding and $\sigma(\theta) = \alpha$. If

$$a = \sum_{i=0}^{n-1} a_i\theta^i, \quad b = \sum_{i=0}^{n-1} b_i\theta^i$$

   where $a_i, b_i \in \mathbb{Q}$ then clearly

$$\sigma(a + b) = \sigma(a) + \sigma(b) = a_0 + b_0 + (a_1 + b_1)\theta + \cdots .$$

   Let $P(x)$ be the minimal polynomial of θ. Let

$$f(x) = \sum_{i=0}^{n-1} a_i x^i, \quad g(x) = \sum_{i=0}^{n-1} b_i x^i$$

   so that $f(\theta) = a, g(\theta) = b$. Then by division algorithm we have $q(x), r(x)$ such that

$$f(x)g(x) = P(x)q(x) + r(x), r(x) = 0 \text{ or } \deg r < \deg P.$$

   Evaluate the above at θ so $ab = r(\theta)$. So

$$\sigma(ab) = \sigma(r(\theta)) = r(\sigma(\theta)) = r(\alpha).$$

   Also $P(\alpha) = P(\sigma(\theta)) = \sigma(P(\theta)) = 0$ and so

$$\sigma(a)\sigma(b) = f(\alpha)g(\alpha) = P(\alpha)q(\alpha) + r(\alpha) = r(\alpha).$$

6. $X^3 - 2X + 6$ is 2-Eisenstein and so it is irreducible. (i) When $\alpha = n - \theta$,

$$T_{K/\mathbb{Q}}(\alpha) = 3n - T_{K/\mathbb{Q}}(\theta) = 3n$$

and

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{j=1}^{3}(n - \theta_j) = n^3 - 2n + 6.$$

(ii) When $\alpha = 1 - \theta^2$, the minimal polynomial of θ^2 is $X^3 - 4X^2 + 4X - 36 = 0$ and so

$$T_{K/\mathbb{Q}}(\alpha) = 3 - 4 = -1$$

and

$$N_{K/\mathbb{Q}}(\alpha) = 1 - 4 + 4 - 36 = -35.$$

(iii) When $\alpha = 1 - \theta^3 = 7 - 2\theta$ we have

$$T_{K/\mathbb{Q}}(\alpha) = 21 - 2 \cdot 0 = 21$$

and

$$N_{K/\mathbb{Q}}(\alpha) = 2^3((7/2)^3 - 2(7/2) + 6) = 335.$$

2 Chapter 2

1. Let $f(X) = X^3 - d$ and $\delta_1, \delta_2, \delta_3$ be roots of f. Then

$$\Delta(1, \delta, \delta^2) = \begin{vmatrix} 1 & 1 & 1 \\ \delta_1 & \delta_2 & \delta_3 \\ \delta_1^2 & \delta_2^2 & \delta_3^2 \end{vmatrix}^2 = \prod_{i<j} (\delta_i - \delta_j)^2 = disc(f) = -27d^2.$$

$\theta := u + v\delta + w\delta^2$. Then a direct computation shows that

$$T_{K/\mathbb{Q}}(\theta) = 3u, N_{K/\mathbb{Q}}(\theta) = d^2w^3 - 3duvw + dv^3 + u^3, T_{K/\mathbb{Q}}(\delta\theta) = 3dw, T_{K/\mathbb{Q}}(\delta^2\theta) = 3dv.$$

These must all be integers and so by considering the traces we set

$$u' = 3u, v' = 3dv, w' = 3dw, u', v', w' \in \mathbb{Z}$$

and so

$$u = \frac{u'}{3}, v = \frac{v'}{3d}, w = \frac{w'}{3d}.$$

Substitute these into $N(\theta)$, we have

$$\frac{w'^3}{27d} - \frac{u'v'w'}{9d} + \frac{v'^3}{27d^2} + \frac{u'^3}{27} \in \mathbb{Z}$$

and so there is some integer r such that

$$dw'^3 - 3du'v'w' + v'^3 + u'^3d^2 = 27d^2r.$$

Since $d|27d^2r, dw'^3, 3du'v'w', u'^3d^2$, so $d|v'^3$ and so $d|v'$ because d is square-free. So we can write $v' = dv''$ and so

$$dw'^3 - 3d^2u'v''w' + v''^3d^3 + u'^3d^2 = 27d^2r$$

which implies

$$w'^3 - 3du'v''w' + v''^3d^2 + u'^3d = 27dr.$$

The above equation shows that $d|w'$. So we conclude that $\frac{v'}{d}, \frac{w'}{d}$ are both integers and so

$$u = \frac{u'}{3}, v = \frac{\frac{v'}{d}}{3}, w = \frac{\frac{w'}{d}}{3} \in \frac{1}{3}\mathbb{Z}.$$

Therefore $\mathcal{O}_K \subset \frac{1}{3}\mathbb{Z}[\delta]$.

The coefficient of x^2 is $-T_{K/\mathbb{Q}}(\theta)$ and the constant term is $-N_{K/\mathbb{Q}}(\theta)$ so we only need to compute the coefficient of x, which is

$$\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 = \frac{(\theta_1 + \theta_2 + \theta_3)^2 - (\theta_1^2 + \theta_2^2 + \theta_3^2)}{2} = \frac{T_{K/\mathbb{Q}}(\theta)^2 - T_{K/\mathbb{Q}}(\theta^2)}{2}.$$

Since $\theta^2 = u^2 + 2vwd + \delta(2uv + w^2) + \delta^2(2uw + v^2)$ so

$$\frac{T_{K/\mathbb{Q}}(\theta)^2 - T_{K/\mathbb{Q}}(\theta^2)}{2} = \frac{(3u)^2 - (3u^2 + 6vwd)}{2} = 3(u^2 - vwd).$$

If $\theta \in \mathcal{O}_K$ then $3u, 3v, 3w \in \mathbb{Z}$ and we may assume they are $0, \pm 1$ by shifting θ by multiples of $1, \delta, \delta^2$. But also the field polynomial of θ should have integer coefficients. So we have

$$3(u^2 - vwd), \quad u^3 + v^3d + w^3d^2 - 3uvwd \in \mathbb{Z}.$$

If $3u = 0$, then $v, w = 0$ for any d. If $3u \neq 0$ then $3v, 3w \neq 0$. Let $3u = \pm 1$ then $3v, 3w = \pm 1$. Since $-d \equiv -1 \bmod 9$ if $d \equiv 1 \bmod 9$, and $d \mapsto -d$ corresponds to $\delta \mapsto -\delta$ and hence corresponds to $v \mapsto -v, w \mapsto w$. Therefore, we only need to check this for $v > 0$.

If $3u = 1, 3v = 1, 3w = 1$ we have

$$\frac{1}{3} - \frac{1}{3}d, \quad \frac{1}{27} + \frac{d}{27} + \frac{d^2}{27} - \frac{d}{9} \in \mathbb{Z}$$

which implies $d \equiv 1 \bmod 3$ and $(d-1)^2 \equiv 0 \bmod 27$. So $d \equiv 1 \bmod 9$. In this case, the element $\frac{1+\delta+\delta^2}{3}$ is indeed an algebraic integer. So when $d \equiv -1 \bmod 9$, the element $\frac{1-\delta+\delta^2}{3}$ is an algebraic integer.

If $3u = 1, 3v = 1, 3w = -1$ then

$$\frac{1}{3} + \frac{1}{3}d, \quad \frac{1}{27} + \frac{d}{27} - \frac{d^2}{27} + \frac{d}{9} \in \mathbb{Z}$$

and so $d \equiv -1 \bmod 3$ and $1 + 4d - d^2 \equiv 0 \bmod 27$. This is impossible. Similarly, the case $3v = -1, 3w = -1$ is impossible.

The cases $3u = -1$ correspond to cases $3u = 1$ by multiplying θ by -1 and so we do not need to check these. Therefore, when $d \not\equiv \pm 1 \bmod 9$, we have $u = 0$ and so $v, w = 0$. So $\{1, \delta, \delta^2\}$ is an integral basis. For the case $d \equiv \pm 1 \bmod 9$, we have an integral basis $\{1, \delta, (1 \pm \delta + \delta^2)/3\}$.

