Math 254B: Number theory

H. W. Lenstra, Jr. (879 Evans, office hours MF 4:15–5:15, tel. 643-7857, e-mail hwl@math).

Spring 1993, MWF 1–2, 85 Evans.

Exercise 1. Let L be a field and let $\operatorname{Aut} L$ be its automorphism group. We view $\operatorname{Aut} L$ as a subset of the set L^L of *all* maps $L \to L$. We give L the discrete topology, L^L the product topology, and $\operatorname{Aut} L$ the induced (or relative) topology. In other words, a base for the topology of $\operatorname{Aut} L$ is formed by the sets $U_{\sigma,E} = \{\tau \in \operatorname{Aut} L : \tau|E = \sigma|E\}$, where σ ranges over $\operatorname{Aut} L$ and E over the finite subsets of L.

Prove that this topology makes $\operatorname{Aut} L$ into a topological group, i. e., both the map $\operatorname{Aut} L \times \operatorname{Aut} L \to \operatorname{Aut} L$ sending (σ, τ) to $\sigma\tau$ and the map $\operatorname{Aut} L \to \operatorname{Aut} L$ sending σ to σ^{-1} are continuous.

Exercise 2. Let L be a field, K a subfield of L, and G a subgroup of $\operatorname{Aut} L$. Prove that $K \subset L$ is a Galois extension with group G if and only if G is *compact* in the topology induced from $\operatorname{Aut} L$ (see Exercise 1) and $K = \{x \in L : \sigma x = x \text{ for all } \sigma \in G\}$.

In Exercises 3–6 we denote by $\hat{\mathbf{Z}}$ the projective limit of the rings $\mathbf{Z}/n\mathbf{Z}$ (with n ranging over the positive integers) with respect to the natural maps $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ (for m dividing n). Explicitly, we have

$$\hat{\mathbf{Z}} = \{(a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} (\mathbf{Z}/n\mathbf{Z}) : a_m = (a_n \bmod m) \text{ for all } n,\ m \text{ with } m \text{ dividing } n\}.$$

This is a compact topological ring. Its additive group is a profinite abelian group, which is likewise denoted by $\hat{\mathbf{Z}}$.

Exercise 3. Let k be a finite field. Prove that the absolute Galois group of k is isomorphic to $\hat{\mathbf{Z}}$.

Exercise 4. Let μ be the group of all roots of unity in some algebraic closure of the field $\mathbf{Q}$ of rational numbers.

(a) Prove that $\hat{\mathbf{Z}}$ is isomorphic to the endomorphism ring of the abelian group μ.

(b) Prove that the group $\hat{\mathbf{Z}}^*$ of units of $\hat{\mathbf{Z}}$, with the topology induced from $\hat{\mathbf{Z}}$, is a profinite group, and that it is isomorphic to the automorphism group of μ.

(c) Prove that $\mathbf{Q} \subset \mathbf{Q}(\mu)$ is a Galois extension, and that $\operatorname{Gal}(\mathbf{Q}(\mu)/\mathbf{Q}) \cong \hat{\mathbf{Z}}^*$.

Exercise 5. Let a be a non-negative integer, and define $(a_n)_{n=0}^{\infty}$ inductively by $a_0 = a$, $a_{n+1} = 2^{a_n}$. Prove that the sequence $(a_n)_{n=0}^{\infty}$ has a limit in $\hat{\mathbf{Z}}$, and that this limit is independent of a.

Exercise 6. (a) Let n be a positive integer. Prove that multiplication by n induces an exact sequence $0 \to \hat{\mathbf{Z}} \to \hat{\mathbf{Z}} \to \mathbf{Z}/n\mathbf{Z} \to 0$.

(b) Let $u \in \hat{\mathbf{Z}}^*$. Prove that for each positive integer n there exists a unique element $a_n \in \hat{\mathbf{Z}}$ such that $u^{n!} = 1 + n!a_n$, and that $a_{n+1} \equiv a_n \bmod n!/\gcd(n!, n+1)$ for all n.

(c) Prove that there is a continuous group homomorphism $\log\colon \hat{\mathbf{Z}}^* \to \hat{\mathbf{Z}}$ defined by

$$\log u = \lim_{n\to\infty} \frac{u^{n!} - 1}{n!}.$$

Exercise 7. Let k be a field, and let $k(X)$ be the field of fractions of the polynomial ring $k[X]$ in one variable over k.

(a) Determine all valuations ψ on $k(X)$ for which the restriction of ψ to k is trivial.

(b) Let φ be a non-archimedean valuation on k, and let r be a positive real number. Prove that there is a valuation ψ on $k(X)$ for which $\psi|k = \varphi$ and $\psi(X) = r$.

Exercise 8. In this exercise you may assume the following fact, which will be proved in class: if φ is a valuation on a field K, and L is a finite extension of K, then φ can be extended to a valuation on L.

Let K be a field. Prove: there exists a non-trivial non-archimedean valuation on K if and only if there does not exist a prime number p with the property that K is an algebraic extension of $\mathbf{F}_p$.

Exercise 9. (a) Let K be a field, φ a non-archimedean valuation on K, and n a positive integer. Denote by S_h the set of those non-zero vectors $(x_1, x_2, \ldots, x_n) \in K^n$ with the property that h is the smallest of the subscripts i for which $\varphi(x_i) = \max\{\varphi(x_j) : 1 \le j \le n\}$. Prove that any sequence v_1, v_2, …, v_n of vectors in K^n satisfying $v_i \in S_i$ for each i forms a basis for K^n over K.

(b) Prove that the two-dimensional Euclidean plane can be written as the union of three dense subsets with the property that no line in the plane intersects all three subsets.

Exercise 10. Denote by $\mathbf{C}$ the field of complex numbers, and let φ be the valuation on $\mathbf{C}$ given by $\varphi(x) = |x|$ for all $x \in \mathbf{C}$. Let K be a field, and let σ, $\tau\colon K \to \mathbf{C}$ be field

homomorphisms. Prove that $\varphi \cdot \sigma = \varphi \cdot \tau$ if and only if $\sigma = \tau$ or $\sigma = \bar{\tau}$; here the overhead bar denotes complex conjugation.

