Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Problem Set 1: The Gaussian Integers/Number Fields
Due in class September 5 (no class September 3: Labor Day)

Reference. Neukirch, Sections 1.1 and 1.2.

General reminder. If you submit a program that implicitly or explicitly requires use of Magma, please print out your Magma code and include it with your solutions. (Magma can be run on the Berkeley system by typing `magma` at any Unix prompt. For documentation, see the Magma home page.)

Exercises: Gaussian Integers.
Please submit four of the following.

1. If you've never seen Wilson's theorem before ($(p-1)! \equiv -1 \pmod{p}$), prove it. (Hint: pair each of $1, \dots, p-1$ with its inverse mod p.)
2. Show that any euclidean ring is factorial. (Hint: the key point is that if an irreducible element α divides a product $\beta\gamma$, then it divides one of β, γ or the other. Use the construction of the greatest common divisor from lecture.)
3. Write a Magma program that, given a prime $p \equiv 1 \pmod{4}$, computes integers a and b such that $p = a^2 + b^2$ using the Euclidean algorithm in the Gaussian integers.
4. Neukirch exercise I.1.3: Show that the integer solutions of the equation $x^2 + y^2 = z^2$ such that $x, y, z > 0$ and $\gcd(x, y, z) = 1$ are all given, up to a permutation of x and y, by the formulae
$$x = u^2 - v^2, \qquad y = 2uv, \qquad z = u^2 + v^2,$$
where $u, v \in \mathbb{Z}$, $u > v > 0$, $(u, v) = 1$, u, v not both odd.
5. Neukirch exercise I.1.7: Show that the ring $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ is euclidean. Show furthermore that its units are given by $\pm(1+\sqrt{2})^n$, $n \in \mathbb{Z}$, and determine its prime elements.
6. State and prove a formula for the number of ways to write a positive integer n as the sum of two squares, in terms of the prime factorization of n.

Exercises: Number Fields.
Please submit four of the following.

1. Find an integral basis of $\mathbb{Q}(\sqrt{D})$, for D squarefree. (Your answer should depend on D modulo 8.)
2. Neukirch exercise I.2.5: Show that $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$ is an integral basis of $\mathbb{Q}(\sqrt[3]{2})$.

3. Let $P(x)$ be a monic polynomial of degree n with integer coefficients, whose discriminant is squarefree. Prove that $1, x, \dots, x^{n-1}$ is an integral basis of $\mathbb{Q}[x]/(P(x))$.

4. Find a monic polynomial $P(x)$ of degree 3 whose discriminant is 4 times an odd squarefree number, but for which $1, x, x^2$ is an integral basis of $\mathbb{Q}[x]/(P(x))$. You may use the result of the previous exercise, and you may use a Magma program in lieu of doing computations by hand. (Hint: do so.)

5. For $n > 1$ an integer, prove that $2\cos(2\pi/n)$ and $2\sin(2\pi/n)$ are algebraic integers, but $\cos(2\pi/n)$ and $\sin(2\pi/n)$ are not. (Hint: recall that $e^{i\theta} = \cos\theta + i\sin\theta$. Also, remember that the product of all conjugates of an algebraic integer is a rational integer.)

6. Show that a root of a monic polynomial with algebraic integer coefficients is an algebraic integer.

Exercises: Interlude on Symmetric Functions.

The purpose of this set of exercises is to outline another method for proving basic closure properties of the sets of algebraic numbers and of algebraic integers, using symmetric functions. These functions are interesting in their own right, particularly to combinatorialists.

In terms of variables $x_1, \dots, x_n$, for $i = 1, \dots, n$, let $\sigma_i(x_1, \dots, x_n)$ be the polynomial consisting of the sum of all i-fold products of distinct x's. That is,

$$(t + x_1)\cdots(t + x_n) = t^n + \sum_{i=1}^{n} \sigma_i(x_1, \dots, x_n) t^{n-i}.$$

Please submit one of the following.

1. Prove that every symmetric polynomial with integer coefficients in $x_1, \dots, x_n$ (that is, every polynomial which remains the same after interchanging any two variables) is a polynomial in $\sigma_1, \dots, \sigma_n$ with integer coefficients. (Hint: order monomials $x_1^{e_1} \cdots x_n^{e_n}$ of a given total degree in lexicographic order, then use induction.)

2. Use the previous problem to prove that, if α and β are algebraic integers, so are $\alpha + \beta$ and $\alpha\beta$. (Hint: form the polynomials whose roots are $\alpha_i + \beta_j$ and $\alpha_i\beta_j$, respectively, for α_i a conjugate of α and β_j a conjugate of β.)