2. Let $k_1 = \mathbb{Q}(i), k_2 = \mathbb{Q}(\sqrt{2}), k_3 = \mathbb{Q}(\sqrt{2}i)$. Let $x \in K$ and write x as $\alpha' + \beta'\sqrt{2}$ where $\alpha' = a' + ib', \beta' = c' + id'$. Then

$$T_{K/k_1}(x) = 2a' + 2ib' \in \mathcal{O}_{k_1}, T_{K/k_2}(x) = 2a' + 2c'\sqrt{2} \in \mathcal{O}_{k_2}, T_{K/k_3}(x) = 2a' + 2d'i\sqrt{2} \in \mathcal{O}_{k_3}$$

and so $2a', 2b', 2c', 2d' \in \mathbb{Z}$. Write $a = 2a', b = 2b', c = 2c', d = 2d'$ so the algebraic integers are of the form $\frac{1}{2}(\alpha + \sqrt{2}\beta)$ where $\alpha = a + ib, \beta = c + id, a, b, c, d \in \mathbb{Z}$.

Let $k = \mathbb{Q}(i)$. Then

$$N_{K/k}(\theta) = \frac{1}{4}(a^2 - b^2 + 2abi - 2c^2 + 2d^2 - 4icd) \in \mathcal{O}_k = \mathbb{Z}[i].$$

This shows that

$$a^2 - b^2 - 2c^2 + 2d^2 \equiv 0 \bmod 4, \quad ab - 2cd \equiv 0 \bmod 2.$$

At least one of a, b is even. But if only one of them is odd, then $a^2 - b^2$ is odd and it is impossible that $a^2 - b^2 - 2c^2 + 2d^2 \equiv 0 \bmod 4$. So both a, b must be even and so $-2c^2 + 2d^2 \equiv 0 \bmod 4$, which means c, d have the same parity.

We now write $a = 2A, b = 2B$ where A, B are integers and so each algebraic integer must have the form

$$A + iB + \frac{((c + id)\sqrt{2}}{2}$$

where c, d have the same parity. The minimal polynomial of $\frac{(1+i)\sqrt{2}}{2}$ is $X^4 + 1$ so it is an algebraic integer. Therefore

$$\mathcal{O}_K \subset \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\sqrt{2} \oplus \mathbb{Z}\frac{(1+i)\sqrt{2}}{2} \subset \mathcal{O}_K$$

where the first inclusion comes from the fact that c, d have the same parity and the second inclusion comes from the fact $\frac{(1+i)\sqrt{2}}{2}$ is an algebraic integer. This forces $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\sqrt{2} \oplus \mathbb{Z}\frac{(1+i)\sqrt{2}}{2}$. In particular, $\{1, i, \sqrt{2}, \frac{1}{2}(1+i)\sqrt{2}\}$ is an integral basis.

$$\mathcal{D}_K = \begin{vmatrix} 1 & 1 & 1 & 1 \\ i & -i & i & -i \\ \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} \\ \frac{1}{2}(1+i)\sqrt{2} & \frac{1}{2}(1-i)\sqrt{2} & -\frac{1}{2}(1+i)\sqrt{2} & \frac{1}{2}(1-i)\sqrt{2} \end{vmatrix}^2 = 256.$$

3. Let $\{x_1, \ldots, x_n\}$ be an integral basis and $\{\sigma_1, \ldots, \sigma_n\}$ be the set of embeddings where $n = r+2s$. Let X be the matrix with entries $X_{ij} = \sigma_j(x_i)$. Then $\mathcal{D}_K = (\det X)^2$. Taking complex conjugate of X is the same as swapping s columns of X because there are $2s$ complex embeddings. So $\overline{\det X} = \det \bar{X} = (-1)^s \det X$. Multiply both sides by $\det X$ and we have

$$|\det X|^2 = (-1)^s (\det X)^2 = (-1)^s \mathcal{D}_K.$$

Since $|\det X|^2$ is a positive real number so the sign of $\mathcal{D}_K$ is $(-1)^s$.

4. (i) Let $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ be the roots of f. Then $f'(\theta) = \prod_{j\neq 1}(\theta - \theta_j)$. So

$$N_{K/\mathbb{Q}}(f'(\theta)) = \prod_{i=1}^{n} \prod_{j\neq i} (\theta_i - \theta_j) = (-1)^{\binom{n}{2}} disc(f).$$

(ii) $f'(\theta) = n\theta^{n-1} + a$ and $\theta^n = -a\theta - b$. So the matrix is

$$\begin{pmatrix} a & -bn & 0 & \cdots & 0 \\ 0 & a(1-n) & -bn & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ n & 0 & 0 & \cdots & a(1-n) \end{pmatrix}$$

and the norm $N_{K/\mathbb{Q}}(f'(\theta))$ is the determinant of this matrix, which is

$$a \begin{vmatrix} a(1-n) & -bn & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & a(1-n) & -bn \\ 0 & 0 & \cdots & a(1-n) \end{vmatrix} + (-1)^{n+1} \begin{vmatrix} -bn & 0 & \cdots & 0 \\ a(1-n) & -bn & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & a(1-n) & -bn \end{vmatrix}$$

and it is equal to $a^n(1-n)^{n-1} + n^n b^{n-1}$.

5. Let X be the matrix with entries $X_{ij} = \sigma_j(e_i)$. Then

$$(XX^t)_i j = \sum_{k=1}^{n} X_{ik} X_{jk} = \sum_{k=1}^{n} \sigma_k(e_i e_j) = T_{K/\mathbb{Q}}(e_i e_j) = T(e_i, e_j) = A_{ij}$$

and so $(\det X)^2 = \det A$.

6. $d = P - N$ where P is the sum of even permutations and N is the sum of odd permutations in the expression of the determinant. Let σ be any embedding of K and so if σ_i is another embedding, we must have $\sigma\sigma_i = \sigma_j$ for some j. Then σ either fixes P and N or swaps P and N. So $\sigma(P+N) = P+N$ and $\sigma(PN) = PN$ for all embeddings σ. Therefore, $P+N, PN \in \mathbb{Q}$. But the entries of the matrix are algebraic integers, so $P+N, PN \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$. Therefore

$$d^2 = (P+N)^2 - 4PN \equiv 0, 1 \bmod 4.$$

$X^3 - X + 2$ has discriminant $4 \cdot -26$. Since $\mathcal{D}_K$ cannot be 2 mod 4, so $\mathcal{D}_K$ has to be $4 \cdot -26$ and so the ring of integer is $\mathbb{Z}[\theta]$.

3 Chapter 3

1. We have seen that $P+Q$ is the greatest common divisor of P, Q and $P \cap Q$ is the least common multiple of P, Q, so
$$(P+Q)(P \cap Q) = PQ.$$
Since $P + Q = D$ so $PQ = P \cap Q$. Define
$$D \to D/P \times D/Q, \quad x \mapsto (x+P, x+Q).$$
The kernel is set of elements x such that $x \in P \cap Q = PQ$. We show this is surjective. Let $(y, z) \in D/P \times D/Q$. Since $P + Q = D$, take $p \in P, q \in Q$ such that $p + q = 1$ and let $x = yq + zp$. Then
$$x \mapsto (yq + P, zp + Q) = (y + P, z + Q).$$

2. We know $AA^{-1} = D$. Take c such that $cA^{-1} \subset D$ and let $B = cA^{-1}$ so $AB = \langle c \rangle$.

3. Let $\mathfrak{p}$ be any non-zero prime ideal and $x \in \mathfrak{p}$. x is not a unit and since D is a UFD we have
$$x = \prod_i p_i^{a_i}$$
where p_i are distinct prime (irreducible) elements. So $\langle p_i \rangle$ are prime ideals. Since $x \in \mathfrak{p}$, so $\mathfrak{p} | \langle x \rangle$ and so $\mathfrak{p} = \langle p_j \rangle$ for some j. So $\mathfrak{p}$ is principal and by unique factorisation, every non-zero ideal is principal.

4. We have
$$I^2 = \langle 4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5} \rangle = \langle 2 \rangle \langle 2, 1 + \sqrt{-5}, -2 + \sqrt{-5} \rangle = \langle 2 \rangle.$$
So $I^{-1} = I/2 = \langle 2, \frac{1+\sqrt{-5}}{2} \rangle$.

5. By question 1 it suffices to prove the statement when A is a prime power $\mathfrak{p}^a$. The only ideals in $D/\mathfrak{p}^a$ correspond to the ones in D containing $\mathfrak{p}^a$, so they have the form $\mathfrak{p}^i + \mathfrak{p}^a, 1 \leq i \leq a$. If $i = a$ then we have the zero ideal so there is nothing to prove. For $1 \leq i \leq a-1$, take $x \in \mathfrak{p}^i \backslash \mathfrak{p}^{i+1}$. So
$$\langle x \rangle + \mathfrak{p}^a = \mathfrak{p}^i$$
in D by considering the GCD. Therefore, in the quotient $D/\mathfrak{p}^a$ we have
$$\langle x \rangle + \mathfrak{p}^a = \mathfrak{p}^i + \mathfrak{p}^a$$
and so every ideal in the quotient is principal.

