Exercises

Chapter I

1. Let N denote a finite extension field of a field L, and let σ_i $(i = 1, \ldots, n)$ denote distinct embeddings of N, over L, into an algebraic closure of L. Show that the σ_i are linearly independent over L, i.e. if $\sum l_i m^{\sigma_i} = 0$ with $l_i \in L$ given, and for all $m \in N$; then the l_i are all zero.

   If now N/L is finite and separable, deduce that $t_{N/K}$ maps onto L.

2. Let N denote a finite Galois extension of F, with $\Gamma = \mathrm{Gal}(N/F)$. Let E, L be subextensions of N which are Galois over F, let $\Delta = \mathrm{Gal}(N/E)$, $\Sigma = \mathrm{Gal}(N/L)$, and let M denote the compositum of E and L in N. Show that the map $e \otimes l \to (el, \ldots, e^{\gamma} l, \cdots)$ induces an isomorphism

$$E \otimes_F L \cong \prod_{\gamma} M$$

   where the γ run over a set of representatives of $\Gamma/\Delta\Sigma$.

3. Let N/K be a finite Galois extension of degree n with Galois group $\Gamma = \{\gamma_i \mid i = 1, \ldots, n\}$ and suppose K is infinite.

   (a) If $f \in N[X_1, \ldots, X_n]$ has the property that $f(a^{\gamma_1}, \ldots, a^{\gamma_n}) = 0$ for all $a \in N$; show that $f = 0$.

   [Hint: For a basis $\{b_i\}$ of N/K set

$$g(Y_1, \ldots, Y_n) = f(\sum Y_i b_i^{\gamma_1}, \ldots, \sum Y_i b_i^{\gamma_n});$$

   deduce that $g = 0$; and then use the invertibility of the matrix $(b_i^{\gamma_j})$ to show $f = 0$.]

(*b*) Write $X_i = X(\gamma_i)$, and set $f(X_1, \ldots, X_n) = \det(X(\gamma_i\gamma_j))$. Show $f(1, 0, \ldots, 0) \neq 0$ and use part (*a*) to show that there exists $c \in N$ such that $\det(c^{\gamma_i\gamma_j}) \neq 0$. Show that c has the property that $\{c^{\gamma_i} \mid i = 1, \ldots, n\}$ is a K-basis of N. [Hence N is a free $K\Gamma$-module on c; such a basis $\{c^\gamma\}$ is called a normal basis of N/K.]

4. Prove that a finite field k of q elements has an extension k_m of degree m for every positive integer m. Show that for given m, k_m is unique to within isomorphism over k. Show that k_m/k is a Galois extension with cyclic Galois group generated by the Frobenius automorphism $x \to x^q$.

5. Let k be a field with q elements, and let l denote an extension of k of degree m. Show that for $x \in l$
   (*a*) $t_{l/k}(x) = \sum_{i=0}^{m-1} x^{q^i}$
   (*b*) $N_{l/k}(x) = x^{q^m-1/q-1}$.
   Hence deduce that both $t_{l/k}$ and $N_{l/k}$ map onto k.

6. Show that any unique factorisation domain is integrally closed.

7. Let m be an integer, which is not a square, and with the property that $m \equiv 1 \bmod (4)$. Show that $\mathbb{Z}[\sqrt{m}]$ is not a principal ideal domain.
   [Hint: A principal ideal domain is integrally closed.]

8. If $\mathfrak{o}$ is a Noetherian ring, show that the formal power series ring $\mathfrak{o}[[x]]$ is also a Noetherian ring.

9. Show that the following algebraic numbers are all algebraic integers
   (*a*) $\sqrt[3]{15}(\sqrt[39]{7} + \sqrt[7]{39})$
   (*b*) $(1+i)/\sqrt{2}$
   (*c*) $\frac{1}{3}(1 + \sqrt[3]{10} + \sqrt[3]{100})$.

10. (Burnside) Let $\zeta^n = 1$ and assume that $\frac{1}{m}(\sum_{i=1}^m \zeta^{k_i})$ is an algebraic integer. Show that either $\sum_{i=1}^m \zeta^{k_i} = 0$ or $\zeta^{k_1} = \zeta^{k_2} = \cdots = \zeta^{k_m}$.

11. Let $\mathfrak{o}$ be an integrally closed integral domain, and let f and g be monic polynomials in $\mathfrak{o}[x]$. Prove that $\mathrm{Disc}(f).\mathrm{Disc}(g)$ divides $\mathrm{Disc}(f.g)$.

Chapter II

1. Let K be a perfect field and L denote an extension of K of degree 3. Let $d(L/K)$ denote the field discriminant of L/K, $d(L/K) =$

$\det(\mathrm{Tr}_{L/K}(x_i x_j))$ for a K-basis $\{x_i\}$ of L. By considering the action of the embeddings over K on a square root of $d(L/K)$, show that L/K is Galois iff $d(L/K)$ is a square in K^*.

2. Determine the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$ and hence calculate $d_{\mathbb{Q}(\sqrt[3]{2})}$.

3. Let m be a negative, square-free integer which has at least two distinct prime factors. Show that $\mathbb{Z}[\sqrt{m}]$ is not a principal ideal domain.

