E. Dummit's Math 7315 ∼ Algebraic Number Theory, Fall 2024 ∼ Homework 4, due Mon Nov 18th.

Solve whichever problems you haven't seen before that interest you the most (suggestion: between 20 and 40 points' worth). Starred problems are especially recommended. Prepare to present 1-2 problems in class on the due date.

0.1 In-Lecture Exercises

0.1.1 Exercises from (Oct 24)

1. [2pts] For a Dedekind domain R with fraction field K, show that the sequence of multiplicative groups $1 \to \mathcal{O}_K^* \hookrightarrow K^* \overset{a \mapsto aR}{\to} J_R \to \text{cl}(R) \to 1$ is exact. (It is analogous to, and in fact generalizes, the exact sequence $1 \to k^* \hookrightarrow k(C)^* \overset{f \mapsto \text{div}(f)}{\to} \text{Div}^0(C) \to \text{Pic}^0(C) \to 1$ for an algebraic curve C defined over an algebraically closed field k.)

2. [4pts*] For ideals I and J of a Dedekind domain R, write $I \sim J$ when there exist nonzero $\alpha, \beta \in R$ with $(\alpha)I = (\beta)J$.
   (a) Show that $\sim$ is an equivalence relation on the ideals of R.
   (b) Show that the multiplication operation $[I][J] = [IJ]$ on equivalence classes is well defined and gives the nonzero equivalence classes the structure of an abelian group G.
   (c) Show that the map $\varphi : G \to \text{cl}(R)$ given by $\varphi([I]) = \overline{I}$, where $\overline{I}$ denotes the image of I in the class group J_R/P_R, is well defined and an isomorphism.

3. [3pts] With the equivalence relation $\sim$ on ideals as given in the exercise above, show that $I \sim J$ if and only if I is isomorphic to J as an R-module. (Thus, the isomorphism classes of ideals are the same as the equivalence classes in the class group, yielding a third natural way to "discover" the class group.)

4. [2pts] Let L/K be an extension of number fields. Use the fact that the class group of $\mathcal{O}_K$ is finite to give another proof that $N_L(I\mathcal{O}_K) = N_K(I)^{[L:K]}$ for any ideal I of $\mathcal{O}_K$. [Hint: What can be said about $I^{h(K)}$?]

0.1.2 Exercises from (Oct 28)

1. [1pt] Show that if $K/\mathbb{Q}$ is Galois, then K must be totally real or totally imaginary.

2. [1pt] Show that if K has signature (r, s), then the sign of $\text{disc}(K)$ is $(-1)^s$. [Hint: What does complex conjugation do to the discriminant matrix?]

3. [4pts*] Suppose G is an additive subgroup of $\mathbb{R}^n$. Show that the following are equivalent (in such a case we say G is discrete):
   (a) G is nowhere dense in $\mathbb{R}^n$.
   (b) Every compact subset of $\mathbb{R}^n$ contains finitely many points of G.
   (c) Some open neighborhood of 0 contains finitely many points of G.
   (d) The rank of G as an abelian group equals the dimension of $G \otimes_{\mathbb{Z}} \mathbb{R}$ as an $\mathbb{R}$-vector subspace of $\mathbb{R}^n$.

4. [1pt] Let K be a number field and $\varphi : K \to \mathbb{R}^n$ be the Minkowski map. Show that $\varphi(K)$ is dense in $\mathbb{R}^n$. [Hint: Replace integer coefficients with rational ones.]

5. [1pt] Suppose Λ is a lattice in $\mathbb{R}^n$ with an integral basis $v_1, \dots, v_n$. Show that the covolume of Λ is equal to $|\det(v_1, \dots, v_n)|$.

6. [2pts] Let Λ be a lattice in $\mathbb{R}^n$ whose fundamental domain has n-measure V. Show that if B is a convex closed centrally-symmetric set in $\mathbb{R}^n$ whose n-measure is greater than or equal to $2^n V$, then B contains a nonzero point of Λ.

