A Hodge-podge of Exercises  

archaic version

©1995, Paul Garrett, garrett@math.umn.edu

- Finite fields and other warm-ups
- Dedekind domains
- Factorization and splitting of primes
- Local fields
- Differents and discriminants
- Approximation
- Ideal class groups
- Adeles and ideles
- Zeta and L-functions
*** Some warm-ups ***

1. Let $K/F$ be a finite extension of finite fields. Show that trace and norm are onto.

2. For a prime $p$, show that $x^2 + y^2 + z^2 = 0 \mod p$ always has a non-trivial solution (i.e., with not all of $x, y, z$ equal 0).

3. Show that the Galois group of $x^5 - x + 1$ over $\mathbb{Q}$ is the symmetric group $S_5$ on 5 things. (**Hint:** think about decomposition groups and the Frobenius map $x \to x^5$).

4. Let $\phi$ be the $n^{th}$ cyclotomic polynomial, i.e., whose roots are the primitive $n^{th}$ roots of unity. Show that (a) If a prime $p$ divides $\phi(m)$ for some integer $m$, then $p \equiv 1 \mod n$. (**Hint:** $m$ is a primitive $n^{th}$ root of 1 modulo $p$). (b) For a prime $p$ and for any integer $m$, $p$ does not divide $\phi(mp)$. (**Hint:** The constant term of $\phi$ is 1). (c) There are infinitely many primes congruent to 1 modulo $n$. (**Hint:** Suppose there were only finitely many, say $p_1, \ldots, p_k$; consider $\phi(mp_1 \ldots p_k)$ for $m$ an integer chosen to avoid $\phi(mp_1 \ldots p_k) = 1$).

5. Determine the integral closure of $\mathbb{Z}$ in $\mathbb{Q}((\sqrt{D}))$ where $D$ is a square-free integer, directly from the definition of integral closure.

6. Show that a PID is integrally closed (in its fraction field). Then show that $\mathbb{Z}[\sqrt{5}]$ cannot be a PID because it is not integrally closed.

**Definition:** Let $k$ be a finite field not of characteristic two. For $T$ transcendental over $k$, let $o = k[T]$ and $K = k(T)$. A finite separable extension $E$ of $K$ is a function field (in one variable) over the finite field $k$.

7. Let $E$ be the extension of $k(T)$ obtained by adjoining the square root of a square-free monic polynomial. Determine the integral closure of $k[T]$ in $E$.

8. Let $o$ be the ring of integers in a number field $K$. Let $a$ be a non-zero ideal in $o$. Let $o/a$ be the quotient ring and $(o/a)\times$ its units. When it the latter group cyclic?

*** Splitting of primes ***

9. Show that, with respect to the usual complex norm, the Gaussian integers $\mathbb{Z}[i]$ form a Euclidean ring, so is a PID.

10. Show that an odd prime $p$ splits in $\mathbb{Q}(i)/\mathbb{Q}$ if and only if $p \equiv 1 \mod 4$.

11. Show that an odd prime $p$ is a sum of two square of integers if and only if $p \equiv 1 \mod 4$.

12. Let $\omega$ be a primitive cube root of unity. Determine the splitting behavior of primes in $\mathbb{Q}(\omega)/\mathbb{Q}$.
(13) Show that, with respect to the usual complex norm, the ring \( \mathbb{Z}[\omega] \) is Euclidean, so is a PID.

(14) Show that a prime \( p \) is of the form \( x^2 + xy + y^2 \) with integers \( x, y \) if and only if \( p \equiv 1 \mod 3 \).

(15) Let \( \zeta \) be a primitive \( n^{th} \) root of unity. \textit{Granting} that the ring of integers is \( \mathbb{Z}[\zeta] \), describe the splitting of a prime in the extension \( \mathbb{Q}(\zeta)/\mathbb{Q} \) in terms of congruence properties of \( p \).

(16) Suppose that a finite field \( k \) does not contain \( \sqrt{-1} \). Determine which primes \( \mathfrak{p} \) split in the extension \( k(T)(i) = k(T, i) \) of \( k(T) \) (with base ‘integers’ \( k[T] \), as usual).

(17) Suppose that the finite field \( k \) \textit{does not} contain a primitive \( n^{th} \) root of unity \( \zeta \). Determine the integral closure of \( k[T] \) in \( k(\zeta)(T) \approx k(T, \zeta) \). Determine which primes \textit{split completely} in this extension.

(18) Suppose that there is a Galois extension of global fields so that some prime is \textit{inertial}. Show that the extension is necessarily \textit{cyclic}. \textbf{(Hint: Think about decomposition groups)}.