4. Let K be the subfield of $\mathbb{R}$ obtained by adjoining to $\mathbb{Q}$ the positive numbers α_n where $\alpha_n^{2^n} = 3$ $(n = 1, 2, 3, \ldots)$. Show that the ring $\mathfrak{o}$ of algebraic integers in K is integrally closed and that every prime ideal of $\mathfrak{o}$ is maximal. By considering the ideal of $\mathfrak{o}$ generated by all the α_n, or otherwise, prove that $\mathfrak{o}$ is not Noetherian.

5. Let $\mathbb{Z}[X]$ denote the ring of polynomials in an indeterminate X over $\mathbb{Z}$. Show that $\mathbb{Z}[X]$ is Noetherian, is integrally closed in its field of fractions, but is not a Dedekind domain.

6. Let R be a subring of the ring of algebraic integers $\mathfrak{o}$ of an algebraic number field K. Establish the equivalence of the following conditions:
   - (a) As a subgroup of the additive group $\mathfrak{o}$, R is of finite index, $[\mathfrak{o} : R] = f$, say.
   - (b) R contains a basis of K over $\mathbb{Q}$.
   - (c) The field of fractions of R is K.

   Now assume these conditions to hold; prove
   - (i) R is Noetherian
   - (ii) Every prime ideal of R is maximal
   - (iii) If $R \neq \mathfrak{o}$, then R is not integrally closed in K.
   - (iv) If $R \neq \mathfrak{o}$, then R has a non-zero ideal which is not invertible. Every ideal of R which is also an ideal of $\mathfrak{o}$ has this property.

   Rings satisfying conditions (a)-(c) are called *orders* in K. If K is a quadratic field show that the orders in K are in bijection with the natural numbers via $f \to R_f$, where $R_f = \mathbb{Z} + f\mathfrak{o} = \{x \in K \mid x = y + fz,\ y \in \mathbb{Z},\ z \in \mathfrak{o}\}$.

7. Show that $\mathbb{Q}_p$ has no continuous automorphisms, apart from the identity map.

8. Show that $\alpha \in \mathbb{Q}_p$ is a unit iff $X^n = \alpha$ is soluble in $\mathbb{Q}_p$ for infinitely many integers n. Deduce that any automorphism of $\mathbb{Q}_p$ must take units to units. Hence show that the identity is the only field automorphism of $\mathbb{Q}_p$.

9. Show that $\mathbb{Q}_p$ is uncountable.

10. Describe the group $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ when (*a*) $p \neq 2$ (*b*) $p = 2$.

11. If p and q are distinct primes, then show that $\mathbb{Q}_q$ and $\mathbb{Q}_p$ are not isomorphic.

12. Show that the congruence $X^8 \equiv 16 \bmod (p)$ is soluble for each prime number p.

13. Show that $k((1/T))$, the ring of finitely tailed Laurent series in $1/T$ with coefficients in k, is the completion of $k(T)$ with respect to a discrete absolute value associated with the valuation v_∞ of $k(T)$.

14. If (K, u) is a valued field with completion $(\overline{K}, \overline{u})$, show that u is an ultrametric iff $\overline{u}$ is an ultrametric.

15. If $\mathfrak{o}$ is a unique factorisation domain and if π is an irreducible element of $\mathfrak{o}$, show that the rule $v(x) = n$, where n is the highest power of π dividing x, induces a valuation on the field of fractions K.
    Now let F be a field, let $\mathfrak{o} = F[X, Y]$, for algebraically independent indeterminates X, Y and let v be the valuation associated with X, as above. Show that with the notation of §2, $\mathfrak{o}/\mathfrak{p}_v \cong F[Y]$, $\mathfrak{o}_v/\mathfrak{p}_v \cong F(Y)$.

16. Let $\mathbb{Q}_p^c$ be an algebraic closure of $\mathbb{Q}_p$ and let $\mathbb{Z}_p^c$ be the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_p^c$. Show that $\mathbb{Z}_p^c$ is integrally closed and has exactly one (non-zero) prime ideal, which is therefore maximal; show $\mathbb{Z}_p^c$ is not Noetherian, by proving that the maximal ideal is not finitely generated.
    Let $a \in \mathbb{Q}_p^{c*}$, so that a belongs to some finite extension, K say, of $\mathbb{Q}_p$. Define $|a| = p^{-v/e}$, where $v = v_{\mathfrak{p}_K}(a)$ for $v_{\mathfrak{p}_K}$ the valuation of K, and where $e = e(K/\mathbb{Q}_p)$ is the ramification index. Prove that this definition is independent of the choice of K (within the stated conditions). Show that $|.|$ is both an ultrametric and a non-discrete absolute value on $\mathbb{Q}_p^c$, and that
    $$\mathbb{Z}_p^c = \{x \in \mathbb{Q}_p^c \mid |x| \leq 1\}.$$
    For each non-negative real ρ, define
    $$I_\rho = \{x \in \mathbb{Q}_p^c \mid |x| < \rho\}.$$
    Prove that the map $\rho \to I_\rho$ is a bijection from the non-negative reals to the set of non-finitely generated ideals of $\mathbb{Z}_p^c$. For each non-negative rational r, define
    $$P_r = \{x \in \mathbb{Q}_p^c \mid |x| \leq r\}.$$
    Prove that $r \to P_r$ is a bijection from the set of non-negative ratio-

nals to the set of finitely generated ideals of $\mathbb{Z}_p^c$, and show that in fact these are all principal.

