Math 129: Algebraic Number Theory
Homework Assignment 1

William Stein

Due: Thursday, February 19, 2004

Notes:

- Unless otherwise noted, if you can figure out how to use a computer program to solve a problem, please do. For complete credit you must describe exactly how you used the computer (commands typed, output, etc.) You might find `http://modular.fas.harvard.edu/calc/` useful.
- You are allowed to work with other people on homework problems, but you must acknowledge their assistance.
- Copying a homework solution if you find it in a book is allowed, but you must reword it in your own way and *cite your sources*. Learning to use the literature is valuable.
- If you have questions, email me at `was@math.harvard.edu`.

The problems:

1. Let $A = \begin{pmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \\ 0 & 0 & 0 \end{pmatrix}$.
   (a) Find invertible integer matrices P and Q such that PAQ is in Smith normal form.
   (b) What is the group structure of the cokernel of the map $\mathbf{Z}^3 \to \mathbf{Z}^3$ defined by multiplication by A?
2. Let G be the abelian group generated by x, y, z with relatoins $2x + y = 0$ and $x - y + 3z = 0$. Find a product of cyclic groups that is isomorphic to G.
3. Prove that each of the following rings have infinitely many prime ideals:
   (a) The integers $\mathbf{Z}$. [Hint: Euclid gave a famous proof of this long ago.]
   (b) The ring $\mathbf{Q}[x]$ of polynomials over $\mathbf{Q}$.
   (c) The ring $\mathbf{Z}[x]$ of polynomials over $\mathbf{Z}$.

(d) The ring $\overline{\mathbf{Z}}$ of all algebraic integers. [Hint: Use Zorn's lemma, which implies that every ideal is contained in a maximal ideal. See, e.g., Prop 1.12 on page 589 of Artin's *Algebra*.]

4. (This problem was on the graduate qualifying exam on Tuesday.) Let $\overline{\mathbf{Z}}$ denote the subset of all elements of $\overline{\mathbf{Q}}$ that satisfy a monic polynomial with coefficients in the ring $\mathbf{Z}$ of integers. We proved in class that $\overline{\mathbf{Z}}$ is a ring.
   (a) Show that the ideals (2) and $(\sqrt{2})$ in $\overline{\mathbf{Z}}$ are distinct.
   (b) Prove that $\overline{\mathbf{Z}}$ is not Noetherian.

5. Show that neither $\mathbf{Z}[\sqrt{-6}]$ nor $\mathbf{Z}[\sqrt{5}]$ is a unique factorization domain. [Hint: Consider the factorization into irreducible elements of 6 in the first case and 4 in the second. A nonzero element a in a ring R is an *irreducible element* if it is not a unit and if whenever $a = qr$, then one of q or r is a unit.]

6. Find the ring of integers of each of the following number fields:
   (a) $\mathbf{Q}(\sqrt{-3})$,
   (b) $\mathbf{Q}(\sqrt{3})$, and
   (c) $\mathbf{Q}(\sqrt[3]{2})$.

   Do not use a computer for the first two.

7. Find the discriminants of the rings of integers of the numbers fields in the previous problem. (Do not use a computer.)

8. Let R be a finite integral domain. Prove that R is a field. [Hint: Show that if x is a nonzero element, then x has an inverse by considering powers of x.]

9. Suppose $K \subset L \subset M$ is a tower of number fields and let $\sigma : L \hookrightarrow \overline{\mathbf{Q}}$ be a field embedding of L into $\overline{\mathbf{Q}}$ that fixes K elementwise. Show that σ extends in exactly $[M : L]$ ways to a field embedding $M \hookrightarrow \overline{\mathbf{Q}}$.

10. (a) Suppose I and J are principal ideals in a ring R. Show that the set $\{ab : a \in I,\, b \in J\}$ is an ideal.
    (b) Give an example of ideals I and J in the polynomial ring $\mathbf{Q}[x, y]$ in two variables such that $\{ab : a \in I,\, b \in J\}$ is not an ideal. Your example illustrates why it is necessary to define the product of two ideals to be the ideal generated by $\{ab : a \in I,\, b \in J\}$.
    (c) Give an example of a ring of integers $\mathcal{O}_K$ of a number field, and ideals I and J such that $\{ab : a \in I,\, b \in J\}$ is not an ideal.