Math 129: Algebraic Number Theory
Take-Home Final Examination

William Stein

Due: Monday, May 24, 2004 at 5pm

Remarks:
The exam is due on Monday May 24 at 5pm. You can turn it in either to my office (under the door) in print (preferred) or via email as a dvi file. This exam is worth 20% of your grade. I'm giving it to you well in advance of the due date so you have more flexibility relative to your schedule in choosing when to work on it.

Rules:
You are allowed to use a wide range of resources on this final exam, including the library, the internet, and computers. However, you can not collaborate with anybody else on the exam (no email or online chatting). If you do, it's cheating, and you'll have some bad luck, so don't risk it. If you find a mistake or have a question about a problem, email me and I'll post my answer to the virtual office hours page.

The 7 Problems: (each of equal weight)

1. (a) Define an analogue of Smith normal form for square matrices with entries in the ring $\mathbf{Z}[i]$ of integers of $\mathbf{Q}(\sqrt{-1})$.

   (b) Illustrate your answer to (a) by finding Smith normal form of the matrix
$$\begin{pmatrix} 2i & 1+i & 2-i \\ i & 2-3i & 3 \\ 1 & -3i & 5 \end{pmatrix}.$$

   (c) Does it make sense to define Smith normal form for squares matrices with entries in the ring of integers $\mathcal{O}_K$ of a general number field?

2. (a) Prove that there exists an algorithm that computes the group of units of a number field. (Remarks: It was clear that class groups are computable from the proof I gave of finiteness of class groups, but the proof I gave of Dirichlet's unit theorem did not show that the unit group can be computed in practice. Explain why it can

in fact be computed. Remember that for computability speed doesn't matter—what matters is that there is a finite procedure that is guaranteed to terminate with the answer. Solutions of this problem can be found in books and probably online, and I encourage you to look them up and explain what you find.)

(b) Compute the group of units of the cubic field $\mathbf{Q}(\sqrt[3]{2})$. Do more than just get the result from a few MAGMA commands; instead, use this as an example to illustrate your answer to the first part of the problem.

3. Use Hensel's lemma (which we didn't prove in class, but which you may assume) to prove that for every integer n the equation

$$3x^3 + 4y^3 + 5z^3 \equiv 0 \pmod{n}$$

has a solution besides the trivial solution $x \equiv y \equiv z \equiv 0 \pmod{n}$.

4. Let $\rho = \zeta_n + \zeta_n^{-1}$, where n is a primitive nth root of unity.

   (a) What additional condition on n is needed for the ring of integers of $\mathbf{Q}(\rho)$ to be $\mathbf{Z}[\rho]$?

   (b) Prove that your answer is correct. (Note: Getting the right answer in (a) without proof in (b) gives you 50% on this problem.)

5. Suppose K is a number field, $\mathcal{O}_K$ is the ring of integers of K, and $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$. Prove that there is a finite extension L of K such that the ideal $\mathfrak{a}\mathcal{O}_L$ of $\mathcal{O}_L$ is principal.

6. Compute the normalized Haar measure of $\mathbb{A}_K^+/K^+$ for $K = \mathbf{Q}$ and $K = \mathbf{Q}(i)$.

7. With some work we proved the following crucial lemma (see Lemma 20.4.1 in the book I made from the course notes, which is available at the course web page):

   Lemma 1.1. *Let K be a global field. There is a constant $C > 0$ that depends only on K with the following property:*
   Whenever $\mathbf{x} = \{x_v\}_v \in \mathbb{A}_K$ is such that

$$\prod_v |x_v|_v > C, \tag{1.1}$$

   then there is a nonzero principal adele $a \in K \subset \mathbb{A}_K$ such that

$$|a|_v \leq |x_v|_v \qquad \text{for all } v.$$

   Problem: Find a value of C that works for $K = \mathbf{Q}$. Then find an $a \in \mathbf{Q}$ as in the conclusion of the lemma for the adele $x = \{x_v\}_v$ with

$$x_\infty = 100,\ x_2 = 8,\ x_3 = 18, \text{ and } x_p = 1, \text{ for all } p \geq 5.$$