If $I = 0$ then $I = \langle 0 \rangle$. If not, let $0 \neq x \in I$ and so every ideal in $D/\langle x \rangle$ is principal. In particular, there exists y such that
$$y + \langle x \rangle = I + \langle x \rangle$$
and so $I = \langle x, y \rangle$.

6. We have seen that for each prime p there is some prime ideal $\mathfrak{p}$ which divides $\langle p \rangle$. So we only need to check that for p, q distinct prime numbers, the prime ideals $\mathfrak{p}, \mathfrak{q}$ are distinct where $\mathfrak{p} | \langle p \rangle, \mathfrak{q} | \langle q \rangle$.

Since $(p, q) = 1$, so $\langle p \rangle + \langle q \rangle = \mathcal{O}_K$. Therefore, $\mathfrak{p} \nmid \langle q \rangle$ by unique factorisation and so $\mathfrak{p} \neq \mathfrak{q}$.

7. (i) Let $I = \langle x_1, \ldots, x_k \rangle$ and since $xI \subset I$ we have $a_{ij} \in D$ such that

$$xx_i = \sum_j a_{ij} x_j.$$

Let A be the matrix with entries $A_{ij} = a_{ij}$, then

$$(xI - A) \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = 0.$$

So $xI - A$ is singular and the determinant of $xI - A$ is a monic polynomial of x with coefficients in D. So x is integral over D. But D is integrally closed so $x \in D$.

4 Chapter 4

1. Suppose I is not a prime then $I = AB$. Then $N(I) = N(A)N(B)$ is a composite number.

2. Since $\mathfrak{p} \nmid \langle a \rangle$, so $\langle a \rangle + \mathfrak{p} = \mathcal{O}_K$. So there exists $b \in \mathcal{O}_K$ such that $ab \equiv 1 \bmod \mathfrak{p}$ and so a reduces to a unit in $\mathcal{O}_K/\mathfrak{p}$. The order of $(\mathcal{O}_K/\mathfrak{p})^\times$ is $N(\mathfrak{p}) - 1$ because $(\mathcal{O}_K/\mathfrak{p})$ is a field. Therefore the result follows.

3. By Chinese remainder theorem and multiplicity of the norm, it suffices to prove the result when $I = \mathfrak{p}^a$ is a prime power.

   Let $x \in \mathcal{O}_K/\mathfrak{p}^a$. The ideals in $\mathcal{O}_K/\mathfrak{p}^a$ correspond to ideals in $\mathcal{O}_K$ containing $\mathfrak{p}^a$ and so they are of the form $\mathfrak{p}^i + \mathfrak{p}^a, 0 \leq i \leq a$. x is a unit if and only if x is not contained in any proper ideal. But we have

   $$\mathcal{O}_K + \mathfrak{p}^a \supset \mathfrak{p} + \mathfrak{p}^a \cdots \supset \mathfrak{p}^{a-1} + \mathfrak{p}^a \supset \langle 0 \rangle.$$

   So x is a unit if and only if $x \notin \mathfrak{p} + \mathfrak{p}^a$.

   The number of elements in $\mathfrak{p} + \mathfrak{p}^a$ is $\frac{N(\mathfrak{p}^a)}{N(\mathfrak{p})} = N(\mathfrak{p})^{a-1}$ by isomorphism theorem of quotients and so the number of units is

   $$N(\mathfrak{p})^a - N(\mathfrak{p})^{a-1} = N(\mathfrak{p}^a)\left(1 - \frac{1}{N(\mathfrak{p})}\right).$$

4. $m \in I$ so $I | \langle m \rangle$ and so for any prime $p | N(I)$ we have $p | m$. Consider the map

   $$\mathbb{Z}/m\mathbb{Z} \to \mathcal{O}_K/I, a + m\mathbb{Z} \mapsto a + I.$$

   It is well-defined because $m \in I$. If $x \in I \cap \mathbb{Z}$, then $x \in m\mathbb{Z}$ because m is the smallest positive integer in I. So the map is an injection and so $m | N(I)$. Therefore for any prime $p | m$ we have $p | N(I)$.

5. (i) There exist $\mathfrak{p} \subset \mathcal{O}_K$ such that $\mathfrak{p}^2$ divides $\langle p \rangle$ and by considering $\mathfrak{p}\mathcal{O}_L$, we conclude that p is also ramified in L.

   (ii) Let $x_1, \ldots, x_m$ generate $\mathcal{O}_L$ as an $\mathcal{O}_K$-module. If $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$ then we can write $x_i = \sum a_{ij} x_j$ for some $a_{ij} \in \mathfrak{p}$. Then the matrix a_{ij} is invertible and so the determinant is a unit. But $\det a_{ij} \in \mathfrak{p}$ so $\mathfrak{p}$ contains a unit, which is a contradiction.

   Suppose $I \neq J$ but $I\mathcal{O}_L = J\mathcal{O}_L$. Then there exists a prime ideal $\mathfrak{p}$ which divides $\frac{I}{J}$ or $\frac{J}{I}$ (one of them has to be contained in $\mathcal{O}_K$). Since $\frac{I}{J}\mathcal{O}_L = \frac{J}{I}\mathcal{O}_L = \mathcal{O}_L$, we have $\mathfrak{p}\mathcal{O}_L \supset \mathcal{O}_L$. But clearly $\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$. Thus $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$, which is a contradiction.

   (iii) Suppose we have two prime ideals in $\mathcal{O}_K$ above p, say P, Q. Then $P + Q = \mathcal{O}_K$ and so $P\mathcal{O}_L + Q\mathcal{O}_L = \mathcal{O}_L$. So any prime ideal above P is distinct from any prime ideal above Q in $\mathcal{O}_L$ and so we have at least two prime ideals above p, contradicting p is totally ramified. So there is a unique prime ideal in $\mathcal{O}_K$ above p.

   Let $\langle p \rangle \mathcal{O}_K = P^e \mathcal{O}_K$ and $\langle p \rangle \mathcal{O}_K = \mathfrak{p}^t \mathcal{O}_K$, where $t = [L : \mathbb{Q}]$ because p is totally ramified in L. So the residue degree of $\mathfrak{p}$ is 1. The natural map

   $$\mathcal{O}_K/P \to \mathcal{O}_L/\mathfrak{p}, x + P \mapsto x + \mathfrak{p}$$

   is an injection of fields because $\mathcal{O}_K \cap \mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ above p, and we have a unique one, which is P. Since $|\mathcal{O}_L/\mathfrak{p}| = p$ so $|\mathcal{O}_K/P| = p$, which means the residue degree of P is also 1. Therefore p is totally ramified in K.

6. Let ϕ be the Euclidean function on $\mathcal{O}_K$. Let x be the element such that $\phi(x)$ for $x \in \mathcal{O}_K \backslash \{0, \pm 1\}$. Then for any $y \in \mathcal{O}_K$, there exist q, r such that

$$y = qx + r, \text{ where } r = 0 \text{ or } \phi(r) < \phi(x).$$

So $r = 0$ or ± 1 and so $|\mathcal{O}_K/\langle x \rangle| \leq 3$.

7. (i) By Chinese remainder theorem, we can pick $x \in \mathcal{O}_K$ such that $x \in \mathfrak{p}_1$ with $x \notin \mathfrak{p}_i$ for $2 \leq i \leq k$. Since $\mathfrak{p}_1 | \langle x \rangle$ and $N_{K/\mathbb{Q}}(x) \in \mathbb{Q}$ so $p | N_{K/\mathbb{Q}}(x) = \prod_{\sigma \in G} \sigma(x)$. Since $\mathfrak{p}_i | \langle p \rangle$ for all i and so $\mathfrak{p}_i | \prod_{\sigma \in G} \langle \sigma(x) \rangle$ for all i. Therefore, for each i, there exists $\sigma \in G$ such that $\mathfrak{p}_i | \langle \sigma(x) \rangle$ and so $\sigma(x) \in \mathfrak{p}_i$. Then $x \in \sigma^{-1}(\mathfrak{p}_i)$. By construction $x \in \mathfrak{p}_1$ and $x \notin \mathfrak{p}_j$ for all $2 \leq j \leq k$. So $\sigma^{-1}(\mathfrak{p}_i) = \mathfrak{p}_1$. So for each i there exists $\sigma \in G$ such that $\sigma(\mathfrak{p}_1) = \mathfrak{p}_i$.

(ii) $\sigma \langle p \rangle = \langle p \rangle$ for all $\sigma \in G$ and by (i) for each i take σ such that $\sigma(\mathfrak{p}_1) = \mathfrak{p}_i$. By unique factorisation we must have $e_1 = e_i$ for each i.