17. Show that the series

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}x^n}{n}$$

converges on $p\mathbb{Z}_p$ with respect to $|.|_p$. Show that for any positive integer n, $v_p(n!) < n/p - 1$ and hence show that

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

converges on $p\mathbb{Z}_p$ if $p > 2$ (resp. on $4\mathbb{Z}_2$ if $p = 2$). Hence show that $(1 + p\mathbb{Z}_p)^\times \cong (p\mathbb{Z}_p)^+$ if $p > 2$, and that $(1 + 4\mathbb{Z}_2)^\times \cong (4\mathbb{Z}_2)^+$ if $p = 2$.

18. Let L denote a finite extension of the p-adic field $\mathbb{Q}_p$. Let v denote the valuation associated with L, let n denote a positive integer and let $t = v(n)$. Show that for $i > t$, raising to the nth power induces an isomorphism $U^{(i)} \cong U^{(i+t)}$. Let V denote an open subgroup of the units of $\mathfrak{o}_L$. Show that $\{u^n \mid u \in V\}$ is open. Show also that $N_{L/\mathbb{Q}_p}$ is continuous on L^*, and that it is an open map.

19. Let $\mathfrak{o}$ be a ring and let M be a finitely generated $\mathfrak{o}$ module. Show that the following conditions are equivalent:
    (*a*) M is isomorphic to a direct summand of a finitely generated free $\mathfrak{o}$-module.
    (*b*) For every surjective map of $\mathfrak{o}$-modules $\pi: P \to M$, there exists an $\mathfrak{o}$-module homomorphism $i: M \to P$ such that $\pi \circ i = \mathrm{id}_M$.
    (*c*) Given homomorphisms of $\mathfrak{o}$-modules $M \xrightarrow{f} T$, $S \xrightarrow{g} T$ with g surjective; then there exists an $\mathfrak{o}$-module homomorphism $M \xrightarrow{h} S$ such that $g \circ h = f$.

20. (Harley Flanders). Let $\mathfrak{o}$ be a Dedekind domain with field of fractions K and let $F = K(X)$ be the rational function field over K in an indeterminate X. Extend the definition of the content ideal $\mathfrak{a}_f$ to rational functions f by

$$\mathfrak{a}_{g/h} = \mathfrak{a}_g \cdot \mathfrak{a}_h^{-1}$$

if $g, h \in K[X]$, $h \neq 0$, and $\mathfrak{a}_0 = (0)$. Prove that $\mathfrak{a}_{g/h}$ only depends on g/h. If $\mathfrak{b}$ is a fractional $\mathfrak{o}$ ideal define

$$\bar{\mathfrak{b}} = \{f \in F \mid \mathfrak{a}_f \subset \mathfrak{b}\}.$$

Prove that $\bar{\mathfrak{o}}$ is a principal ideal domain with field of fractions F and that the map $\mathfrak{b} \to \bar{\mathfrak{b}}$ defines an isomorphism $I_{\mathfrak{o}} \cong I_{\bar{\mathfrak{o}}}$, with inverse

$\overline{\mathfrak{b}} \to \overline{\mathfrak{b}} \cap K$. Show that $\overline{\mathfrak{p}}$ is a prime ideal of $\overline{\mathfrak{o}}$ iff $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$.

21. Show $x^4 + 1$ is reducible in $\mathbb{Q}_p$ for all primes $p > 2$.

Chapter III

1. Find the ring of integers of $\mathbb{Q}(\theta)$ when
   (*a*) $\theta^3 + \theta + 1 = 0$;
   (*b*) $\theta^3 - 2\theta + 2 = 0$;
   (*c*) $\theta^3 + \theta^2 - 2\theta + 8 = 0$.

2. (*a*) Calculate the ring of integers of $\mathbb{Q}(\zeta)$, where ζ denotes a primitive pth root of unity.

   (*b*) By considering ramification, show that $\mathbb{Q}(\sqrt{\left(\frac{-1}{p}\right)p})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta)$.

3. Let N/K denote an extension of number fields. Show that $\mathfrak{o}_K$ is a $\mathfrak{o}_K$-direct summand of $\mathfrak{o}_N$.
   Suppose now that K is a quadratic imaginary number field, and let N/K denote a non-ramified quadratic extension of K. If $\{\pm 1\}$ are the only roots of unity in N, show that $\mathfrak{o}_N$ is not free over $\mathfrak{o}_K$.

4. Show how ideals generated by $2, 3, 5, 7$ and 11, each factorise in $\mathbb{Q}(\sqrt[3]{6})$ and $\mathbb{Q}(\sqrt[3]{10})$.

5. Show that no prime number p stays prime in $\mathbb{Q}(\omega, \sqrt[3]{2})$, where $\omega^3 = 1$, $\omega \neq 1$:
   (*a*) by considering the decomposition group;
   (*b*) by factoring $x^3 - 2 \bmod (p)$.