*** Local fields ***

(19) Let \( K \) be a local field not of characteristic 2, with valuation ring \( o \). Let \( \alpha \in o^\times \). Show that \( \alpha \) is a square in \( o^\times \) if and only if it is a square in \( (o/p)^\times \).

(20) Let \( K \) be a local field not of characteristic 2. Describe the structure of the group \( K^\times/K^\times 2 \). (First treat the case that the \textit{residue} characteristic is not 2, which is much easier).

(21) Determine all quadratic extensions of \( \mathbb{Q}_p \). Which are ramified? \textbf{(Hint: Treat \( p = 2 \) separately, and certainly use the structure of \( \mathbb{Q}_p^\times/\mathbb{Q}_p^\times 2 \)).}

(22) Determine all quadratic extensions of the \( T \)-adic completion \( k((T)) \) (i.e., formal finite Laurent series field) of \( k(T) \).

(23) Generalizing the previous exercise, determine all quadratic extensions of the \( P \)-adic completion of \( k(T) \).

(24) Determine all cyclic (Galois) cubic extensions of \( \mathbb{Q}_p \).

(25) Determine all \textit{non-Galois} cubic extensions of \( \mathbb{Q}_p \).

(26) For a local field \( K \), determine the structure of \( K^\times/K^\times m \) for positive integer \( m \). \textbf{(Hint: First treat the case that the residue characteristic does not divide \( m \)).}

(27) Suppose that a local field contains all \( m^{th} \) roots of unity. Determine all cyclic extensions of it.

(28) Show (qualitatively) that a local field has finitely-many extensions of a given degree.
(29) Show that a local field has a unique unramified extension of a given degree. (Hint: If an extension is unramified, then the Galois group is the decomposition group, which is the Galois group of the residue class field extension, which is generated by a root of unity. Use Hensel’s lemma).

(30) Let $K/k$ be a finite and unramified extension of local fields, with rings of integers $O,o$. Show that trace maps $O$ surjectively to $o$ and the norm maps $O^\times$ surjectively to $o^\times$.

(31) In the previous situation, show that if the norm maps $O^\times$ surjectively to $o^\times$ then the extension is unramified.

(32) Let $S$ be a symmetric $n$-by-$n$ matrix over $\mathbb{Q}_p$. When $p \neq 2$, show that there is $A \in GL(n, \mathbb{Z}_p)$ so that $A^T S A$ is diagonal. Show that this fails if $p = 2$.

(33) Redo the previous exercise over an arbitrary local field of residue characteristic not 2.

*** Differents, discriminants, ramification ***

(34) Find a $\mathbb{Z}$-basis for the ring of algebraic integers in $\mathbb{Q}(\alpha)$, where $\alpha^3 = a$ with $a \in \mathbb{Z}$ square-free. Determine the ramification. You can accomplish this by brute force.

(35) Carefully compute the discriminant and different of $\mathbb{Z}[\zeta]$ for roots of unity $\zeta$.

(36) Find a $\mathbb{Z}$-basis for the ring of algebraic integers in $\mathbb{Q}(\alpha)$, where $\alpha^n = a$ with $a \in \mathbb{Z}$ square-free. Determine the ramification of some small primes. You probably cannot accomplish this by brute force alone.

(37) Let $E = K(\alpha)$ where $K$ is a global field and $\alpha^2 = a$ with a square-free element $a \in \mathfrak{o}$ where $\mathfrak{o}$ is the ring of integers in $K$. Extending the standard computation for $K = \mathbb{Q}$, determine the ring of integers in $E$. (Hint: Brute force probably will fail. Do local computations).

(38) Do the notions of different and discriminant work the same way for function fields as for number fields?

(39) If the extension $K/k(T)$ of a function field $k(T)$ is obtained merely by ‘extending scalars’ $K = k(T)$ (with $k'$ a finite extension of the finite field $k$), then what are the different, discriminant, and ramification?

*** Approximation ***

(40) Let $S$ be a finite set of primes in $\mathbb{Z}$, including the infinite prime $\infty$. Let $\mathbb{Z}_S$ be the ring of rational numbers which are $p$-integral for every finite prime $p \notin S$. Consider the natural imbedding $\mathbb{Z}_S \rightarrow \prod_{p \in S} \mathbb{Q}_p$. Show that the image is discrete. Show that the image of $\mathbb{Z}_S$ in $\prod_{p \in T} \mathbb{Q}_p$ is dense for any proper subset $T$ of $S$.