Exercise 11. (a) Prove that for any sequence of elements $(c_n)_{n=1}^{\infty}$ of elements of $\hat{\mathbf{Z}}$ the sum $\sum_{n=1}^{\infty} c_n n!$ converges, and that for any $x \in \hat{\mathbf{Z}}$ there exists a unique sequence $(c_n)_{n=1}^{\infty}$ of integers for which

$$x = \sum_{n=1}^{\infty} c_n n!, \qquad 0 \leq c_n \leq n \quad \text{for all } n.$$

In this case, we shall write $x = (\ldots c_3 c_2 c_1)_!$. This representation of elements of $\hat{\mathbf{Z}}$ is called the *factorial number system*.

(b) Write -1 in the factorial number system.

(c) Prove that the topology on $\hat{\mathbf{Z}}$ is induced by the metric

$$d((\ldots b_3 b_2 b_1)_!, (\ldots c_3 c_2 c_1)_!) = 1/\min\{n : b_n \neq c_n\}$$

($= 0$ if $b_n = c_n$ for all n).

Exercise 12. For a prime number p, let $\mathbf{Z}_p$ be the projective limit of the rings $\mathbf{Z}/p^n\mathbf{Z}$ (with n ranging over the positive integers) with respect to the natural maps $\mathbf{Z}/p^n\mathbf{Z} \to \mathbf{Z}/p^m\mathbf{Z}$ (for $m \leq n$). This is a compact topological ring, the *ring of p-adic integers*.

Prove that there is a topological ring isomorphism

$$\hat{\mathbf{Z}} \cong \prod_p \mathbf{Z}_p,$$

with p ranging over the set of prime numbers and the product being given the product topology.

Exercise 13. Prove that the field $\mathbf{Q}(\mathrm{i})$, with $\mathrm{i}^2 = -1$, has a valuation φ with the following property: if x, $y \in \mathbf{Q}(\mathrm{i})$ are non-zero elements with $\varphi(x + y) = \max\{\varphi(x), \varphi(y)\}$, then $\varphi(x) \neq \varphi(y)$.

Exercise 14. Let K be a field.

(a) Let φ be a non-archimedean valuation on K, with valuation ring A and residue class field k. Let $\zeta \in K$ be a root of unity. Prove that $\zeta \in A$, and that ζ belongs to the kernel of the natural map $A^* \to k^*$ if and only if the order of ζ is a power of the characteristic of k.

(b) Suppose that φ, ψ are non-archimedean valuations on K with finite residue class fields k, l, and that $\gcd(\#k, \#l) = 1$. Prove that the number of roots of unity in K is finite, and that it divides $\gcd\big((\#k)^{\#l}(\#k-1), (\#l)^{\#k}(\#l-1)\big)$.

Exercise 15. Let K be a field that is complete with respect to a non-archimedean valuation φ, and let n be an integer that is not divisible by the characteristic of the residue class field of φ. Prove that the map sending x to x^n is an automorphism of the multiplicative subgroup $\{x \in K : \varphi(x-1) < 1\}$ of K^*.

Exercise 16. Let K be a field and let φ be a non-archimedean valuation on K. Suppose that the characteristic p of the residue class field of φ is non-zero.

(a) Let $x \in K$, $\varphi(x-1) < 1$. Prove that $\varphi(x^p - 1) \leq \max\{\varphi(p \cdot (x-1)), \varphi(x-1)^p\}$.

(b) Suppose that K is complete with respect to φ, and let $\epsilon \in \mathbf{R}$, $0 < \epsilon < \varphi(p)^{1/(p-1)}$. Prove that the map sending x to x^p is an isomorphism from the group $\{x \in K : \varphi(x-1) \leq \epsilon\}$ to the group $\{x \in K : \varphi(x-1) \leq \varphi(p) \cdot \epsilon\}$.

In the following two exercises we let p be a prime number, and we denote by $\mathbf{Q}_p$ the field of p-adic numbers. The *p-adic expansion* of a p-adic number r is the unique expansion $r = \sum_{i \in \mathbf{Z}} c_i p^i$ in $\mathbf{Q}_p$ for which $c_i \in \{0, 1, \ldots, p-1\}$ for all i and $c_i = 0$ for $i \ll 0$.

Exercise 17. How can you tell from the p-adic expansion of a p-adic number r whether r belongs to $\mathbf{Z}$? and to $\frac{1}{2} + \mathbf{Z}$?

Exercise 18. Let r be a positive rational number. Prove the correctness of the following method for obtaining the p-adic expansion of r. How does it have to be modified for negative $r \in \mathbf{Q}$?

Write r in $\mathbf{R}$ in base p, say $r = \sum_{i \in \mathbf{Z}} a_i p^i$, with $a_i \in \{0, 1, \ldots, p-1\}$, $a_i = 0$ for $i \gg 0$. It is well known that the sequence $(a_i)_{i=-1}^{-\infty}$ is ultimately periodic, say with a period consisting of m digits. Let $b_i \in \{0, 1, \ldots, p-1\}$, for $i \in \mathbf{Z}$, be given by $b_i = a_{i-km}$ for $k \in \mathbf{Z}$ sufficiently large, so that $(b_i)_{i \in \mathbf{Z}}$ is purely periodic. The p-adic expansion $\sum_{i \in \mathbf{Z}} c_i p^i$ of r is now obtained by subtracting the expression $\sum_{i \in \mathbf{Z}} b_i p^i$ from $\sum_{i \in \mathbf{Z}} a_i p^i$ by means of the usual subtraction method in base p.

Example. Take $p = 5$ and $r = 42\frac{8}{15}$. The representation of r in base 5 in $\mathbf{R}$ is given by

$$132.2313131313\ldots .$$

The purely periodic expression $\sum_{i \in \mathbf{Z}} b_i p^i$ can be written as

$$\ldots 1313131313.1313131313\ldots .$$

Subtracting this expression from the previous one in base 5, going from right to left, we find

$$\ldots 3131313314.1.$$

This is the 5-adic expansion of $42\frac{8}{15}$; so $c_i = 0$ for $i < -1$, $c_{-1} = 1$, $c_0 = 4$, $c_1 = 1$, $c_2 = 3$, $c_i = 3$ for odd $i \geq 3$, and $c_i = 1$ for even $i \geq 4$.