6. Let L/K denote an extension of algebraic number fields. If $\mathfrak{o}_L$ is a free $\mathfrak{o}_K$-module, show that the discriminant $\mathfrak{d}(L/K)$ is $\mathfrak{o}_K$-principal. Conversely, if K has odd class number, show that $\mathfrak{o}_L$ is $\mathfrak{o}_K$-free if $\mathfrak{d}(L/K)$ is $\mathfrak{o}_K$-principal.

7. Let $\mathfrak{o}$ be a Dedekind domain with field of fractions K; let L/K be a finite separable extension and let $\mathfrak{o}_L$ denote the integral closure of $\mathfrak{o}$ in L. If $\mathfrak{P}$ is a tamely ramified prime ideal of $\mathfrak{o}_L$ in L/K, show $t_{L/K}(\mathfrak{P}) = \mathfrak{P} \cap \mathfrak{o}$. Give an example of a wildly ramified prime ideal which has this property.

8. If N and L are linearly disjoint finite Galois extensions of a number field K, and if there is a prime ideal $\mathfrak{P}$ of $\mathfrak{o}_{NL}$ which ramifies in both

NL/L and NL/N; show that $\mathfrak{o}_N \otimes_{\mathfrak{o}_K} \mathfrak{o}_L$ identifies with a proper subring of $\mathfrak{o}_{NL}$.

9. Let K denote a finite extension of the rational p-adic field and let L/K denote a finite field extension. Let $\mathfrak{P}$ resp. $\mathfrak{p}$ denote the unique maximal ideal of $\mathfrak{o}_L$ resp. $\mathfrak{o}_K$; let $U_L^{(i)} = 1 + \mathfrak{P}^i$, $U_K^{(i)} = 1 + \mathfrak{p}^i$ for $i > 0$ and put $U_L^{(0)} = U_L$, $U_K^{(0)} = U_K$.
   (*a*) If L/K is non-ramified, show that, for all $i \geq 0$, $t_{L/K}(\mathfrak{P}^i) = \mathfrak{p}^i$ and $N_{L/K}(U_L^{(i)}) = U_K^{(i)}$.
   (*b*) If L/K is at most tamely ramified, with ramification index e, show that $N_{L/K}(U_L^{(ei)}) = U_K^{(i)}$ for all $i \geq 1$.

Chapter IV

1. Show that $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$ are both Euclidean domains.
   (Hint: embed $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$).

2. Let K be an algebraic number field. Show that $\mathfrak{o}_K$ is a principal ideal domain iff for every $\alpha \in K$, with $\alpha \notin \mathfrak{o}_K$, there exists $\beta, \gamma \in \mathfrak{o}_K$ such that $0 < |N_{K/\mathbb{Q}}(\alpha\beta - \gamma)| < 1$.

3. Using the Minkowski bound show that: $\mathbb{Q}[\sqrt{-23}]$ has class number 3; $\mathbb{Q}[\sqrt{-47}]$ has class number 5; $\mathbb{Q}[\sqrt{-14}]$ has class number 4; $\mathbb{Q}[\sqrt{-41}]$ has class number 8.

4. Show that $\mathbb{Q}(\sqrt[3]{2})$ has class number 1.

5. Let θ denote a root of $X^3 - X - 4$ and let $K = \mathbb{Q}(\theta)$. Show that $\mathfrak{o}_K$ has $\mathbb{Z}$-basis 1, θ, $\frac{\theta+\theta^2}{2}$ and that
$$\mathfrak{o}_K = \mathbb{Z}[\frac{\theta + \theta^2}{2}];$$
hence show that K has class number 1.
[Hint: Show that $(\theta + \theta^2)/2$ is an algebraic integer and consider the square factors of the discriminant of $X^3 - X - 4$.]

6. Let θ denote a root of $X^3 - X + 2$ and let $K = \mathbb{Q}(\theta)$. Show that $\mathfrak{o}_K = \mathbb{Z}[\theta]$ and that K has class number 1. [Hint: Consider the square factors of the discriminant of $X^3 - X + 2$ and show that $\frac{1}{2}(a + b\theta + c\theta^2)$ is an algebraic integer iff a, b and c are all even.]

7. Suppose $\theta^3 - 7\theta^2 + 14\theta - 7 = 0$, and put $K = \mathbb{Q}(\theta)$. Show that $K/\mathbb{Q}$ is Galois, that $\mathfrak{o}_K = \mathbb{Z}[\theta]$ and that K has class number 1. Show that $e_7(K/\mathbb{Q}) = 3$, and that every element of $\mathfrak{o}_K$, which is coprime to 7, has norm congruent to ± 1 mod (7). Deduce that a prime number p different from 7 stays prime in K unless $p \equiv \pm 1$ mod (7).

8. (Hermite). Let K denote a number field of degree n over $\mathbb{Q}$. Given $1 \leq k \leq s+t$ show that
   (*a*) If $k \leq s$, then there exists non-zero $x \in \mathfrak{o}_K$ with
   $$|x^{\sigma_j}| \leq \frac{1}{2} \qquad 1 \leq j \leq s+t,\ j \neq k$$
   $$|x^{\sigma_k}| \leq 2^{n-t}|d_K|.$$
   (*b*) If $k > s$, then there exists non-zero $x \in \mathfrak{o}_K$ with
   $$|x^{\sigma_j}| \leq \frac{1}{2} \qquad 1 \leq j \leq s+t,\ j \neq k$$
   $$|\mathrm{Re}\, x^{\sigma_k}| \leq \frac{1}{2} \qquad |\mathrm{Im}\, x^{\sigma_k}| \leq 2^{n-t}|d_K|.$$
   Show that $K = \mathbb{Q}(x)$, and hence deduce that for any given real number N there are only finitely many algebraic number fields K of degree n, whose discriminant d_K satisfies $|d_K| \leq N$. Now use the proof of Theorem 36 to show that there are only finitely many algebraic number fields whose discriminant has absolute value less than or equal to N.