Let $r = f_1$ and pick an $\mathbb{F}_p$-basis for $\mathcal{O}_K/\mathfrak{p}_1$, say $\{x_1, \ldots, x_r\}$. Take $\sigma \in G$ such that $\sigma(\mathfrak{p}_1) = \mathfrak{p}_i$. Since σ is an automorphism, so $\{\sigma(x_1), \ldots, \sigma(x_r)\}$ is an $\mathbb{F}_p$-basis for $\mathcal{O}_K/\mathfrak{p}_i$ and so $f_i = f_1 = r$.

8. p is a prime so $[K : \mathbb{Q}] = p - 1$ (by standard Galois theory).

(i) Pick a basis $\{\zeta_p, \ldots, \zeta_p^{p-1}\}$ and let $\alpha = \sum_i a_i \zeta_p^i$. If $j = 0$ then $Tr(\alpha) = -\sum_i a_i$. If $1 \leq j \leq p-1$, then

$$T_{K/\mathbb{Q}}(\zeta_p^j \alpha) = \sum_{i \neq p-j} -a_i + (p-1)a_{p-j}.$$

These must all be integers if α is an algebraic integer. Then taking differences between $T_{K/\mathbb{Q}}(\alpha)$ and $T_{K/\mathbb{Q}}(\zeta_p^j \alpha)$ for each j, we conclude that $pa_j \in \mathbb{Z}$ for each $1 \leq j \leq p-1$. Therefore, $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_K \subset \frac{1}{p}\mathbb{Z}[\zeta_p]$.

(ii) Since r, s are coprime to t so there exists t coprime to p such that $r \equiv st \bmod p$. Then $(1-\zeta_p^r)/(1-\zeta_p^s) = (1-\zeta_p^{st})/(1-\zeta_p^s) = 1+\zeta_p^s+\cdots+\zeta_p^{(t-1)s} \in \mathbb{Z}[\zeta_p]$. Similarly, $(1-\zeta_p^s)/(1-\zeta_p^r) \in \mathbb{Z}[\zeta_p]$ and so it is a unity. Then

$$\pi^{p-1} = (1-\zeta_p)^{p-1} = (1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1})\frac{1-\zeta_p}{1-\zeta_p^2}\cdots\frac{1-\zeta_p}{1-\zeta_p^{p-1}} = pu$$

where u is a unit.

(iii) $N_{K/\mathbb{Q}}(\pi) = p$ and so $\langle \pi \rangle$ is a prime ideal above p. So the images of $0, \ldots, p-1$ are distinct. Therefore it is surjective because $|\mathcal{O}_K/\langle \pi \rangle| = p$. Take a_0 such that $\alpha \equiv a_0 \bmod \pi$. a_0 exists since the above map is surjective. So $\alpha - a_0 = \pi\alpha_1$ for some α_1. Then take a_1 such that $\alpha_1 \equiv a_1 \bmod \pi$ and so $\alpha - a_0 = \pi(a_1 + \pi\alpha_2)$ for some α_2. Repeat this so that we have

$$\alpha \equiv a_0 + a_1\pi + \cdots + a_{m-1}\pi^{m-1} \bmod \pi^m \mathcal{O}_K.$$

(iv) Take $m = p-1$ in (iii) so $\alpha = a_0 + a_1\pi + \cdots + a_{p-2}\pi^{p-2} + \pi^{p-1}\beta$ for some $\beta \in \mathcal{O}_K$. By (ii) $\pi^{p-1} = pu$ and so

$$\alpha = a_0 + a_1\pi + \cdots + a_{p-2}\pi^{p-2} + p\gamma, a_i \in \mathbb{Z}, \gamma \in \mathcal{O}_K.$$

By (i), $\mathcal{O}_K \subset \frac{1}{p}\mathbb{Z}[\zeta_p]$ and so $p\gamma \in \mathbb{Z}[\zeta_p]$. This shows that $\alpha \in \mathbb{Z}[\zeta_p]$ and so $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

9. Write $g_i(X) = \frac{f(X)}{X-\theta_i}$ for each i and so $g_i(\theta_j) = f'(\theta_i)\delta_{ij}$.

So the polynomial

$$h(X) = \sum_{i=1}^{n} \frac{g_i(X)\theta_i^r}{f'(\theta_i)} = \sum_{i=1}^{n} \frac{f(X)\theta_i^r}{f'(\theta_i)(X-\theta_i)}.$$

We have $h(\theta_i) = \theta_i^r$ for each i and so $h(X) - X^r$ has n roots. But $h - X^r$ is a polynomial of degree at most $n-1$, so we conclude that

$$h(X) = X^r \text{ for each } 0 \leq r \leq n-1.$$

Now compare the coefficients of X^s on both sides, we conclude that

$$T_{K/\mathbb{Q}}\left(\frac{b_s\theta^r}{f'(\theta)}\right) = \delta_{rs}.$$

Therefore, the inverse different $\mathcal{D}_{K/\mathbb{Q}}^{-1}$ has a basis $\{\frac{b_s}{f'(\theta)} : s = 0, 1, \ldots, n-1\}$. But $b_{n-1} = 1$ so we conclude that

$$\mathcal{D}_{K/\mathbb{Q}}^{-1} = \langle \frac{1}{f'(\theta)} \rangle$$

and so the result follows.

10. It is clear that $\mathfrak{p}|\langle x\rangle$. So for each $r \geq e$ we have $\mathfrak{p}^r(\langle p\rangle/\mathfrak{p}^e)|\langle x^r\rangle$. So $p|x^r$ and so $p|T_{K/\mathbb{Q}}(x^r)$.
Now let $r = p^j$ for some j with $p^j > e$. Then

$$(T_{K/\mathbb{Q}}(x))^{p^j} \equiv T_{K/\mathbb{Q}}(x^{p^j}) \equiv 0 \bmod p.$$

Since $T_{K/\mathbb{Q}}(x)$ is an integer so $p|T_{K/\mathbb{Q}}(x)$.
This shows that $\langle p\rangle/\mathfrak{p}^{e-1} \subset p\mathcal{D}_{K/\mathbb{Q}}^{-1}$, and so

$$\langle p\rangle/\mathfrak{p}^{e-1}\mathcal{D}_{K/\mathbb{Q}} \subset (p\mathcal{D}_{K/\mathbb{Q}}^{-1})\mathcal{D}_{K/\mathbb{Q}} = \langle p\rangle$$

which implies $\mathcal{D}_{K/\mathbb{Q}} \subset \mathfrak{p}^{e-1}$.

11. (i) We have $\alpha^3 + \alpha^2 - 2\alpha + 8 = 0$ and so $8 + \frac{8}{\alpha} - \frac{16}{\alpha^2} + \frac{64}{\alpha^3} = 0$. Then $\beta^3 - \beta^2 + 2\beta + 8 = 0$ and so $\beta \in \mathcal{O}_K$. Suppose $\beta \in \mathbb{Z}[\alpha]$ then there exist $a, b, c \in \mathbb{Z}$ such that $\beta = \frac{4}{\alpha} = a + b\alpha + c\alpha^2$. So

$$c\alpha^3 + b\alpha^2 + a\alpha - 4 = 0$$

and since $\alpha^3 = -\alpha^2 + 2\alpha - 8$ so $\alpha^2(-c+b) + \alpha(a+2c) - 4 - 8c = 0$. This shows that $c = \frac{-1}{2}$ which is a contradiction. Since the discriminant of f has a squared factor 4, so $\mathcal{O}_K = \mathbb{Z}[\alpha]$, or $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 2$. But $\beta \in \mathcal{O}_K, \notin \mathbb{Z}[\alpha]$ so $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$ because $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is at most 2.
(ii) Since $[K : \mathbb{Q}] = 3$ so $\{1, \alpha, \beta\}$ is an integral basis for $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$. So each element can be written uniquely as $a + b\alpha + c\beta$ for some $a, b, c \in \mathbb{Z}$. Define $\theta : \mathcal{O}_K \to \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$ by $\theta(a + b\alpha + c\beta) = (\bar{a}, \bar{a} + \bar{b}, \bar{a} + \bar{c})$ where $\bar{a}$ is a mod 2 for any $a \in \mathbb{Z}$. It is clearly surjective. We can check that $\alpha^2 = 2 - \alpha + 2\beta$ and $\beta^2 = -2 - 2\alpha + \beta$. So

$$\begin{aligned}\theta((a + b\alpha + c\beta)(a_1 + b_1\alpha + c_1\beta)) &= (aa_1, aa_1 + ab_1 + ba_1 + b_b1, aa_1 + ac_1 + a_1c + cc_1) \\ &= (aa_1, (a+b)(a_1+b_1), (a+c)(a_1+c_1))\end{aligned}$$

which is the same as $(a, a+b, a+c)(a_1, a_1+b_1, a_1+c)$.

$$\theta((a + b\alpha + c\beta) + (a_1 + b_1\alpha + c_1\beta)) = (a + a_1, a + a_1 + b + b_1, a + a_1 + c + c_1)$$

which is the same as $(a, a+b, a+c)+(a_1, a_1+b_1, a_1+c_1)$. Therefore this is a ring homomorphism. The kernel is the set of elements $a+b\alpha+c\beta$ with a, b, c even so the kernel is $2\mathcal{O}_K$. Alternatively, we can pick a basis $\{c_0, c_1, c_2\}$ for $\mathbb{Z}[\alpha, \beta]$ where $c_0 = 1 + \alpha + \beta, c_1 = \alpha, c_2 = \beta$. Then we have

$$c_0c_1 \equiv c_0c_2 \equiv c_1c_2 \equiv 0 \bmod 2$$

so sending $ac_0 + bc_1 + cc_2$ to $(\bar{a}, \bar{b}, \bar{c})$ gives a ring isomorphism.