0.1.3 Exercises from (Oct 31)

1. [2pts] Show that if K is a number field of degree n over $\mathbb{Q}$ with signature (r, s), show that $|\operatorname{disc} K| \geq (\frac{\pi}{4})^{2s}(\frac{n^n}{n!})^2$. Show also that if $n > 1$ then $|\operatorname{disc} K| > 1$, and deduce that $\mathbb{Q}$ has no unramified extensions.
2. [3pts] Show that for $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$, the class group of $\mathbb{Q}(\sqrt{D})$ is trivial.
3. [3pts] Show that for $D = 2, 3, 6, 11, 13, 15, 17, 19$, the class group of $\mathbb{Q}(\sqrt{D})$ is trivial.
4. [3pts] Show that for $D = 101, 103, 107, 109$, the class group of $\mathbb{Q}(\sqrt{D})$ is trivial.
5. [3pts] Show that $\mathbb{Q}(\sqrt{-10})$, $\mathbb{Q}(\sqrt{-13})$, and $\mathbb{Q}(\sqrt{-15})$ all have class number 2.
6. [3pts] Show that $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(\sqrt{14})$, $\mathbb{Q}(\sqrt{23})$, and $\mathbb{Q}(\sqrt{29})$ all have class number 2.
7. [3pts] Show that $\mathbb{Q}(\sqrt{-23})$, $\mathbb{Q}(\sqrt{-59})$, and $\mathbb{Q}(\sqrt{-83})$ all have class number 3.
8. [2pts] Show that $\mathbb{Q}(\sqrt{79})$ has class number 4. Which group is its class group isomorphic to?
9. [4pts] Show that $\mathbb{Q}(\sqrt{-17})$ and $\mathbb{Q}(\sqrt{-21})$ both have class number 4 but that their class groups are not isomorphic.
10. [3pts] Show that $\mathbb{Q}(\sqrt{-103})$ has class number 5.
11. [3pts] Show that $\mathbb{Q}(\sqrt{-29})$ has class number 6.
12. [3pts] Show that $\mathbb{Q}(\sqrt{-71})$ has class number 7.

0.1.4 Exercises from (Nov 4)

1. [1pt] Show that the class group of $K = \mathbb{Q}(\sqrt[3]{5})$ is trivial.
2. [2pts] Show that the class group of $K = \mathbb{Q}(\sqrt[3]{6})$ is trivial. (This can be done without computing an integral basis for the ring of integers, but it ends up being $\mathbb{Z}[\sqrt[3]{6}]$.)
3. [1pt] For $K = \mathbb{Q}(\alpha)$ with $\alpha^3 - \alpha + 1 = 0$, show that the class group of K is trivial.
4. [2pts*] Show that the class group of $\mathbb{Q}(\zeta_8)$ is trivial. [Hint: What is $N(1 - \zeta_8)$?]
5. [2pts] Show that the class group of $\mathbb{Q}(\zeta_9)$ is trivial.
6. [3pts] Show that the class group of $\mathbb{Q}(\zeta_{11})$ is trivial. [This isn't as bad as it might look, but there is one difficult prime. Try computing $N(1 + \zeta_{11} - \zeta_{11}^8)$.]
7. [3pts*] Show that the class group of $\mathbb{Q}(\zeta_{23})$ has order divisible by 3. [Hint: Let P be a prime lying above 23 in $\mathbb{Q}(\sqrt{-23})$ and let Q lie above P in $\mathbb{Q}(\zeta_{23})$. Show that $N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}(\sqrt{-23})}(Q) = P$ and that P is nonprincipal; deduce Q is nonprincipal and in fact that $[Q]$ has order 3.]
8. [2pts] Show that the class group of $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ is trivial but that the class group of $F = \mathbb{Q}(\sqrt{-6})$ has order 2. Deduce that a subring of a principal ideal domain need not be a principal ideal domain.

0.1.5 Exercises from (Nov 6)

1. [1pt] Let F be a field and let G be a finite multiplicative subgroup of the multiplicative group $F^\times$. Show that G is cyclic. [Hint: Consider solving $x^{\#G} - 1 = 0$ in $F[x]$.]
2. [2pts] Suppose that M is an $m \times m$ real matrix whose diagonal entries are positive, whose off-diagonal entries are negative, and whose row sums are all zero. Show that M has rank $m - 1$ and that any $m - 1$ columns are a basis for M. [Hint: Suppose there is a linear dependence involving $m - 1$ of the columns. Rescale to assume that the largest coefficient a_k of the dependence is 1 and the others are at most 1. Look at the kth row to obtain a contradiction.]
3. [2pts] Suppose K is a real quadratic field. Show that there are four possible fundamental units, and if one of them is u then the others are $-u$, $\overline{u}$, and $-\overline{u}$. Conclude that there is a unique fundamental unit of the form $a + b\sqrt{D}$ where $a, b \in \mathbb{Q}$ are positive, and indeed that among all units of $\mathcal{O}_K$ with positive coefficients, the fundamental unit is the one with a and b minimal.