9. If S is a closed, bounded, convex, symmetric set in $\mathbb{R}^n$ with $\mathrm{vol}(S) \geq m2^n$, then show that S contains at least m pairs of points in $\mathbb{Z}^n$ (other than the origin).

10. Let B denote a closed, bounded, convex region in $\mathbb{R}^n$.
   (*a*) If B has no interior points, show that B is Jordan measurable with content zero.
   (*b*) Suppose B has an interior point $\mathbf{0}$. Show that the projection map from a large sphere S centre $\mathbf{0}$ into the boundary ∂B defines a homeomorphism between S and ∂B. Use this map to show that ∂B has content zero, so that B is Jordan measurable.

11. Let $r > 1$ and let q denote a prime number. Show that
   $$\frac{T^{q^r}-1}{T^{q^{r-1}}-1} = (T^{q^{r-1}}-1)^{q-1} + \sum_{n=1}^{q-1} \binom{q}{n} (T^{q^{r-1}}-1)^{n-1}.$$
   By putting $T = (a^{q^r}-1)/(a^{q^{r-1}}-1)$ and considering divisors of this number, show that for a given integer $a > 1$, there exists a prime p such that a has order q^r mod (p).

12. If $p = 4n-1 > 7$, show that $K = \mathbb{Q}(\sqrt{-p})$ has class number one iff m^2+m+n is prime for all m: $0 \leq m \leq n-2$.
   [Since $\mathbb{Q}(\sqrt{-163})$ has class number one, we obtain the remarkable fact, observed by Euler, that X^2+X+41 takes on prime values for $X = 1, 2, \ldots, 39$.]

Chapter V

1. Find the ring of integers, the class number and a fundamental unit of $\mathbb{Q}(\theta)$ when (a) $\theta^3+\theta+1=0$ (b) $\theta^3-2\theta+2=0$ (c) $\theta^3+\theta^2-2\theta+8=0$.

2. Let a and b be positive integers which are not squares. Show that every unit of $\mathbb{Z}[\sqrt{a},\sqrt{-b}]$ is a unit of $\mathbb{Z}[\sqrt{a}]$.

3. Show that $2-\sqrt[3]{7}$ is a fundamental unit in $\mathbb{Q}(\sqrt[3]{7})$.

4. By first observing that $\sqrt[3]{5}-2$ has norm -3 or otherwise, show that $41+24\sqrt[3]{5}+14\sqrt[3]{25}$ is a fundamental unit of $\mathbb{Q}(\sqrt[3]{5})$.

5. By first observing that $2-\sqrt[3]{14}$ has norm -6 or otherwise, show that $29+14\sqrt[3]{14}+5\sqrt[3]{196}$ is a fundamental unit of $\mathbb{Q}(\sqrt[3]{14})$.

6. In each of the following cases show that the algebraic number given is a fundamental unit of the given biquadratic field:
   (a) $\frac{(1+\sqrt{-1})(1+\sqrt{3})}{2}$ in $\mathbb{Q}(\sqrt{-1},\sqrt{3})$,
   (b) $\frac{10\sqrt{-3}-4\sqrt{-19}}{2}$ in $\mathbb{Q}(\sqrt{-3},\sqrt{-19})$,
   (c) $\frac{\sqrt{-11}+\sqrt{-7}}{2}$ in $\mathbb{Q}(\sqrt{-7},\sqrt{-11})$.

7. Determine the fundamental unit of:
   (a) $\mathbb{Q}(\sqrt{-1},\sqrt{-7})$ (b) $\mathbb{Q}(\sqrt{-1},\sqrt{-19})$ (c) $\mathbb{Q}(\sqrt{-3},\sqrt{-23})$.

8. Given any $c\in C_K^+$ and an ideal $\mathfrak{f}$ of $\mathfrak{o}_K$, show that there is an ideal $\mathfrak{a}$ of $\mathfrak{o}_K$ with class c which is coprime to $\mathfrak{f}$.

Chapter VI

1. Let l,p be odd primes, with $l\equiv 1 \bmod (3)$. By considering the factorisation of p in the cubic subfield L of $\mathbb{Q}[l]$, show that l splits completely in $\mathbb{Q}(\sqrt[3]{p})$ iff p splits completely in L.

2. Let p be a prime number and let ζ denote a primitive p^nth root of unity for $n\geq 1$; let N_n and t_n denote the norm and trace from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}(\zeta^p)$. Show that
   (a) $t_n(\mathbb{Z}[\zeta])=\begin{cases} p\mathbb{Z}[\zeta^p] & \text{if } n>1 \\ \mathbb{Z} & \text{if } n=1 \end{cases}$
   (b) for $x,y\in\mathbb{Z}[\zeta]$, and for $n>1$,
   $$N_n(x+y)\equiv N_n(x)+N_n(y) \bmod p\mathbb{Z}[\zeta^p].$$
   Deduce that $N_n(x)\equiv x^p \bmod p\mathbb{Z}[\zeta]$.