We consider all possible ramification behavior of 2. Suppose $\langle 2 \rangle$ is a prime, then $\mathcal{O}_K/2\mathcal{O}_K$ is a field. Suppose $\langle 2 \rangle$ is ramified then $\mathcal{O}_K/2\mathcal{O}_K$ has nilpotent elements. Suppose $\langle 2 \rangle$ splits into a product of two primes, then $\mathcal{O}_K/2\mathcal{O}_K$ is a product of two fields. Finally if $\langle 2 \rangle$ splits completely then it is a product of three fields. So we conclude $\langle 2 \rangle$ splits completely.

(iii) If $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some algebraic integer θ with minimal polynomial g. Then by Kummer-Dedekind the factorisation of $\langle 2 \rangle$ is determined by g mod 2. However, there are only two distinct linear factors in $\mathbb{F}_2[X]$. So this implies $\langle 2 \rangle$ does not split completely, which is a contradiction.

5 Chapter 5

1. (i) If $\mathfrak{p} = \langle p, \sqrt{-d}\rangle$ then $\mathfrak{p}^2 = \langle p\rangle\langle p, \sqrt{-d}, -d/p\rangle$. Since d is square free so p is coprime to $-d/p$ and so $\langle p, \sqrt{-d}, -d/p\rangle = \langle 1\rangle$. Therefore $\mathfrak{p}^2 = p$. $\mathcal{O}_K$ is either $\mathbb{Z}[\sqrt{-d}]$ or $\mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$. So the norms are of the form $a^2 + b^2d$ or $a^2 + ab + \frac{1+d}{4}b^2$. Suppose the norm of some element is equal to p. Then either $a^2 + b^2d = p$, but $d > p$ so $b = 0, a^2 = p$ which is impossible; or $a^2 + ab + \frac{1+d}{4}b^2 = p$, then $(2a + b)^2 + db^2 = 4p$. Since d is composite so $d > p$. Therefore we must have $b^2 < 4$ so $b = 0$ or ± 1. If $b = 0$ then $4a^2 = 4p$ gives a contradiction. If $b = \pm 1$ then we have $(2a \pm 1)^2 = 4p - d$. Since $-d \equiv 1 \bmod 4$ so d is odd and since d is composite so $d \geq 3p$. If $d = 3p$ then $(2a \pm 1)^2 = p$ which gives a contradiction. Since d is square free so $d \neq 4p$. So then we have $d \geq 5p$, in which case $(2a \pm 1)^2 = 4p - d \leq -p$ and this also gives a contradiction.

   (ii) If $d = 1$ then $\langle 2\rangle = \langle 1 + i\rangle^2$ and if $d = 2$ then $\langle 2\rangle = \langle\sqrt{-2}\rangle^2$. If $d \neq 1, 2$ and $d \equiv 1$ or $2 \bmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$. If d is odd, let $\mathfrak{p} = \langle 2, 1 + \sqrt{-d}\rangle$. We have

$$\mathfrak{p}^2 = \langle 2\rangle\langle 2, 1 + \sqrt{-d}, \frac{1-d}{2} + \sqrt{-d}\rangle.$$

   Since $d \equiv 1 \bmod 4$ so $\frac{1-d}{2}$ is even and so $1 + \sqrt{-d} - (\frac{1-d}{2} + \sqrt{-d})$ is odd. Therefore $\mathfrak{p}^2 = \langle 2\rangle$. If d is even, let $\mathfrak{p} = \langle 2, \sqrt{-d}\rangle$ then

$$\mathfrak{p}^2 = \langle 2\rangle\langle 2, \sqrt{-d}, \frac{-d}{2}\rangle.$$

   Since $d \equiv 2 \bmod 4$ so $\frac{-d}{2}$ is odd. So $\mathfrak{p}^2 = \langle 2\rangle$. These are not principal because the norms are $a^2 + b^2d$ which cannot be equal to 2 when $d \neq 1, 2$.

   (iii) If $d \equiv 7 \bmod 8$, then let $\mathfrak{p} = \langle 2, \frac{1+\sqrt{-d}}{2}\rangle$. Then

$$\mathfrak{p}\bar{\mathfrak{p}} = \langle 2\rangle\langle 2, \frac{1+\sqrt{-d}}{2}, \frac{1-\sqrt{-d}}{2}, \frac{1+d}{8}\rangle.$$

   $1 = \frac{1+\sqrt{-d}}{2} + \frac{1-\sqrt{-d}}{2}$ so $\mathfrak{p}\bar{\mathfrak{p}} = \langle 2\rangle$. If $d = 7$ then $\mathfrak{p} = \langle 2, \frac{1+\sqrt{-7}}{2}\rangle = \langle\frac{1+\sqrt{-7}}{2}\rangle$ because $2 = \frac{1+\sqrt{-7}}{2}\frac{1-\sqrt{-7}}{2}$. If $d > 7$, the norms are $a^2 + ab + \frac{1+d}{4}b^2$ and if it is equal to 2 then

$$(2a + b)^2 + db^2 = 8.$$

   $d > 7$ and d is odd so $d > 8$. Then $b = 0$ and $(2a)^2 = 8$ which is impossible.

   By (i),(ii),(iii) if K has class number 1 then either $d = 1, 2$ or 7 or d is a prime and $d \equiv 3 \bmod 8$.

2. As m is even so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-m}]$. Since the class number is prime to 3, therefore we conclude that

$$y + \sqrt{-m} = (a + b\sqrt{-m})^3$$

   and so by comparing the coefficients of $\sqrt{-m}$ we have

$$1 = (3a^2 - b^2m)b$$

   and so $b = \pm 1$. So we have $3a^2 - m = 1$ or $3a^2 - m = -1$ and at most one of these have solutions because we require $1 + m$ or $-1 + m$ to be a multiple of 3. Thus at most one of these holds and so we have at most one solution for b and then two solutions for a.

3. The Minkowski's bound is < 4. By Dedekind's creterion, we have

$$\langle 2\rangle = \langle 2, \sqrt{14}\rangle^2, \quad \langle 3\rangle \text{ inerts }.$$

There is an element of norm 2, which is $4+\sqrt{14}$ so $\langle 2, \sqrt{14}\rangle = \langle 4+\sqrt{14}\rangle$ is principal. Therefore the class group is trivial.

4. The Minkoski's bound $c_K \geq 1$, and $c_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\mathcal{D}_K|}$, so

$$|\mathcal{D}_K| \geq \left(\frac{\pi}{4}\right)^{2s} \frac{n^{2n}}{(n!)^2}.$$

By Stirling's formula, we have

$$|\mathcal{D}_K| \geq e^{2n-\frac{\theta}{6n}} \left(\frac{\pi}{4}\right)^{2s} \frac{1}{2\pi n}.$$

Since $\frac{e\pi}{4} > 1$ and $2s \leq 2n$ so

$$|\mathcal{D}_K| \geq \left(\frac{e\pi}{4}\right)^{2n-\frac{\theta}{6n}} \frac{1}{2\pi n} \to \infty$$

as $n \to \infty$.

5. Minkowski's bound is < 4. Since $-31 \equiv 1 \bmod 4$ so $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-31}}{2}]$. The minimal polynomial of $\frac{1+\sqrt{-31}}{2}$ is $X^2 - X + 8$. By Dedekind's criterion we have

$$\langle 2\rangle = \mathfrak{p}_2\mathfrak{q}_2, \quad \langle 3\rangle \text{ inerts.}$$

The element $\frac{1+\sqrt{-31}}{2}$ has norm 8 and it is not divisible by 2. So it is either $\mathfrak{p}^3$ or $\mathfrak{q}^3$. Further, $[\mathfrak{q}] = [\mathfrak{p}]^{-1}$ so the class group is cyclic. Since there is no element of norm 2, $\mathfrak{p}_2, \mathfrak{q}_2$ are not principal. So the class group is cyclic of order 3.