0.1.6 Exercises from (Nov 7)

1. [3pts*] Find the fundamental units for the quadratic fields $\mathbb{Q}(\sqrt{D})$ for $D = 15$, 17, 19, 21, 22, 23, 26.
2. [2pts] For $\alpha^3 - \alpha + 1 = 0$, show that α is the fundamental unit of $\mathbb{Q}(\alpha)$.
3. [3pts] Show that $4 + 2\sqrt[3]{7} + \sqrt[3]{49}$ is the fundamental unit of $\mathbb{Q}(\sqrt[3]{7})$.
4. [3pts] Show that $\frac{1}{3}(23 + 11\sqrt[3]{10} + 5\sqrt[3]{100})$ is the fundamental unit of $\mathbb{Q}(\sqrt[3]{10})$.
5. [1pt] Show that the unit ranks of $K = \mathbb{Q}(\zeta_n)$ and $K_+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ are both equal to $\frac{1}{2}\varphi(n) - 1$.
6. [2pts] Suppose that L/K is an extension of number fields. Show that L and K have the same unit rank if and only if L is totally complex, K is totally real, and $[L : K] = 2$, in which case $K = L \cap \mathbb{R}$ is the maximal real subfield of L.
7. [2pts*] Show that $1 + \zeta_8 + \zeta_8^2$ is a fundamental unit for $\mathbb{Q}(\zeta_8)$.

0.2 Additional Exercises

1. [7pts] The goal of this problem is to give an upper bound estimate, due to Landau, for the class number in terms of the discriminant. Let K be a number field of degree n over $\mathbb{Q}$ and let $\Delta = |\mathrm{disc}(K)|$. For an integer a, let $F(a)$ denote the number of distinct ideals of $\mathcal{O}_K$ of norm a.

   (a) Show that $F(ab) = F(a)F(b)$ for relatively prime a, b.

   (b) For a prime p, show that $F(p^d)$ equals the number of nonnegative integer solutions $(a_1, \ldots, a_k)$ to $d = a_1 f_1 + \cdots + a_k f_k$ where the f_k are the inertial degrees of the prime ideals of $\mathcal{O}_K$ lying above p. Deduce that $F(p^d) \le \binom{d+n}{n}$.

   (c) Show that $F(a) = O(a^\epsilon)$ for any $\epsilon > 0$, in the sense that for any $\epsilon > 0$ there exists a positive constant C_ϵ such that $F(a) \le C_\epsilon a^\epsilon$ for all a.

   (d) Show that $h(K) = O(\Delta^{(1/2)+\epsilon})$ for any $\epsilon > 0$. [Hint: The number of distinct ideal classes is at most $\sum_{a \le c_K} F(a)$ where c_K is the Minkowski constant for K.]

   Remark: We remark that another (much harder) theorem of Siegel shows that there exists a positive constant c such that $h(K) > c\Delta^{(1/2)-\epsilon}$ for all imaginary quadratic fields K, so that the upper bound of Landau is essentially sharp up to the $+\epsilon$ (which can in fact be replaced by a suitable power of $\log \Delta$, if one goes more carefully through the argument above).

2. [5pts*] The goal of this problem is to prove the following result of Kummer: for any number field K, there exists an extension field L/K such that every ideal of $\mathcal{O}_K$ becomes principal in $\mathcal{O}_L$.

   (a) Suppose the classes of the ideals $X_1, \ldots, X_k$ generate the ideal class group. Show that there exist elements $a_i \in \mathcal{O}_K$ with $X_i^{h(K)} = (a_i)$.

   (b) Continuing (a), let b_i be a root of the polynomial $x^{h(K)} - a_i$ in the algebraic closure $\overline{K}$. Show that X_i becomes principal in the extension $K(b_i)$.