Exercise 19. (a) Let K be a field with a non-archimedean valuation φ. Denote the valuation ring and its maximal ideal by A and P. Write S for the set of those $x \in K$ for which $1 + x$ has an nth root in K for infinitely many positive integers n. Prove: if K is complete with respect to φ then $P \subset S$, and if φ is discrete than $S \subset A$.

(b) Let K be a field that is complete with respect to a non-trivial valuation φ. Prove that any discrete valuation on K is equivalent to φ.

(c) For $i = 0, 1$, let K_i be a field that is complete with respect to a discrete valuation. Prove that any field homomorphism $K_0 \to K_1$ of which the image is not contained in the valuation ring of K_1 is continuous.

Exercise 20. Let $\mathbf{Q}_p$ be the completion of $\mathbf{Q}$ with respect to any (finite or infinite) prime divisor p of $\mathbf{Q}$. Prove that $\mathbf{Q}_p$ has no field automorphism except the identity. Prove also that $\mathbf{Q}_p$ and $\mathbf{Q}_{p'}$ are not isomorphic as fields for $p \neq p'$.

Exercise 21. Let L be a field that is complete with respect to a discrete valuation ψ, and let K be a subfield of L for which $K \subset L$ is finite and separable. Prove that K is complete with respect to the restriction of ψ to K.

Exercise 22. Let A be a local ring with residue class field k, and let g, $h \in A[X]$. Suppose that g is monic, and that the images of g and h in $k[X]$ are coprime. Prove that $gA[X] + hA[X] = A[X]$.

Exercise 23. Let K be a field that is complete with respect to a non-archimedean valuation. Denote the valuation ring and its maximal ideal by A and P, and suppose that the residue class field A/P is a finite field of q elements. Prove that for every $a \in A$ there is a unique element $\omega(a) \in a + P$ satisfying $\omega(a)^q = \omega(a)$, and that one has $\omega(a) = \lim_{n \to \infty} a^{q^n}$.

Exercise 24. Let k be a field, and let $f \in k[X]$ be an irreducible separable polynomial. Let φ be a valuation on $k(X)$ such that the restriction of φ to k is trivial and $\varphi(f) < 1$. (This determines φ up to equivalence; cf. Exercise 7(a).) Write $l = k[X]/fk[X]$. Prove that f has a zero in the completion $k(X)_\varphi$, and that there is a topological isomorphism of fields

$k(X)_\varphi \cong l((Y))$ that is the identity on k; here $l((Y))$ denotes the field of formal Laurent series with coefficients in l.

In the following three exercises K denotes a field with a non-archimedean valuation φ, and r is a positive real number.

Exercise 25. For $f = \sum_i a_i X^i \in K[X]$, $f \neq 0$, denote the largest and the smallest value of i for which $\varphi(a_i)r^i = \max_j \varphi(a_j)r^j$ by $l_r(f)$ and $s_r(f)$, respectively.

(a) Prove that l_r and s_r extend to group homomorphisms $K(X)^* \to \mathbf{Z}$.

(b) Suppose that K is algebraically closed, and let $f \in K[X]$, $f \neq 0$. Prove that the number of zeroes α of f in K with $\varphi(\alpha) = r$, counted with multiplicities, is equal to $l_r(f) - s_r(f)$.

Exercise 26. Let $f = \sum_i a_i X^i \in K[X]$, $f \neq 0$. The *Newton polygon* of f is defined to be the "lower convex hull" of the points $(i, -\log \varphi(a_i))$, with i ranging over all non-negative integers for which $a_i \neq 0$; more precisely, if $C \subset \mathbf{R} \times \mathbf{R}$ is the convex hull of the set of those points, then the Newton polygon equals $\{(x, y) \in C : \text{there is no } (x, y') \in C \text{ with } y' < y\}$. The Newton polygon is the union of finitely many line segments of different slopes.

(a) Draw, for each prime number p, the Newton polygon of $3X^3 - \frac{6}{7}X^2 + \frac{3}{2}X + 5 \in \mathbf{Q}[X]$ with respect to the p-adic valuation of $\mathbf{Q}$.

(b) Prove: if $\log r$ occurs as the slope of one of the line segments that constitute the Newton polygon of f, then $l_r(f) - s_r(f)$ (as defined in the previous exercise) is equal to the length of the projection of that line segment on the x-axis, and otherwise $l_r(f) - s_r(f) = 0$.

Remark. Combining (b) with Exercise 25(b) one sees that the valuations of the zeroes of f (in some algebraic extension of K) can be read from the Newton polygon of f.

Exercise 27. Let $f \in K[X]$, and suppose that $f(0) \neq 0$.

(a) Suppose that K is complete with respect to φ, and that f is irreducible. Prove that the Newton polygon of f is a single line segment.

(b) Suppose that the Newton polygon of f intersects the set $\mathbf{Z} \times (-\log \varphi(K^*))$ in exactly two points. Prove that f is irreducible.

(c) Prove that $3X^3 - \frac{6}{7}X^2 + \frac{3}{2}X + 5$ is the product of two irreducible factors in each of $\mathbf{Q}_2[X]$ and $\mathbf{Q}_7[X]$, that it is irreducible in $\mathbf{Q}_3[X]$, and that it is the product of three linear factors in $\mathbf{Q}_5[X]$. How does it factor in $\mathbf{Q}[X]$?

In the following two exercises we denote by ζ_m a primitive mth root of unity in some extension of the base field.

Exercise 28. Let K be a field that is complete with respect to a discrete valuation, with a perfect residue class field k.

(a) Let m be a positive integer that is not divisible by $\operatorname{char} k$. Prove that $K(\zeta_m)$ is unramified over K.