(41) Do the previous exercise for any global field.
(42) Let \(1 < N \in \mathbb{Z}\). Show that the natural map
\[
SL(2, \mathbb{Z}) \to SL(2, \mathbb{Z}/N)
\]
is a surjection.

(43) More generally, let \(k\) be a global field with integers \(o\). Let \(a\) be a proper ideal of \(o\). Show that the natural map
\[
SL(n, o) \to SL(n, o/a)
\]
is a surjection. Do the same for groups \(GL(n)\).

(44) For a finite field \(k\) with \(q\) elements, compute the cardinality of \(SL(n, k)\) and \(GL(n, k)\).

(45) Let \(o\) be the integers in a global field and \(p\) a non-zero prime ideal in \(o\). Compute the cardinality of \(SL(n, o/p^m)\) and \(GL(n, o/p^m)\).

(46) Let \(o\) be the integers in a global field and \(a\) a non-zero ideal in \(o\). Compute the cardinality of \(SL(n, o/a)\) and \(GL(n, o/a)\).

*** Ideal class groups ***

(47) Determine the (absolute) ideal class group structure for the ring of algebraic integers in \(\mathbb{Q}(\sqrt{-D})\) for \(D = 1, 2, 3, 5, 6, 7, 10, 11, 13, 15\) using the Minkowski estimate for a representative for ideal classes. Here one can take advantage of the fact that the only units are \(\pm 1\). (Hint: Use relations coming from norms, as follows: for example, suppose that the norm from \(\mathbb{Q}(\sqrt{-D})\) to \(\mathbb{Q}\) of \(a\) is \(pq\) with distinct primes \(p, q\). Then we can conclude that there are primes \(p, q\) lying over \(p, q\), respectively, so that \(pq = \alpha\) is principal, so is trivial in the ideal class group.)

(48) Determine the (absolute) ideal class group structure for the ring of algebraic integers in \(\mathbb{Q}(\sqrt{D})\) for \(D = 1, 2, 3, 5, 6, 7, 10, 11, 13, 15\) using the Minkowski estimate for a representative for ideal classes, after determining a ‘fundamental unit’. Use relations coming from norms.

(49) Try the same sort of thing for \(\mathbb{Q}(\zeta_5)\) and \(\mathbb{Q}(2^{1/3})\).

(50) Let \(p_1, \ldots, p_m\) be distinct odd primes in \(\mathbb{Z}\), and put \(D = p_1 \ldots p_m\). Show that the ideal class group of the ring of algebraic integers in \(\mathbb{Q}(\sqrt{p_1 \ldots p_m})\) has a subgroup isomorphic to
\[
\mathbb{Z}/2 \oplus \ldots \oplus \mathbb{Z}/2 \quad m - 1 \text{ summands}
\]
(Hint: Each \(p_i\) is ramified, so becomes \(p_i^2\), but it is hard for products of the various \(p_i\) to be principal ideals, since the norms of algebraic integers in the extension are ‘too large’).

(51) Do the previous exercise for a quadratic extension of \(k(T)\) so that the infinite prime is inert, where \(k\) is a finite field. (Hint: The condition on the infinite prime assures that the unit group is finite...)

(52) Let $\alpha$ be the integers in a global field $k$ so that there is a non-principal ideal $a$. Let $m$ be the least integer so that $\alpha^m$ is principal, i.e., is coprime for some algebraic integer $\alpha$. Suppose that $k$ contains the $m^{th}$ roots of unity. Let $K$ be the extension of $k$ obtained by adjoining an $m^{th}$ root of $\alpha$. Show that $K/k$ is not ramified at any prime not dividing $m$.

*** Adeles and ideles ***

(53) Show that the topology on the adeles $\mathbb{A}$ of a global field, restricted to the ideles $\mathbb{J}$, is strictly coarser than the idele topology.

(54) Embed $\mathbb{J} \rightarrow \mathbb{A} \times \mathbb{A}$ by $\alpha \rightarrow (\alpha, \alpha^{-1})$. Show that the idele topology is that given by the subspace topology on the image by this map.

(55) Let $k$ be a global field. Show (or recall) that the natural image of $k$ in its adeles is discrete. Show that for any prime $p$ of $k$, the set $k + k_p$ is dense.

*** Zeta and L-functions ***

(56) Write the zeta function of a quadratic extension of $\mathbb{Q}$ as a product of two Dirichlet L-functions over $\mathbb{Q}$.

(57) Write the zeta function of $\mathbb{Q}(\zeta_n)$ as a product of Dirichlet L-functions over $\mathbb{Q}$.