Suppose y is even, then $y^2 + 31 \equiv 3 \bmod 4$ and so $x \equiv 3 \bmod 4$. Then

$$y^2 + 4 = x^3 - 27 = (x-3)(x^2+3x+9).$$

Since $x^2 + 3x + 9 \equiv 3 \bmod 4$, there is a prime $p | x^2 + 3x + 9$ which is 3 mod 4. So $y^2 + 4 \equiv 0 \bmod p$ and so -4 is a square mod p, which is a contradiction. So y is odd and x is even. In particular, $(y + \sqrt{-31})/2 \in \mathcal{O}_K$.

Consider now

$$\langle (y+\sqrt{-31})/2\rangle\langle (y-\sqrt{-31})/2\rangle = \langle 2\rangle\langle x/2\rangle^3.$$

Then $\langle (y+\sqrt{-31})/2\rangle, \langle (y-\sqrt{-31})/2$ must be coprime and since 2 splits, so we must have

$$\langle (y+\sqrt{-31})/2\rangle = \mathfrak{p}_2 I^3$$

for some ideal I. But I^3 is principal because the class number is 3, and this implies that $\mathfrak{p}_2$ is principal, which is a contradiction. So we conclude that the equation has no integer solution.

6. $1175 = 25 \cdot 47$. Let $K = \mathbb{Q}(\sqrt{-47})$. Minkoski's bound is < 5. Let $\alpha = (1+\sqrt{-47})/2$. So $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and α has minimal polynomial $X^2 - X + 12$. By Dedekind's criterion, we have

$$\langle 2\rangle = \langle 2, \alpha\rangle\langle 2, \alpha - 1\rangle, \quad \langle 3\rangle = \langle 3, \alpha\rangle\langle 3, \alpha - 1\rangle.$$

The element α has norm 12, and it is not divisible by $2, 3$, but contained in $\langle 2, \alpha\rangle, \langle 3, \alpha\rangle$, so

$$\langle \alpha\rangle = \langle 2, \alpha\rangle^2\langle 3, \alpha\rangle.$$

By writing $[\langle 2, \alpha - 1\rangle] = [\langle 2, \alpha - 1\rangle]^{-1}$, $[\langle 3, \alpha - 1\rangle] = [\langle 3, \alpha\rangle]^{-1}$, we conclude that the class group is generated by $\langle 2, \alpha\rangle, \langle 3, \alpha\rangle$ and we have

$$[\langle 2, \alpha\rangle]^2[\langle 3, \alpha\rangle] = 1$$

so $[\langle 3, \alpha\rangle] = [\langle 2, \alpha\rangle]^{-2}$. The class group must be cyclic. Further, $2 + \alpha$ has norm 18 and it is contained in $\langle 2, \alpha\rangle, \langle 3, \alpha - 1\rangle$ so

$$1 = [\langle 2 + \alpha\rangle] = [\langle 2, \alpha\rangle][\langle 3, \alpha - 1\rangle]^2 = [\langle 2, \alpha\rangle][\langle 3, \alpha\rangle]^{-2} = [\langle 2, \alpha\rangle]^5.$$

Therefore, $[\langle 2, \alpha\rangle]$ has order 5 and the class group is cyclic of order 5.

Now y must be odd and so we can write

$$\langle (y + 5\sqrt{-47})/2\rangle\langle (y - 5\sqrt{-47})/2\rangle = \langle x\rangle^3.$$

Since $\langle (y + 5\sqrt{-47})/2\rangle, \langle (y - 5\sqrt{-47})/2\rangle$ are coprime, so

$$\langle (y + 5\sqrt{-47})/2\rangle = I^3$$

for some ideal I. But the class number is coprime to 3, so I is principal and so

$$\frac{y + 5\sqrt{-47}}{2} = (\frac{a + b\sqrt{-47}}{2})^3.$$

Expand this and compare the coefficients of $\sqrt{-47}$ we conclude that

$$20 = b(3a^2 - 47b^2).$$

Reduce both sides mod 3 we see that $b \equiv 2 \bmod 3$, so $b = -1, 2, 5, -4, -10$. The only one for this to work is $b = -1$ and $a = \pm 3$. This gives $x = \pm 99, y = 14$.

7. Let h be the class number of K. Take representatives $I_1, \ldots, I_h$ of the class group. Then I_j^h is principal for each j and let $I_j^h = \langle a_j\rangle$ for some $a_j \in K$. Let $L = K(\sqrt[h]{a_j}, j = 1, \ldots, h)$. Then for each ideal $\mathfrak{a} \subset \mathcal{O}_K$, there exists $b \in \mathcal{O}_K$ and $j \leq n$ such that

$$\mathfrak{a} = \langle b\rangle I_j.$$

Then $\mathfrak{a}^h = \langle b^h\rangle I_j^h = \langle b^h\rangle\langle a_j\rangle$ and so

$$\mathfrak{a}^h\mathcal{O}_L = \langle b^h\rangle\langle \sqrt[h]{a_j}\rangle^h.$$

By unique factorisation of ideals we conclude that

$$\mathfrak{a}\mathcal{O}_L = \langle b\rangle\langle \sqrt[h]{a_j}\rangle = \langle b\sqrt[h]{a_j}\rangle$$

is principal.

8. The first part follows from Dedekind's criterion. Suppose $\prod_i \mathfrak{p}_i^{r_i}$ is principal. Since $m \not\equiv 3 \bmod 4$, then there exists an element of norm $\prod_i \mathfrak{p}_i^{r_i}$ and so we have integers a, b such that $a^2 + b^2m = \prod_i \mathfrak{p}_i^{r_i}$. If $r_i \neq 0$ for some i, and $r_j \neq 1$ for some j, then $\prod_i p_i^{r_i}$ is strictly between 0 and m. Then $b = 0$ and $a^2 = \prod_i \mathfrak{p}_i^{r_i}$ which is impossible.

This shows that if r_i are not all equal to zero or one then the product is not principal. If $r_i = 0$ for all i then it is clear that the product is principal. If $r_i = 1$ for all i, then $\prod_i \mathfrak{p}_i = \langle\sqrt{-m}\rangle$ because $\sqrt{-m}$ must be a product of prime ideals with norm dividing m, and for each $p|m$, there is only one prime ideal with norm p. Finally, the above shows that $[\mathfrak{p}_1], \ldots, [\mathfrak{p}_{k-1}]$ generate a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{k-1}$.

9. (i) We have $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ and so one of p, q is 1 mod 4. Assume $p \equiv 1 \bmod 4$. Let u' be an odd integer such that

$$u'^2 \equiv p^{-1} \bmod q$$

and so $q|pu'^2 - 1$. Also, $4|pu'^2 - 1$ and so $4q|pu'^2 - 1$. Let $u = pu'$ so $4q|u^2 - p$. Similarly, pick v' such that

$$v'^2 \equiv q^{-1} \bmod p$$

and let $v = pv'$.

(ii) If $(x_i, y_i, z_i) \in \Lambda$, $i = 1, 2$, then it is clear that $2|z_1 + z_2$. We have

$$x_i \equiv uy_1 + vz_1 \bmod 2pq$$

and so

$$x_1 + x_2 \equiv u(y_1 + y_2) + v(z_1 + z_2) \bmod 2pq.$$

So Λ is an additive subgroup of $\mathbb{R}^3$. It is easy to see that

$$\mathbb{Z}(u, 1, 0) \oplus \mathbb{Z}(2v, 0, 2) \oplus \mathbb{Z}(0, 2q, 2p) \subset \Lambda$$

and so it has rank 3 over $\mathbb{R}$. So it is a lattice.

We have

$$x^2 - py^2 - qz^2 \equiv (u^2 - p)y^2 + (v^2 - q)z^2 + 2uvyz \bmod 2pq.$$

Since $q|u^2 - p, q|v$ so $q|x^2 - py^2 - qz^2$. Similarly, $p|x^2 - py^2 - qz^2$ and so $pq|x^2 - py^2 - qz^2$.

Since $4|z^2$, and so $x^2 - py^2 - qz^2 \equiv x^2 - py^2 \bmod 4$. But $x^2 \equiv uy^2 \bmod 4$ and $4|u - p$, so $4|x^2 - py^2 - qz^2$.