(b) Suppose that k is a finite field of q elements. Prove that every finite unramified extension L of K is of the form $K(\zeta_m)$, with m as in (a), and that for any such m the order of $(q \bmod m)$ in $(\mathbf{Z}/m\mathbf{Z})^*$ equals $[L : K]$.

Exercise 29. Let p be a prime number.

(a) Prove that for each positive integer s the extension $\mathbf{Q}_p \subset \mathbf{Q}_p(\zeta_{p^s})$ is totally ramified of degree $(p-1)p^{s-1}$.

(b) Prove that $\mathbf{Q}_p(\zeta_p) = \mathbf{Q}_p((-p)^{1/(p-1)})$.

Exercise 30. Let K be a field that is complete with respect to a discrete valuation, and suppose that the residue class field is perfect. Let $K \subset L \subset M$ be finite field extensions.

(a) Denote by E the maximal subextension of $K \subset M$ that is unramified over K. Prove that $E \cap L$ is the maximal subextension of $K \subset L$ that is unramified over K, and that $E \cdot L$ is the maximal subextension of $L \subset M$ that is unramified over L.

(b) This is the same as (a), with "unramified" everywhere replaced by "tamely ramified".

Exercise 31. Let K be a field that is complete with respect to a discrete valuation with a finite residue class field. Prove that K is either isomorphic to a finite extension of $\mathbf{Q}_p$, for some prime number p, or to the field $k((t))$ of formal Laurent series over k, for some finite field k.

Exercise 32. Let K be a field that is complete with respect to a discrete valuation with a perfect residue class field. Let $K \subset L$ be a finite Galois extension, with Galois group, inertia group, and ramification group G, I, and V, respectively. Let $H \subset G$ be a subgroup, and $E = L^H$ the corresponding subfield.

(a) Prove that $I \cap H$ and $V \cap H$ are the inertia group and the ramification group of $E \subset L$, respectively.

(b) Suppose that E is Galois over K, with Galois group Γ ($\cong G/H$). Prove that the images of I and V under the natural map $G \to \Gamma$ are the inertia group and the ramification group of $K \subset E$, respectively.

Exercise 33. Do the following for $p = 2$, 3, 5, 7, and 31. Determine the degree of a splitting field M of $X^3 - 2$ over $\mathbf{Q}_p$, as well as the Galois group, the inertia group, and the

ramification group of $\mathbf{Q}_p \subset M$. In addition, compute $e(L/K)$ and $f(L/K)$ for all fields K, L with $\mathbf{Q}_p \subset K \subset L \subset M$.

Exercise 34. Let K be as in Exercise 31, and suppose that the characteristic of the residue class field of K is different from 2. Let the field L be obtained by adjoining the square roots of all elements of K to K. Prove that L is a tamely ramified finite Galois extension of K, the Galois group being the non-cyclic group of order 4. Can you describe the maximal unramified subextension of $K \subset L$?

Exercise 35. Let K be as in Exercise 32, and let L_1, L_2 be two totally ramified finite extensions of K inside a common overfield. Does it follow that $L_1 \cdot L_2$ is totally ramified over K? Give a proof or a counterexample.

Exercise 36. Let $L = \mathbf{Q}_5(\sqrt[4]{50})$, and let E be the maximal unramified subextension of $\mathbf{Q}_5 \subset L$. Exhibit a prime element π_E of the valuation ring of E such that $L = E(\sqrt{\pi_E})$. Can π_E be chosen in $\mathbf{Q}_5$? Prove the correctness of your answer.

Exercise 37. Let G be a profinite group.

(a) Prove that for every $g \in G$ there exists a unique continuous group homomorphism $f\colon \hat{\mathbf{Z}} \to G$ with $f(1) = g$.

(b) Suppose that $N \subset G$ is a closed normal subgroup such that $G/N \cong \hat{\mathbf{Z}}$ (as profinite groups). Prove that G is, as a profinite group, isomorphic to a semidirect product of $\hat{\mathbf{Z}}$ by N.

(c) This is the same as (b), with $\hat{\mathbf{Z}}$ replaced by $\mathbf{Z}_p$ for some prime number p.

In the following three exercises K denotes a field that is complete with respect to a discrete valuation with a finite residue class field, and L is a finite extension of K. The ramification index of L over K is denoted by e.

Exercise 38. Let M be the largest subextension of $K \subset L$ for which $K \subset M$ is abelian.

(a) Use local class field theory to show that $N_{L/K}L^* = N_{M/K}M^*$.

(b) Let q denote the cardinality of the residue class field of K. Suppose that $K \subset L$ is totally ramified, and that $\gcd(e, q(q-1)) = 1$. Prove that $M = K$ and that $N\colon L^* \to K^*$ is surjective. Can you prove both statements without local class field theory?

Exercise 39. (a) Suppose that $\operatorname{char} K = 0$. Prove that every subgroup of K^* of finite index is open. (*Hint*: Exercises 15 and 16.)

(b) Suppose that $\operatorname{char} K \neq 0$. Prove that K^* has a subgroup of finite index that is not open.

(c) Let H be a subgroup of $\mathbf{R}^*$ or $\mathbf{C}^*$. Prove that H is of finite index if and only if H is open.

Exercise 40. (a) Suppose that L is unramified over K. Prove that $K^*/N_{L/K}L^* \cong \mathbf{Z}/[L : K]\mathbf{Z}$. (Do not use local class field theory.)

(b) Suppose that L is abelian over K, and denote the rings of integers of K and L by A and B, respectively. Use local class field theory to show that $A^*/N_{L/K}B^*$ is of order e.

Exercise 41. Do the following for $p = 2$, 3, 5, 7, and 31. Let M be a splitting field of $X^3 - 2$ over $\mathbf{Q}_p$ (cf. Exercise 33). Describe $N_{M/\mathbf{Q}_p}M^*$ as a subgroup of $\mathbf{Q}_p^*$. (You may use local class field theory.)

Exercise 42. Let K be a field that is complete with respect to a discrete valuation with a perfect residue class field, and let L be a finite separable extension of K. Denote the ramification index of L over K by e, the maximal ideal of the valuation ring of L by Q, and the different of L over K by $\mathcal{D}_{L/K}$.