3. (Liang) Let ζ denote a root of unity and let $K=\mathbb{Q}(\zeta+\zeta^{-1})$. Show that $\mathfrak{o}_K=\mathbb{Z}[\zeta+\zeta^{-1}]$.

4. Let p be a fixed prime. By considering the behaviour of prime

divisors of numbers of the form $N^{p-1} + N^{p-2} + \ldots + N + 1$ in $\mathbb{Q}[p]$, show that there are an infinite number of primes q such that $q \equiv 1 \bmod (p)$.

5. Let $P = (x, y)$, $P' = (x', y')$ denote two finite points on an elliptic curve $Y^2 = X^3 + aX^2 + bX + c$, with $a, b, c \in K$. If $x \neq x'$, show that $P + P'$ has x and y-coordinates

$$x(P + P') = \left(\frac{y - y'}{x - x'}\right)^2 - a_2 - x - x'$$
$$y(P + P') = -\left(\frac{y - y'}{x - x'}\right) x(P + P') - \left(\frac{yx' - y'x}{x' - x}\right).$$

6. For an elliptic curve E, as in (5), show that the group of points of order less than or equal to two in $E(\mathbb{C})$, is isomorphic to $C_2 \times C_2$.

7. Let N/K denote an extension of number fields, with abelian Galois group $\Gamma = \mathrm{Gal}(N/K)$. Suppose that there exists $a \in \mathfrak{o}_N$ such that $(a^\gamma)_{\gamma \in \Gamma}$ is an $\mathfrak{o}_K$-basis of $\mathfrak{o}_N$. Use the Frobenius determinant formula (A14) to show that

$$\delta(N/K) = \prod_{\chi \in \hat{\Gamma}} \left(\sum a^\gamma \chi(\gamma^{-1})\right)^2 \mathfrak{o}_K.$$

Use this decomposition to determine the discriminant of $\mathbb{Q}[p]$.

8. For a primitive quadratic residue class character λ, define the normalised Gauss sum by

$$\tau(\lambda) = \sum \lambda(x) \exp\left(\frac{2\pi i x}{f}\right)$$

$f = f(\lambda)$ its conductor and the sum extending over a complete system of prime residues $x \bmod (f)$. Assuming Theorem 50, prove that

$$\tau(\lambda) = \begin{cases} +\sqrt{f} & \text{if } \lambda(-1) = 1 \\ i\sqrt{f} & \text{if } \lambda(-1) = -1 \end{cases}$$

where $+\sqrt{f}$ is the positive square root. (Hint: Proceed by induction on the number of distinct primes dividing f, using the expression for $\tau(\lambda_1 \lambda_2)$ in terms of $\tau(\lambda_1)$, $\tau(\lambda_2)$, where λ_1, λ_2 have coprime conductors.)

9. Let l denote an odd prime and let $\mathfrak{p}$ denote a prime ideal in $\mathbb{Q}[l]$ not dividing l. Given $a \in \mathbb{Z}[l]$, the ring of integers in $\mathbb{Q}[l]$, with $a \not\equiv 0 \bmod \mathfrak{p}$, prove that there exists an lth root of unity $\left(\frac{a}{\mathfrak{p}}\right)_l \in \mu_l$,

so that

$$a^{(N\mathfrak{p}-1)/l} \equiv \left(\frac{a}{\mathfrak{p}}\right)_l \bmod \mathfrak{p}.$$

Show that this determines $\left(\frac{a}{\mathfrak{p}}\right)_l$ uniquely. Show also that

(*a*) $\left(\frac{a}{\mathfrak{p}}\right)_l \left(\frac{b}{\mathfrak{p}}\right)_l = \left(\frac{ab}{\mathfrak{p}}\right)_l$ for $\mathfrak{p} \nmid a, b \in \mathbb{Z}[l]$.

(*b*) $\left(\frac{a}{\mathfrak{p}}\right)_l = 1 \iff$ there exists b so that $a \equiv b^l \bmod \mathfrak{p}$.

(*c*) If $a \in \mu_l$, then $\left(\frac{a}{\mathfrak{p}}\right)_l = a^{(N\mathfrak{p}-1)/l}$.

Now suppose that p is a prime number, $p \equiv 1 \bmod (l)$. Establish a bijection from the set of prime ideal divisors of p in $\mathbb{Q}[l]$ onto the set of primitive lth power residue class characters χ of $\mathbb{F}_p^*$ so that for all $a \in \mathbb{Z}$, $l \nmid a$, we have

$$\chi(a) = \left(\frac{a}{\mathfrak{p}}\right)_l$$

if $\mathfrak{p} \leftrightarrow \chi$.

10. Let m be an integer, $m > 2$, and let p be a prime number with $p^r \equiv 1 \bmod (m)$ for some odd integer r. Let $\mathfrak{p}$ be a prime ideal dividing p, in the maximal real subfield K of $\mathbb{Q}[p^n m]$ for given $n \geq 1$. Prove that $K_{\mathfrak{p}} \cong \mathbb{Q}_p[p^n m]$.