(iii) The volume of X is $m(X) = 2^3 \cdot \frac{4\pi pq}{3}$. Consider

$$\Lambda_1 = \{(x, y, z) : z \equiv 0 \bmod 2\}.$$

Then the covolume of Λ_1 is 2. Now the index of Λ in Λ_1 is $2pq$ because we only have a congruence condition on x and we are free to pick any y, z. So the covolume of Λ is $4pq$. Since $\pi > 3$ so $m(X) > 2^3\mathrm{cov}(\Lambda)$. Then by Minkowski's convex body theorem, there is a non-zero element $(x, y, z) \in \Lambda \cap X$. So

$$x^2 + py^2 + qz^2 < 4pq$$

and by (ii)

$$x^2 - py^2 - qz^2 \equiv 0 \bmod 4pq.$$

It is clear that $x^2 - py^2 - qz^2 \leq 4pq$ because $x^2 + py^2 + qz^2 < 4pq$. Suppose $x^2 - py^2 - qz^2 \leq -4pq$ then

$$-x^2 + py^2 + qz^2 \geq 4pq$$

and so $x^2 + py^2 + qz^2 > 4pq$ which is a contradiction. So

$$|x^2 - py^2 - qz^2| < 4pq, \quad x^2 - py^2 - qz^2 \equiv 0 \bmod 4pq.$$

So $x^2 - py^2 - qz^2 = 0$ which gives a non-trivial solution.

10. (i) $f(x - 1)$ is 3-Eisenstein so it is irreducible. Discriminant of f is 81.

(ii) Since $\alpha^3 = 3\alpha - 1$, so

$$\langle \alpha + 1 \rangle^3 = \langle \alpha^3 + 3\alpha^2 + 3\alpha + 1 \rangle = \langle 3\alpha^2 + 6\alpha \rangle = \langle 3 \rangle \langle \alpha^2 + 2\alpha \rangle.$$

It is easy to see that $N_{K/\mathbb{Q}}(\alpha) = -1$ and $N_{K/\mathbb{Q}}(\alpha+2) = 1$ so $\alpha^2 + 2\alpha$ is a unit. Therefore, $\langle \alpha + 1 \rangle^3 = \langle 3 \rangle$. The residue field is $\mathbb{F}_3$ by considering the norm.

The map $\mathbb{Z} \mapsto \mathcal{O}_K/\mathfrak{p}$ is surjective as the images of $0, 1, 2$ are distinct. Then for each $\beta \in \mathcal{O}_K$, we can write (by induction)

$$\beta = a_0 + a_1(1+\alpha) + a_2(1+\alpha)^2 + (1+\alpha)^3\gamma$$

for some $\gamma \in \mathcal{O}_K$. Since $(1+\alpha)^3 = 3u$ where u is a unit, so $\beta = a_0 + a_1(1+\alpha) + a_2(1+\alpha)^2 + 3\gamma'$ for some $\gamma' \in \mathcal{O}_K$. Therefore $\mathcal{O}_K \subset \mathbb{Z}[\alpha] + 3\mathcal{O}_K$. Since $\mathbb{Z}[\alpha] + 3\mathcal{O}_K \subset \mathcal{O}_K$ so we have $\mathcal{O}_K = \mathbb{Z}[\alpha] + 3\mathcal{O}_K$.

(iii) By (i) $\mathcal{D}_K = 1, 9$ or 81. But $K \neq \mathbb{Q}$ so $\mathcal{D}_K \neq 1$. Therefore, $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$ or 3 and so $3\mathcal{O}_K \subset \mathbb{Z}[\alpha]$. So by (ii)

$$\mathcal{O}_K = \mathbb{Z}[\alpha] + 3\mathcal{O}_K \subset \mathbb{Z}[\alpha] \subset \mathcal{O}_K$$

and so $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

The Minkowski's bound is < 3. Since $x^3 - 3x + 1$ is irreducible mod 2, therefore $\langle 2 \rangle$ is a prime and so K has class number 1.

6 Chapter 6

1. (i) $2+\sqrt{3}$. The element $4+\sqrt{3}$ has norm 13 and so the solutions are given by

$$x+\sqrt{3}y = \pm(2+\sqrt{3})^n(4+\sqrt{3}), n \in \mathbb{Z}$$

(ii) $3+\sqrt{10}$. Note that the norm of $3+\sqrt{10}$ is -1. The element $2+\sqrt{10}$ has norm -6 and so the solutions are given by

$$x+\sqrt{10}y = \pm(3+\sqrt{10})^n(2+\sqrt{10}), n \text{ odd }.$$

2. If $|\sigma_i(u)| = 1$ for all i then the image of u is 0 under the log map

$$L : \mathcal{O}_K \backslash \{0\} \to \mathbb{R}^{r+s}.$$

Moreover, $L^{-1}(\{0\})$ is finite and the subgroup generated by u is in $L^{-1}(\{0\})$. Therefore u has finite order and so $u \in \mu_K$.

3. Since L is totally real, so complex conjugation commutes with any embedding of L, and the embeddings of K are of the form $\sigma\tau$ where τ is the complex conjugation, σ is a real embedding of L. It is clear that for each $\alpha \in U_K$,

$$\left|\sigma\tau\left(\frac{\alpha}{\tau(\alpha)}\right)\right| = 1$$

and so α is a root of unity by the previous question. So the image of λ is inside μ_K.

Therefore, we can define a map

$$\delta : U_K \to \mu_K/\mu_K^2, \quad \alpha \mapsto \lambda(\alpha) + \mu_K^2.$$

Suppose α is in the kernel of δ, then $\lambda(\alpha) = z^2$ where $z \in \mu_K$. But $1/\bar{z} = z$ and so we have

$$\frac{\alpha}{z} = \frac{\bar{\alpha}}{\bar{z}}$$

and so $\frac{\alpha}{z}$ is a real unit. So $\alpha \in \mu_K U_L$.

Conversely, if $\alpha \in \mu_K U_L$, then $\alpha = zu$ for some $z \in \mu_K$ and $u \in U_L$. Then $\lambda(\alpha) = \frac{z}{\bar{z}} = z^2$ and so α is in the kernel of δ. So we conclude that

$$U_K/\mu_K U_L \hookrightarrow \mu_K/\mu_K^2$$

and so $[U_K : \mu_K U_L] = 1$ or 2 because μ_K is a cyclic group.

4. $[K : \mathbb{Q}] = 4$. Let $f(X) := (X-\zeta_8)(X-\zeta_8^3)(X-\zeta_8^5)(X-\zeta_8^7) = X^4+1$. $N(1-\zeta_8) = (1-\zeta_8)(1-\zeta_8^3)(1-\zeta_8^5)(1-\zeta_8^7) = f(1) = 2$. So $N(\mathfrak{p}) = 2$. $\mathfrak{p}^2$ has norm 4.

Note that $0, 1, \zeta_8, 1-\zeta_8$ are distinct elements in $\mathcal{O}_K/\mathfrak{p}^2$ (by considering the differences of them, which are not in $\mathfrak{p}^2$). So $\mathcal{O}_K/\mathfrak{p}^2 = \{0, 1, \zeta_8, 1-\zeta_8\}$. We have $(1-\zeta_8)^2 = (1+i)(1-\sqrt{2}) = \sqrt{2}\frac{1+i}{\sqrt{2}}(1-\sqrt{2})$ where $\frac{1+i}{\sqrt{2}}(1-\sqrt{2})$ is a unit. Since $\zeta_8 - \zeta_8^{-1} = i\sqrt{2}$ so $\zeta_8 \equiv \zeta_8^{-1} \bmod \mathfrak{p}^2$. So complex conjugation acts trivially.

The rank of U_K is 1. K is a CM field with $L = \mathbb{Q}(\zeta_8 + \zeta_8^{-1})$. So $[U_K : \mu_K U_L] = n$ where $n = 1$ or 2. Since $1+\sqrt{2}$ is a fundamental unit of L, there exists $\alpha \in U_K$ such that

$$\alpha^n = \zeta_8^i(1+\sqrt{2}), n = 1, 2.$$

Let $\alpha = re^{i\theta}$ and then $\frac{\alpha}{\bar{\alpha}} = e^{2i\theta} \in K$. But $\frac{\alpha^n}{\bar{\alpha}^n} = \zeta_8^{2i}$ where $n = 1$ or 2 so $e^{2i\theta}$ is a root of unity in K. Since α is a unit and complex conjugation acts trivially on $\mathcal{O}_K/\mathfrak{p}^2$, so

$$1 \equiv \frac{\alpha}{\bar{\alpha}} = e^{2i\theta} \bmod \mathfrak{p}^2.$$

If $e^{2i\theta} = \zeta_8^j$ where $j = 1, 3, 5, 7$ then the above congruence fails to hold and so $e^{2i\theta}$ is a 4th root of unity. So $e^{i\theta} \in K$ and $\beta = \alpha e^{-i\theta} \in K \cap \mathbb{R}$. Then taking complex norms we have

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

and so this forces n to be 1 because β is a real unit. Therefore, $1 + \sqrt{2}$ is a fundamental unit.