(a) Prove: $eQ^{e-1} \subset \mathcal{D}_{L/K}$.

(b) Suppose that $\operatorname{char} K = p \neq 0$, and let $m(L/K) \in \mathbf{Z}$ be such that $\mathcal{D}_{L/K} = Q^{m(L/K)}$. Prove that $m(L/K) \not\equiv -1 \bmod p$.

Exercise 43. Let p be a prime number, and let $\mathbf{F}_p((t))$ be the field of formal Laurent series over the field $\mathbf{F}_p$ of p elements.

(a) Prove that there exists an element $u \in \mathbf{F}_p((t))$ that is transcendental over the subfield $\mathbf{F}_p(t)$ generated by t.

(b) Let u be as in (a), and put $K = \mathbf{F}_p(t, u^p)$, $L = \mathbf{F}_p(t, u)$. Prove that $[L : K] = p$, and that K has a discrete valuation φ with the property that $\sum_\psi e(\psi/\varphi)f(\psi/\varphi) < [L : K]$, the sum ranging over the valuations ψ of L that extend φ.

In Exercises 44–48 we let K be an algebraic number field, i. e., a finite extension of $\mathbf{Q}$. We let $K \subset L$ be a finite Galois extension and G its Galois group. By Q we denote a prime of L, by P its restriction to K, by G_Q the decomposition group of Q over P, and by $I_Q \subset G_Q$ the inertia group of Q over P. Let $H \subset G$ be a subgroup, $E = L^H$ the corresponding subfield of L, and R the restriction of Q to E. We write X for the transitive G-set G/H belonging to E; it may alternatively be thought of as the set of K-homomorphisms $E \to L$, or, if $E \cong_K K[t]/fK[t]$, as the set of zeroes of f in L.

Exercise 44. (a) Prove that $G_Q \cap H$ is the decomposition group of Q over R.

(b) Suppose that H is normal in G. Prove that the decomposition group of R over P is the image of G_Q in the group G/H.

Exercise 45. Suppose that Q is unramified over P, and denote by $[L/K, Q]$ the Frobenius automorphism of Q over P.

(a) Prove that $[L/E, Q] = [L/K, Q]^{f(R/P)}$.

(b) Suppose that H is normal in G. Prove that $[E/K, R]$ is the restriction of $[L/K, Q]$ to E.

Exercise 46. Prove that there is a bijection between the set of extensions R' of P to E and the set of orbits Y of X under the action of G_Q, with the following property. If R' corresponds to Y, then the length $\#Y$ of the orbit Y equals $e(R'/P)f(R'/P)$, and Y is the disjoint union of $f(R'/P)$ orbits of length $e(R'/P)$ under the action of I_Q.

Exercise 47. Suppose that G is isomorphic to the symmetric group S_5 of order 120, that G_Q has order 6, and that I_Q has order 2.

(a) Prove that, if the identification of G with S_5 is suitably chosen, G_Q is generated by the permutation $(1\,2\,3)(4\,5)$ and I_Q by $(4\,5)$.

(b) Suppose that $[E : K] = 5$. How many extensions R' does P have to E, and what are the numbers $e(R'/P)$ and $f(R'/P)$?

(c) Suppose that $[E : K] = 15$. How many extensions R' does P have to E, and what are the numbers $e(R'/P)$ and $f(R'/P)$?

Exercise 48. Suppose that G is isomorphic to the symmetric group S_4 of order 24, and that Q is the *only* prime of L extending P.

(a) Prove that P is 2-adic, in the sense that the restriction of P to $\mathbf{Q}$ is the 2-adic prime of $\mathbf{Q}$.

(b) Determine G_Q and I_Q as subgroups of S_4.

(c) Suppose that H is cyclic of order 4. Determine $e(Q/R)$, $f(Q/R)$, $e(R/P)$, and $f(R/P)$.

Exercise 49. Let m be a positive integer, and denote by ζ a primitive mth root of unity in some extension of the base field.

(a) Let K be an algebraic number field, let P be a non-zero prime ideal of the ring of integers of K, and $\mathbf{N}P$ its norm (i. e., the cardinality of the residue class field of P). Prove

that if $m \notin P$, then P is unramified in $K(\zeta)$, and the Artin symbol $(K(\zeta)/K, P)$ maps ζ to $\zeta^{\mathbf{N}P}$.

(b) Let p be a prime number, and let m_0 be the largest divisor of m that is not divisible by p. Prove that, under the isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong (\mathbf{Z}/m\mathbf{Z})^*$ that sends σ to $(a \bmod m)$ if $\sigma\zeta = \zeta^a$, the inertia group of p for the extension $\mathbf{Q} \subset \mathbf{Q}(\zeta)$ corresponds to $\{a \in (\mathbf{Z}/m\mathbf{Z})^* : a \equiv 1 \bmod m_0\}$, and the decomposition group to $\{a \in (\mathbf{Z}/m\mathbf{Z})^* : a \equiv p^i \bmod m_0 \text{ for some } i \in \mathbf{Z}\}$. What is the decomposition group of the infinite prime for the same extension?

Exercise 50. Let $\mathbf{Q} \subset L$ be a finite Galois extension with group G. Prove that G is, as a group, generated by the inertia groups I_P of the non-archimedean primes P of L over $\mathbf{Q}$.

Exercise 51. Let n be a positive integer, and denote by S_n the symmetric group of degree n.

(a) Let $G \subset S_n$ be a transitive subgroup that is generated by transpositions. Prove that $G = S_n$.

(b) Let K be an algebraic number field with $n = [K : \mathbf{Q}]$. Suppose that the discriminant of K over $\mathbf{Q}$ is squarefree. Prove that the Galois closure L of K over $\mathbf{Q}$ has degree $n!$, and that $\mathrm{Gal}(L/\mathbf{Q}) \cong S_n$.

Exercise 52. Let $K \subset L$ be a finite Galois extension of algebraic number fields, with Galois group G, and with rings of integers $A \subset B$. For $\sigma \in G$, let J_σ be the B-ideal generated by $\{\sigma b - b : b \in B\}$. Let $H \subset G$ be a subgroup, and let $E = L^H$ be the corresponding intermediate field. We write X for the transitive G-set G/H corresponding to E.