11. Let p_1, p_2 be distinct odd prime numbers, and let $d \mid (p_1 - 1, p_2 - 1)$. Show that $\mathbb{Q}[p_1 p_2]$ has a subfield L so that
    (*a*) $(\mathbb{Q}[p_1 p_2] : L) = d$.
    (*b*) $\mathbb{Q}[p_1 p_2]/L$ is non-ramified, i.e. for all prime ideals $\mathfrak{p}$ of $\mathfrak{o}_L$, $e_{\mathfrak{p}}(\mathbb{Q}[p_1 p_2]/L) = 1$.

12. Suppose $m \geq 2$ and put $E = Q[4]$. Let $K = \mathbb{Q}[2^m]$, let $L = \mathbb{Q}[2^m]_+$ denote the maximal real subfield of K and let $\rho \in \mathrm{Gal}(K/\mathbb{Q})$ denote complex conjugation. Show that if $u \in U_K$ does not lie in $\mu_K U_L$, then $u^{1-\rho} = \zeta$ say, is a primitive 2^mth root of unity. Prove that $U_K = \mu_K U_L$ by showing that $N_{K/E}\zeta$ is a primitive fourth root of unity, while $N_{K/E}(u)^{1-\rho}$ must be ± 1.

Chapter VII

1. Let k be a finite field, and let $d \in k$, $c \in k$. Show that there exist x, y in k such that $x^2 + dy^2 = c$.

2. What integers can be expressed in the form (*a*) $X^2 - 5Y^2$, (*b*) $X^2 - 6Y^2$, for integral X, Y?

3. Find all integral solutions to $3X^2 - 4Y^2 = 11$.

4. Solve the following equations for integral X, Y
   (*a*) $X^3 = Y^2 + 2$
   (*b*) $X^5 = Y^2 + 19$
   (*c*) $X^3 = Y^2 + 54$
   (*d*) $X^3 = Y^2 + 200$.

5. Solve $4X^3 = Y^2 + p$ for integral X, Y when $p \equiv 3 \bmod (4)$, $p \neq 3$, and when 3 does not divide the class number of $\mathbf{Q}(\sqrt{-p})$.

6. What integers can be expressed in the form (*a*) x^2+5y^2; (*b*) x^2+15y^2; (*c*) $x^2 - 23y^2$; (*d*) $x^2 + 23y^2$ for integral x, y?

7. Let m be an even, square-free positive integer, and suppose that $\mathbf{Q}(\sqrt{-m})$ has class number which is not divisible by 3. Show that $X^3 = Y^2 + m$ has at most one solution in natural numbers.

8. Show that $\mathbf{Z}[\sqrt[3]{6}]$ has class number 1; hence show that $X^3 + 6Y^3 = 10Z^3$ has no non-trivial integer solutions.

Chapter VIII

1. Using the results of Ex.6 of Ch.V show that
$$\mathbf{Q}(\sqrt{-1}, \sqrt{3})$$
$$\mathbf{Q}(\sqrt{-3}, \sqrt{-19})$$
$$\mathbf{Q}(\sqrt{-7}, \sqrt{-11})$$
all have class number 1.

2. Show that $\mathbf{Q}(\sqrt{5}, \sqrt{13})$ has class number 2, and that $\mathbf{Q}(\sqrt{-3}, \sqrt{-23})$ has class number 3.

3. Let χ be the primitive residue class character with conductor $f(\chi) = 4$. Prove that $L(x, \chi) > 0$ for all $x > 0$.

4. Let K be a cyclotomic field of odd prime degree l over $\mathbf{Q}$. Let $f = \prod p_i$ denote the product of primes p_i which ramify in K, with all $p_i \equiv 1 \bmod (l)$. For the units $\omega_{f,a}$ defined in (5.6), write $\omega_{K,a} = N_{\mathbf{Q}[f]_+/K}(\omega_{f,a})$, and let Ω_K denote the subgroup of K^* generated by the $\omega_{K,a}$. Prove that Ω_K is a subgroup of finite index in the group U_K of units of K and that
$$[U_K : \Omega_K] = h_K.$$

5. For a non-zero real number x define $s(x)$ by $x/|x| = (-1)^{s(x)}$, viewing $s(x)$ as an element of the field $\mathbf{F}_2$ of two elements. Call a sub-

group V of the group of units U_K of a totally real algebraic number field K *full* if $[V : V^2] = 2^{(K:\mathbb{Q})}$. Suppose V is full. For a set of elements $\{v_j\}$ of V whose classes mod V^2 form a basis of V/V^2 over $\mathbb{F}_2$, consider the matrix $A_V = (s(v_j^{\sigma_k}))$, where σ_k ranges over the embeddings $K \to \mathbb{R}$. Prove that the rank $r(A_V)$ of A_V depends only on V, and show that, with h_K^+ as defined in (V,§1),

$$(a) \qquad 2^{r(A_V)} h_K^+ \mid h_K 2^{(K:\mathbb{Q})}$$

with equality for $V = U_K$.