5. $N_{K/L}(1+\zeta_{12}) = (1+\zeta_{12})(1+\zeta_{12}^{11}) = 2 + 2\cos(\pi/6) = 2 + \sqrt{3}$. So $1 + \zeta_{12}$ is a unit. U_K has rank 1 and K is a CM field. So $[U_K : \mu_K U_L] = 1$ or 2. But $1 + \zeta_{12}$ is a unit, which is not in $\mu_K U_L$, otherwise the norm will be at least the square of a fundamental unit in U_L. Therefore, $1 + \zeta_{12}$ is a fundamental unit.

6. (i) We have

$$\begin{aligned} f(x) &= x^2 + 4 - \sin^2\theta(x^2 + 4\cos^2\theta - 4x\cos\theta), \\ &= x^2\cos^2\theta + 4x\sin^2\theta\cos\theta + 4(1 - \sin^2\theta\cos^2\theta) \\ &= (x\cos\theta + 2\sin^2\theta)^2 + 4 - 4\cos^2\theta\sin^2\theta - 4\sin^4\theta \\ &= (x\cos\theta + 2\sin^2\theta)^2 + 4(1 - \cos^2\theta\sin^2\theta - \sin^4\theta) \\ &= (x\cos\theta + 2\sin^2\theta)^2 + 4\cos^2\theta > 0 \end{aligned}$$

(ii) The norm of u is ± 1 and so $ur^2 = \pm 1$. Since $u > 1$ and $r > 0$, we conclude that $ur^2 = 1$ and so $u = \frac{1}{r^2}$. The discriminant of $\mathbb{Z}[u]$ is

$$\begin{aligned} \begin{vmatrix} 1 & u & u^2 \\ 1 & re^{i\theta} & r^2e^{2i\theta} \\ 1 & re^{-i\theta} & r^2e^{-2i\theta} \end{vmatrix}^2 &= ((r^3e^{-i\theta} - r^3e^{i\theta}) - u(r^2e^{-2i\theta} - r^2e^{2i\theta}) + u^2(re^{-i\theta} - re^{i\theta}))^2 \\ &= (-2ir^3\sin\theta + 2ur^2\sin(2\theta) - 2u^2r\sin\theta)^2 \\ &= (-2ir^3\sin\theta + 2\sin(2\theta) - 2r^{-3}\sin\theta)^2 \\ &= -4\sin^2\theta(r^3 + r^{-3} - 2\cos\theta)^2. \end{aligned}$$

By (i), if we set $x = r^3 + r^{-3}$ then

$$4\sin^2\theta(r^3 + r^{-3} - 2\cos\theta) < 4((r^3 + r^{-3})^2 + 4) = 4(u^3 + u^{-3} + 6).$$

(iii) Since $|\mathcal{D}_K| \leq \mathrm{disc}(\mathbb{Z}[u]) < 4(u^3 + u^{-3} + 6)$, so

$$u^6 - \left(\frac{|\mathcal{D}_K|}{4} - 6\right)u^3 + 1 > 0$$

and so

$$\left(u^3 - \left(\frac{|\mathcal{D}_K|}{8} - 3\right)\right)^2 > \left(\frac{|\mathcal{D}_K|}{8} - 3\right)^2 - 1.$$

Since $|\mathcal{D}_K| > 32$, so

$$\left(\frac{|\mathcal{D}_K|}{8} - 3\right)^2 > \left(\frac{|\mathcal{D}_K|}{8} - \frac{15}{4}\right)^2$$

and so the statement follows by taking square roots.

Suppose $u^3 - \left(\frac{|\mathcal{D}_K|}{8} - 3\right) < -\frac{|\mathcal{D}_K|}{8} + \frac{15}{4}$ then $u^3 < \frac{3}{4}$ which is a contradiction. So

$$u^3 > \frac{|\mathcal{D}_K| - 27}{4}.$$

(iv) The discriminant is -83 so it has one real embedding and two complex embeddings. Moreover, $|\mathcal{D}_K| = 83$. If θ is a root, then $\theta^3 - \theta^2 + \theta - 1 = 1$ and so

$$(1 + \theta^2)(\theta - 1) = 1.$$

So $1 + \theta^2$ is a unit. By (iii) if u is a fundamental unit, then

$$u^3 > \frac{83 - 27}{4} = 14$$

and so $u^2 > 14^{\frac{2}{3}}$. But $1 + \theta^2 < 5$ and so

$$1 < 1 + \theta^2 < u^2.$$

This implies that $1 + \theta^2 = u$ is a fundamental unit.

7. Let $\bar{\gamma}$ be the conjugate of γ. Suppose $N_{K/\mathbb{Q}}(u) = 1$, then $u\bar{u} = 1$ and so $\bar{\gamma} = u\gamma$. This shows that $\langle\gamma\rangle = \langle\bar{\gamma}\rangle$. For each prime ideal $\mathfrak{q}|\langle\gamma\rangle$, we conclude that $\bar{\mathfrak{q}}$ also divides $\langle\gamma\rangle$. So we have the following possible cases.

   Suppose $\mathfrak{q} = \langle q\rangle$ then this implies $q|\gamma$, contradicting the definition of m. Suppose $\mathfrak{q} \neq \bar{\mathfrak{q}}$ then

   $$\langle q\rangle = \mathfrak{q}\bar{\mathfrak{q}}|\langle\gamma\rangle$$

   again contradicting the definition of m. So the only possible case is $\mathfrak{q}^2 = \langle q\rangle$. This means q is ramified and since $p \equiv 1 \bmod 4$, $q = p$ because $\mathcal{D}_K = p$ so the only ramified prime is p. Also $\langle q\rangle = \langle\sqrt{p}\rangle$ and so

   $$\langle\gamma\rangle = \langle\sqrt{p}\rangle^j$$

   for some j. If $j \geq 2$ then $p|\gamma$ which again gives a contradiction. So $j \leq 1$.

   If $j = 0$, then γ is a unit and so $N_{K/\mathbb{Q}}(\gamma\bar{\gamma}) = \pm 1$ and we have

   $$u = \frac{\gamma}{\bar{\gamma}} = \frac{\gamma^2}{\gamma\bar{\gamma}} = \pm\gamma^2.$$

   This contradicts the assumption that u is a fundamental unit.

   Finally if $j = 1$ then $\langle\gamma\rangle = \langle\sqrt{p}\rangle$. This shows that $\gamma = w\sqrt{p}$ for some unit w and so

   $$u = \frac{\gamma}{\bar{\gamma}} = \frac{w\sqrt{p}}{-\bar{w}\sqrt{p}} = \frac{w}{-\bar{w}} = \pm w^2$$

   which again contradicts that u is a fundamental unit.

8. Let $\alpha_1, \ldots, \alpha_r$ be the real conjugates of α and $\alpha_{r+1}, \ldots, \alpha_{r+s}$ be the complex conjugates such that $\alpha_{r+j} \neq \bar{\alpha}_{r+k}$ (each complex root appears once). So we have

   $$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{r} \alpha_i \prod_{j=1}^{s} |\alpha_{r+j}|^2.$$

   Since each $|\alpha_{r+j}|^2 > 0$ so the sign of $N_{K/\mathbb{Q}}(\alpha)$ is the same as the sign of $\prod_{i=1}^{r} \alpha_i$. Suppose $r = 0$ then the result follows. Suppose now we have a real conjugate. Let $L = \mathbb{Q}(\zeta)$ where ζ

is a non-real roots of unity in K. Let $g(x)$ be the minimal polynomial of β in L so $g(\beta) = 0$. Suppose $g(x) \notin \mathbb{R}[x]$, then $h(x) = g(x) - \overline{g(x)}$ is a polynomial of smaller degree such that $h(\beta) = 0$. This gives a contradiction and so $g(x) \in \mathbb{R}[x]$. In particular, $a = N_{K/\mathbb{Q}}(\beta) \in \mathbb{R}$.

But

$$N_{K/\mathbb{Q}}(\beta) = N_{L/\mathbb{Q}}(a) = N_{L\cap\mathbb{R}/\mathbb{Q}}(N_{L/L\cap\mathbb{R}}(a)) = N_{L\cap\mathbb{R}/\mathbb{Q}}(a^2) = (N_{L\cap\mathbb{R}/\mathbb{Q}}(a))^2 > 0$$

and since β is a conjugate of α,

$$N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta) > 0.$$