(a) Prove: if $\mathcal{D}_{E/K}$ denotes the different of E over K, then

$$\mathcal{D}_{E/K} B = \prod_{\sigma \in G - H} J_\sigma.$$

(You may assume the corresponding local fact.)

(b) Define $m(\sigma) = \#\{x \in X : \sigma x \neq x\}$ for $\sigma \in G$. Prove: if $\Delta_{E/K}$ denotes the discriminant of E over K, then

$$\Delta_{E/K}^{[L:K]} = \prod_{\sigma \in G - \{1\}} (\mathbf{N}_{L/K} J_\sigma)^{m(\sigma)}.$$

Exercise 53. Let K be an algebraic number field. For an irreducible monic polynomial $f \in K[t]$ we let $\delta(f)$ be the discriminant of $K[t]/fK[t]$ over K; this is an ideal of the ring

of integers of K. We extend the definition of $\delta(f)$ to all monic polynomials f by means of the rule $\delta(f_1)\delta(f_2) = \delta(f_1 f_2)$.

(a) Let $f \in K[t]$ be a monic separable polynomial, and let L be a finite Galois extension of K that contains a splitting field of f. Express $\delta(f)$ in terms of the ideals J_σ from the previous exercise and the numbers $\#\{\alpha \in L : f(\alpha) = 0,\ \sigma\alpha \neq \alpha\}$, for $\sigma \in \mathrm{Gal}(L/K)$.

(b) Let n be a positive integer and $a \in K^*$. Prove that $\delta(t^n - a)$ is divisible by $\delta(t^n - 1)$.

Exercise 54. Let K be an algebraic number field. Construct a translation invariant metric on the adele ring V_K of K that induces the given topology on V_K, and show that V_K is complete with respect to this metric.

In Exercises 55–59 we let K be an algebraic number field and A its ring of integers. We write $\hat{A}$ for the projective limit of the finite rings A/nA, with n ranging over the set of positive integers. The idele class group of K is denoted by C_K, and the ideal class group of A by Cl_A.

Exercise 55. Prove that $\hat{A}^* \cong \prod_{v<\infty} A_v^*$ (as topological groups), with v ranging over the finite primes of K and A_v denoting the valuation ring of the completion of K at v.

An exact sequence $0 \to B \to C \to D \to 0$ of topological abelian groups with continuous group homomorphisms is said to *split* if there is an isomorphism $f\colon C \to B \times D$ of topological groups such that (i) the map $B \to C \to B \times D$ is the canonical inclusion $B \to B \times D$; and (ii) the map $C \to B \times D \to D$ is the given map $C \to D$.

Exercise 56. Denote by $V_{\mathbf{Q}}$ the adele ring of $\mathbf{Q}$. In class it was shown that there is an exact sequence $0 \to \hat{\mathbf{Z}} \to V_{\mathbf{Q}}/\mathbf{Q} \to \mathbf{R}/\mathbf{Z} \to 0$ of topological abelian groups.

(a) Prove that $V_{\mathbf{Q}}/\mathbf{Q}$ is connected. Deduce that the sequence does not split, even if in the definition given above the map f is only required to be an isomorphism of topological *spaces* satisfying (i) and (ii).

(b) Prove that $V_{\mathbf{Q}}/\mathbf{Q}$ has a $\mathbf{Q}$-vector space structure. Deduce that the sequence does not split, even if in the definition given above the map f is only required to be a *group* isomorphism satisfying (i) and (ii).

Exercise 57. In class we proved that there is a surjective group homomorphism $g\colon C_K \to \mathrm{Cl}_A$ such that the kernel $\ker g$ of g fits in an exact sequence

$$(*) \qquad 0 \to \hat{A}^* \to \ker g \to (K \otimes_{\mathbf{Q}} \mathbf{R})^*/A^* \to 0$$

of topological abelian groups.

(a) Suppose that $K \neq \mathbf{Q}$. Prove that A^* contains a unit $u \neq 1$ that is *totally positive* in the sense that $\sigma u > 0$ for every field homomorphism $\sigma\colon K \to \mathbf{R}$. Prove also that for every such u there is a path in $\ker g$ from 1 to u, where u is now viewed as an element of $\hat{A}^*$ via the natural inclusion $A^* \subset \hat{A}^*$. (A *path* is a continuous image of the unit interval $[0, 1]$.)

(b) Prove that the sequence $(*)$ splits if and only if $K = \mathbf{Q}$.

Exercise 58. Let D_K be the intersection of all open subgroups of C_K, and denote by G_K^{ab} the Galois group of the maximal abelian extension of K over K.

(a) Prove that $C_K/D_K \cong G_K^{\mathrm{ab}}$. (You may use class field theory.)

(b) Denote by S the set of real places of K. Prove that there is an exact sequence

$$0 \to \big(\hat{A}^* \times \{\pm 1\}^S\big)/\operatorname{cl} A^* \to C_K/D_K \to \mathrm{Cl}_A \to 0$$

of topological abelian groups; here A^* is viewed as a subgroup of $\hat{A}^* \times \{\pm 1\}^S$ via the natural inclusion $A^* \subset \hat{A}^*$ and the map $A^* \to \{\pm 1\}^S$ that sends a unit to its signs under the real embeddings of K, and $\operatorname{cl} A^*$ denotes the closure of A^* in $\hat{A}^* \times \{\pm 1\}^S$.

(c) What do (a) and (b) come down to for $K = \mathbf{Q}$?

Exercise 59. Let $K \subset E$ be a finite extension, and let L be the largest subextension of $K \subset E$ for which $K \subset L$ is abelian. Use the main theorem of class field theory to show that $N_{E/K} C_E = N_{L/K} C_L$.

Exercise 60. Let k be a finite field, and let $K = k(t)$, where t is transcendental over k. We write $A = k[t]$, and we let $\hat{A}$ be the projective limit of the rings A/fA, with f ranging over $A - \{0\}$. Let V_K and $J_K = V_K^*$ be the adele ring and the idele group of K. We denote by $k[[u]]$ the ring of power series in one variable u over k.