Now let K be a cyclotomic field of odd prime degree l, and let V be the group generated by Ω_K and -1. Prove that if $r(A_V) = (K : \mathbb{Q})$, then h_K^+ is odd. (Hasse) State and prove analogues for $K = \mathbb{Q}[p]_+$, p an odd prime.

6. A prime ideal $\mathfrak{p}$ of $\mathfrak{o}_K$ is said to have degree 1 if $\mathbf{N}\mathfrak{p}$ is a prime number. By considering the behaviour of $\zeta_K(x)$ as $x \to 1+$, show that $\mathfrak{o}_K$ always has an infinite number of degree 1 prime ideals.

7. Suppose that $N/\mathbb{Q}$ is Galois with Galois group A_4, the alternating group on 4 elements. Express $\zeta_N(x)$ in terms of Dedekind zeta functions of proper subfields of N.

8. (Brauer) With the notation of Theorem 73, let $W_{N_a}^{(p)}$ denote the exact power of p dividing W_{N_a} (the number of roots of unity in N_a). Show that if $p > 2$ then

$$\prod_a W_{N_a}^{(p)} = \prod_b W_{N_b}^{(p)}$$

but that the above equality fails to hold in general when $p = 2$.

[Hint: Let $W_N^{(p)} = p^m$. Note that for $p > 2$, $\mathrm{Gal}\,(\mathbb{Q}[p^n]/\mathbb{Q}) = \Gamma_n$ is always cyclic. For $n \leq m$, let χ_n denote a faithful abelian character of Γ_n, which can then also be viewed as a character of Γ, via the surjection $\Gamma \to \Gamma_n$. Show that $W_{N_a}^{(p)} = p^t$ where

$$t = (\rho_a, \sum_{n=1}^{m} \chi_n)$$

where ρ_a denotes the character of $\mathbb{C}(\Lambda_a \backslash \Gamma)$ and where $(,)$ denotes the standard inner product of character theory.]

Appendix A

(The notation here is that of Appendix A.)

1. Let Γ denote a finite abelian group, let $M = (\chi(\gamma))_{\gamma,\chi}$ for $\gamma \in \Gamma$,

$\chi \in \hat{\Gamma}$, and let $M^* = (\chi^{-1}(\gamma))_{\chi,\gamma}$. Show that

$$MM^* = \operatorname{diag}\begin{pmatrix} |\Gamma| & & \\ & \ddots & \\ & & |\Gamma| \end{pmatrix};$$

hence deduce that $\det(M)^2 = (-1)^N |\Gamma|^{|\Gamma|}$ where $2N$ denotes the number of elements in Γ with order greater than 2.

2. Let V be a finitely generated $K\Gamma$-module. Show that V is the direct sum of the K spaces Ve_χ ($\chi \in \hat{\Gamma}$); furthermore, given another such module V', then V and V' are isomorphic $K\Gamma$-modules iff $\dim_K(Ve_\chi) = \dim_K(V'e_\chi)$ for all $\chi \in \hat{\Gamma}$.

3. Let E/F be a Galois extension of algebraic number fields with abelian Galois group Γ, viewed as contained in the algebraically closed field K. Suppose that F contains all the values $\chi(\gamma)$ ($\chi \in \hat{\Gamma}$, $\gamma \in \Gamma$). Using Ex 3 of Chapter I, prove that E has an F-basis $\{a_\chi\}$ ($\chi \in \hat{\Gamma}$) such that

$$a_\chi^\gamma = a_\chi \chi(\gamma) \qquad \text{for all } \gamma \in \Gamma.$$

Show also that $E = F(b_1, \ldots, b_r)$ where for all i, $b_i^{n_i} \in F^*$ for some $n_i > 0$.

4. (Alternative approach: assume only the definition of $K\Gamma$ and $\hat{\Gamma}$.)
   (*a*) Show that
   $$t_{K\Gamma/K}(\gamma) = \begin{cases} |\Gamma| & \text{if } \gamma = 1_\Gamma \\ 0 & \text{otherwise.} \end{cases}$$
   (*b*) By evaluating $\det(t_{K\Gamma/K}(\gamma\delta))$, show that $K\Gamma$ is a commutative separable K-algebra, i.e. $K\Gamma = \sum A_i$ (direct sum), where each A_i is a simple ideal; thus, as a K-algebra, each $A_i \cong K$, since K is algebraically closed.
   (*c*) For each i, $A_i = K\Gamma e_i$ with e_i a primitive idempotent; and show also that $e_i\gamma = e_i\chi(\gamma)$ for some $\chi \in \hat{\Gamma}$. Using this equation and writing $e_i = \sum a_\gamma \gamma$, show that $e_i = e_\chi$, where e_χ is as defined in (A4).
   (*d*) Deduce that $|\hat{\Gamma}| = |\Gamma|$.
   (*e*) If $\chi \in \hat{\Gamma}$, $\chi \neq \epsilon_\Gamma$; then, by evaluating $\chi(\sigma)\sum_\gamma \chi(\gamma)$, prove that $\sum \chi(\gamma) = 0$.
   (*f*) Deduce (A10).
   (*g*) Use (A10) to prove that the matrix $(\chi(\gamma))_{\chi,\gamma}$ ($\chi \in \hat{\Gamma}$, $\gamma \in \Gamma$) is invertible.
   (*h*) Deduce (A7) and (A7.*a*).