   (c) Continuing (b), let $L = K(a_1, \ldots, a_k)$. Show that every ideal I of $\mathcal{O}_K$ becomes principal in $\mathcal{O}_L$. [Hint: Write the ideal class of I as a product of powers of the X_i.]

3. [6pts] Here is another proof of Stickelberger's criterion that uses our results about ramification. Suppose K is a number field with discriminant D.

   (a) Suppose that D is even, so that 2 is ramified in K. Let P be a prime ideal of $\mathcal{O}_K$ lying above 2 with $e(P|p) > 1$. Show that P^2 divides $D_{K/\mathbb{Q}}$ and conclude that $D \equiv 0 \pmod 4$. [Hint: Consider the two cases $e(P|p) = 2$ and $e(P|p) \ge 3$.]

   (b) Suppose that $D = u^2 d$ where u, d are both odd and d is squarefree and greater than 1. Show that 2 must be unramified in $\mathbb{Q}(\sqrt{d})$ and deduce that $D \equiv 1 \pmod 4$. [Hint: K contains $\sqrt{\mathrm{disc}(K)}$.]

   (c) Show that $D \equiv 0$ or $1 \pmod 4$.

4. [6pts*] By Stickelberger's criterion (see above, or homework 1), the discriminant D of a number field must be 0 or 1 modulo 4. The goal of this problem is to find all of the number fields with discriminant D for various small values of D, and in particular to see that for some of these D there are no such fields.

   (a) Show that any cubic field has $|D| \geq 13$ and any field of degree 4 or higher has $|D| \geq 44$. [Use exercise 0.3.1.1.]

   (b) Show that there is a unique number field of each discriminant $D = -12, -11, -8, -7, -4, -3, 1, 5, 8$ and that there are no number fields of discriminants $D = 4$ and $D = 9$.

   (c) Show that there is no number field of discriminant $D = 16$ or 25. [Hint: A cubic field with such a discriminant must have Galois group A_3 hence by Kronecker-Weber it is a subfield of $\mathbb{Q}(\zeta_n)$ for some n. Considering ramification, explain why $n = 2^d$ or 5^d respectively, and obtain a contradiction.]

   Remark: With rather substantially more work, by using Minkowski's theorem and some very careful analysis of binary cubic forms, it can be shown that the smallest cubic discriminant is actually -23, from the field $K = \mathbb{Q}(\alpha)$ where $\alpha^3 - \alpha + 1 = 0$.

5. [8pts] All of the computations we have discussed can and have been implemented quite efficiently into software, such as Sage. The goal of this problem is to give a brief discussion of how to use Sage to perform some relevant calculations. For the field $K = \mathbb{Q}(a)$ where $a^3 - 109 = 0$, we may construct the field as follows:

```
R.<x> = PolynomialRing(QQ); K.<a> = NumberField( x^3 - 109 )
```

   The element a is now defined to be generator of the field K obtained as a root of the polynomial $x^3 - 109$. We can then construct ideals and elements in terms of the generator a: for instance, the ideal $I = (3, a - 1)$ can be constructed as

```
I = K.ideal([ 3, a - 1 ])
```

   and for instance we can ask for a reduced set of generators via

```
I.gens_reduced()
```

   and for a prime ideal factorization via

```
I.factor()
```

   The Sage documentation details how to use all of the relevant methods defined for number fields and ideals. For instance,

```
K.class_group()
```

   will return the ideal class group of K as an abstract group, while

```
K.class_group().gens()
```

   will compute an explicit list of generators for the ideal class group, and

```
K.unit_group()
```

   will return the unit group of $\mathcal{O}_K$ as an abstract group.

   For the fields $K = \mathbb{Q}(\sqrt[3]{109})$ and for $K = \mathbb{Q}(\zeta_{13})$, do the following:

   (a) Find the discriminant and regulator of K.

   (b) Find the prime factorization of the ideals (2), (3), (5), and (7) in $\mathcal{O}_K$.

   (c) Find the group structure for the ideal class group of K and an explicit list of generators.

   (d) Find the group structure for the unit group of $\mathcal{O}_K$ and an explicit list of generators.