(a) Prove: $V_K/K \cong uk[[u]] \times \hat{A}$ as topological groups.

(b) Prove: $J_K/K^* \cong \mathbf{Z} \times (1 + uk[[u]]) \times \hat{A}^*$ as topological groups; here $1 + uk[[u]]$ denotes the kernel of the map $k[[u]]^* \to k^*$ that maps a power series to its constant term.

In Exercises 61–66 you may use the main theorem of class field theory. We let K be an algebraic number field. The class number of K is denoted by h_K.

Exercise 61. Let $K \subset L$ be a finite abelian extension, and let v be a finite prime of K. Prove that v^2 divides the conductor of L over K if and only if v is wildly ramified in L.

Exercise 62. Let $K \subset L$ be a finite abelian extension, and let v be a finite prime of K, lying over the rational prime p. Denote by e the ramification index of v over p, by e' the least integer $> e/(p-1)$, and by k the number of factors p in the exponent of the inertia group of v in $\mathrm{Gal}(L/K)$. Prove: if v^m is the largest power of v dividing the conductor of L over K, then $m \leq e' + ke$. (*Hint*: use Exercise 16.)

Exercise 63. (a) Prove that the Hilbert class field of $\mathbf{Q}(\sqrt{-15})$ is $\mathbf{Q}(\sqrt{-3}, \sqrt{5})$.

(b) Prove that the Hilbert class field of $\mathbf{Q}(\sqrt{-23})$ is the splitting field of $X^3 - X - 1$ over $\mathbf{Q}$.

Exercise 64. Let E, F be two finite extensions of $\mathbf{Q}$ inside a common overfield. Prove: if $h_E = h_F = 1$, then $h_{E \cap F} = 1$.

Exercise 65. The *Hilbert class field tower* of K is the sequence of fields $K = H^{(0)}(K) \subset H^{(1)}(K) \subset H^{(2)}(K) \subset \ldots \subset H^{(i)}(K) \subset \ldots$, where each $H^{(i)}(K)$ is the Hilbert class field of $H^{(i-1)}(K)$. The Hilbert class field tower is said to be *finite* if $H^{(i+1)}(K) = H^{(i)}(K)$ for some i. Prove that the Hilbert class field tower of K is finite if and only if there is a finite extension E of K with $h_E = 1$.

Exercise 66. Let p be a prime number, and let $K \subset L$ be an abelian extension of degree p.

(a) Let G be a p-group, i. e., a finite group of which the cardinality is a power of p, and let H be a subgroup of G with $H \neq G$. Prove that G has a normal subgroup N with $H \subset N$, $N \neq G$.

(b) Suppose that at most one prime of K is ramified in L. Prove: if p divides h_L, then p divides h_K.

(c) Suppose that at least one prime of K is ramified in L. Prove: if p divides h_K, then p divides h_L.

Exercise 67. Let G be a cyclic group, and let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules. Prove that there is a map $C^G \to A_G$ such that the sequence $0 \to A^G \to B^G \to C^G \to A_G \to B_G \to C_G \to 0$ is exact. In which way does your map depend on the choice of a generator for G?

Exercise 68. Let G be a finite cyclic group, n the order of G, and q a positive rational number. Prove that there exists a G-module A for which the Herbrand quotient $Q(G, A)$ is defined and equal to q if and only if $q \in \mathbf{Z}[1/n]^*$.

Exercise 69. Let $K \subset L$ be a finite Galois extension of algebraic number fields, with a cyclic Galois group G. Let J_L be the group of ideles of L. Prove that $H^1(G, J_L) = 0$.

In Exercises 70–72 you may use the main theorem of class field theory.

Exercise 70. Let K be an algebraic number field, and let L be a finite extension of K inside some algebraic closure of K. Prove that the norm map of class groups $\mathrm{Cl}_L \to \mathrm{Cl}_K$ is trivial if and only if L contains the Hilbert class field of K.

Exercise 71. In this exercise and the following we let $K = \mathbf{Q}(\sqrt{-3})$ and $L = K(2^{1/3})$. We write μ_3 for the subgroup of K^* generated by the cube root of unity $(-1 + \sqrt{-3})/2$. The unique primes of K lying over 2 and 3 are denoted by 2 and $\mathfrak{t}$, respectively.

(a) Prove that $K \subset L$ is cyclic of degree 3, and that the map $\epsilon\colon \mathrm{Gal}(L/K) \to \mu_3$ sending σ to $\sigma(2^{1/3})/2^{1/3}$ is a group isomorphism.

(b) Show that the conductor $\mathfrak{f}_{L/K}$ divides $2\mathfrak{t}^4$.

(c) Let $\mathfrak{p}$ be a finite prime of K not dividing $2\mathfrak{t}$, and let $\mathbf{N}\mathfrak{p}$ be the cardinality of its residue class field. Prove that $\epsilon((\mathfrak{p}, L/K))$ is the unique element of μ_3 that is congruent to $2^{(\mathbf{N}\mathfrak{p}-1)/3}$ modulo $\mathfrak{p}$.

Exercise 72. (a) Show that L is the ray class field of K modulo 6 $(= 2 \cdot \mathfrak{t}^2)$.

(b) Let p be a prime number, and let m be the number of distinct cube roots of $(2 \bmod p)$ in $\mathbf{F}_p$. Prove the following:

$m = 0$ if and only if $p \equiv 1 \bmod 3$ and p is not of the form $a^2 + 27b^2$, with $a, b \in \mathbf{Z}$;

$m = 1$ if and only if $p \not\equiv 1 \bmod 3$;

$m \neq 2$;

$m = 3$ if and only if $p = a^2 + 27b^2$ for certain $a, b \in \mathbf{Z}$.

In Exercises 73–78 we denote by K an algebraic number field, with discriminant Δ_K and with ring of integers A.

