Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Lectures 2-3: Algebraic Numbers and Algebraic Integers
August 29 and 31, 2001

Addendum to Monday's lecture. To clarify the confusing point from the end of last time: we had a prime $p \equiv 1 \pmod 4$ and an integer a such that $a^2 + 1 \equiv 0 \pmod p$. We took $c + di = \gcd(a + i, p)$, noticed that $c^2 + d^2 = |c + di|^2$ divides p^2 and wanted to know that $c^2 + d^2$ was equal to p, not p^2. Two ways to see this:

1. (What I said in class.) Note that $|c+di|^2$ also divides $|a+i|^2$. If the latter is not divisible by p^2, great. If it is, repeat with a replaced by $a+p$, since $(a+p)^2+1 = (a^2+1)+p^2+2ap$ cannot also be divisible by p^2.

2. The fact that $c+di$ divides p is the same as saying that $p/(c+di) = p(c-di)/(c^2+d^2)$ belongs to $\mathbb{Z}[i]$. If $c^2+d^2 = p^2$, then this means $(c-di)/p$ is in $\mathbb{Z}[i]$, so c/p and d/p are integers. But then p divides $c+di$ and $c+di$ divides $a+i$, so p divides $a+i$, which it doesn't.

Strictly speaking, I should have also checked that $c^2 + d^2$ is not equal to 1, but I'll leave that to you. (Hint: for all α in the ideal generated by $a + i$ and p, $|\alpha|^2$ is a multiple of p.)

Reference. Neukirch, Section 1.2. (Warning: the book works in somewhat greater generality than I will work in class. But you should read it anyway.)

Jargon watch. A *principal ideal domain* is an integral domain (ring without zero divisors) in which each ideal is generated by some element. Examples: $\mathbb{Z}$, $K[x]$ for any field K, and (from Lecture 1) $\mathbb{Z}[i]$. Nonexample: $K[x, y]$, since the ideal (x, y) has no single generator.

The *discriminant* of a monic polynomial $P(x)$ with roots $r_1, \dots, r_n$ is defined as $\prod_{i<j}(r_i - r_j)^2$. This expression can be computed as a polynomial in the coefficients of P (this follows from the symmetric polynomials theorem on the problem set). It can also be computed by a built-in Magma function, as follows. (The first line creates a ring R of polynomials over the rationals with x as the variable. After that, Magma knows to interpret $x^3 + x + 1$ as an element of R.)

```
> R<x> := PolynomialRing(RationalField());
> Discriminant(x^3+x+1);
-31
```

Outline of lectures.

1. Define algebraic number, number field (and integral field extension).

2. Define algebraic integer, ring of integers (and integral closure).

3. Examples: roots of unity, $\cos(2\pi/n)$, $(1 + \sqrt{-3})/2$, $\sqrt{2} + \sqrt{3}$. Also a couple of nonexamples: e, π.

4. As an aside, mention Gelfond-Schneider theorem: if α, β are algebraic numbers and $\beta \notin \mathbb{Q}$, then α^β is not algebraic.

5. Explain linear algebraic proof that sum, product of algebraic numbers/integers is algebraic. Allude to symmetric functions proof (on homework).

6. Discuss minimal polynomial. Note that an algebraic number is integral if and only if its minimal polynomial is integral. Compute some examples.

7. Define trace, norm, trace pairing. Show that the trace pairing is nondegenerate for separable extensions. Define integral basis (absolute and relative).

8. Reinterpret trace and norm for Galois extensions.

9. Examples: quadratic fields, cyclotomic fields, the maximal real subfield of a cyclotomic field.

10. Define discriminant of a number field.