Exercise 73. (a) Let $a \in A$. Suppose that for all but finitely many prime ideals $\mathfrak{p}$ of A there exists $b_\mathfrak{p} \in A$ with $a \equiv b_\mathfrak{p}^2 \bmod \mathfrak{p}$. Prove that there exists $b \in A$ with $a = b^2$.

(b) Let $m \in \mathbf{Z}$, $m > 0$. Suppose that for all but finitely many primes v of K the completion K_v contains a primitive mth root of unity. Prove that K contains a primitive mth root of unity.

Exercise 74. Let $l \in \mathbf{Z}$, $l > [K : \mathbf{Q}]$. Prove that the number of roots of unity in K is equal to the greatest common divisor of the numbers $\mathbf{N}\mathfrak{p} - 1$, where $\mathfrak{p}$ ranges over all prime ideals of A for which $A/\mathfrak{p}$ has characteristic greater than l; here we write $\mathbf{N}\mathfrak{p} = \#A/\mathfrak{p}$.

In Exercises 75–78 you may use the main theorem of class field theory.

Exercise 75. Suppose that K is cubic, i. e., $[K : \mathbf{Q}] = 3$, and that Δ_K is not a square.

(a) Prove that the Galois closure M of K over $\mathbf{Q}$ contains a unique quadratic subfield L, and that Δ_L divides Δ_K.

(b) Prove that $\Delta_L = \Delta_K$ if and only if M is totally unramified over L, and that in this case the class number of L is divisible by 3.

Exercise 76. Suppose that K is quartic, i. e., $[K : \mathbf{Q}] = 4$, and that K does not contain a quadratic subfield.

(a) Prove that the Galois closure M of K over $\mathbf{Q}$ contains a cubic subfield L, which is uniquely determined up to isomorphism, and that Δ_L divides Δ_K.

(b) Prove that $\Delta_L = \Delta_K$ if and only if there is no finite prime of the Galois closure of L over $\mathbf{Q}$ that ramifies in M, and that in this case the strict class number of L is even.

Exercise 77. Let d be a squarefree integer with $d \equiv 3 \bmod 8$, $d > 3$. Prove that there exists a cubic field with discriminant $-d$ or $-4d$.

Exercise 78. Suppose that the class number of K is a prime number p. Prove that the class number of the Hilbert class field of K is not divisible by p.

In Exercises 79–84 we denote by K an algebraic number field. You may use the main theorem of class field theory.

Exercises 79 and 80 concern the following result, which was proved in class as a consequence of the first inequality:

(A) *if $K \subset L$ is a finite Galois extension, and S is a finite set of primes of L containing the infinite ones and the primes that ramify over K, then* $\mathrm{Gal}(L/K)$ *is generated by* $\{[\mathfrak{q}, L/K] : \mathfrak{q}$ *is a prime of* L, $\mathfrak{q} \notin S\}$.

Actually a stronger theorem is valid:

(B) *if $K \subset L$ is a finite Galois extension, then for every element $\sigma \in \mathrm{Gal}(L/K)$ there exist infinitely many finite primes $\mathfrak{q}$ of L, unramified over K, such that $\sigma = [\mathfrak{q}, L/K]$.*

Statement (B) is a consequence of Čebotarev's density theorem (Nikolai Gregorovič Čebotarev, Russian mathematician, 1894–1947), and its only known proof employs complex L-functions; see S. Lang, *Algebraic number theory*, Ch. VIII, §4, Theorem 10. (Čebotarev's density theorem itself asserts a bit more, in that it makes "infinitely many" more precise.)

Exercise 79. (a) Dirichlet's theorem on primes in arithmetic progression asserts that for any two positive integers a, m with $\gcd(a, m) = 1$ there exist infinitely many prime

numbers p with $p \equiv a \bmod m$ (Peter Gustav Lejeune Dirichlet, German mathematician, 1805–1859). Show how to deduce this theorem from (B).

(b) Show how to deduce the special case $m = 24$, $a \not\equiv 1 \bmod 24$ of Dirichlet's theorem from (A).

Exercise 80. (a) Let G be a group acting transitively on a finite set Ω with $\#\Omega > 1$. Prove that there exists $\sigma \in G$ such that for all $\omega \in \Omega$ one has $\sigma\omega \neq \omega$.

(b) Let $f \in \mathbf{Z}[X]$ be an irreducible polynomial with the property that ($f \bmod p$) has a zero in $\mathbf{F}_p$, for all but finitely many primes p. Use (B) to show that f has degree 1.

(c) The classification of finite simple groups can be used to show that, for *finite* G, the element σ in (a) can be chosen to be of prime power order (see B. Fein, W. M. Kantor, M. Schacher, *J. Reine Angew. Math.* **328** (1981), 159–173). Prove that now (A) suffices to deduce the statement in (b).

Exercise 81. Let $K \subset L$ be a finite extension for which the group $K^*/N_{L/K}L^*$ is finite. Prove that $L = K$.

Exercise 82. Let α, β, $\gamma \in K$.

(a) Prove that there exist x, $y \in K$ with $\alpha x^2 + \beta y^2 = \gamma$ if and only if for each prime $\mathfrak{p}$ of K there exist x, $y \in K_\mathfrak{p}$ with $\alpha x^2 + \beta y^2 = \gamma$.

(b) Suppose that α, β and γ are non-zero. Prove that for all but finitely many primes $\mathfrak{p}$ of K there exist x, $y \in K_\mathfrak{p}$ with $\alpha x^2 + \beta y^2 = \gamma$.

Exercise 83. Let n be a positive integer, and denote by ζ_n a primitive n-th root of unity.

(a) Prove that the class number of $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$ divides the class number of $\mathbf{Q}(\zeta_n)$.

(b) Suppose that n is a power of 2, and that K is a subfield of $\mathbf{Q}(\zeta_n)$. Prove that the strict class number of K is odd.

Exercise 84. Let S be a set of primes of K containing the set of infinite primes, and let L be the maximal abelian totally unramified extension of K in which all primes in S split completely. Prove that there is a subring $B \subset K$, which is a Dedekind ring with field of fractions K, such that $\mathrm{Gal}(L/K)$ is isomorphic to the class group of B.