September 21:

Math 432 Class Lecture Notes

- Quadratic fields
- Units in real quadratic fields
- Primes

0.1 Quadratic fields

A quadratic number field F is an extension of $\mathbf{Q}$ of degree 2, If $F = \mathbf{Q}(\sqrt{d})$ and $d < 0$ then F is said to be **imaginary**, and if $d > 0$ then F is said to be **real**.

If u is an element of $\mathbf{Z}_F$ and $N(u) = \pm 1$ then u is clearly a unit. On the other hand, if $u \in \mathbf{Z}_F^*$ then $uv = 1$ for some $v \in \mathbf{Z}_F$, and $N(u)N(v) = 1$. The norm of an algebraic integer is an integer, so the only solution to this equation in the integers is $N(u) = \pm 1$.

Thus an element of Z_F is a unit if and only if its norm is a unit in $\mathbf{Z}$. (The same is true of an arbitrary number field.)

Let $F = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer. If $d \equiv 2, 3 \bmod 4$, then $\mathbf{Z}_F = \mathbf{Z}[\delta], \delta = \sqrt{d}$, and

$$N(a + b\delta) = a^2 - db^2.$$

Thus finding units comes down to solving the famous "Pell's equation."

If $d \equiv 1 \bmod 4$ then $\mathbf{Z}_F = \mathbf{Z}[\delta], \delta = (1 + \sqrt{d})/2$ and a simple calculation shows that

$$N(a + b\delta) = a^2 + ab + (1 - d)b^2/4,$$

Finding units in these fields comes down to solving the equation

$$= a^2 + ab + (1-d)b^2/4 = \pm 1,$$

though multiplying by 4 and completing the square shows that this is the same as the equation

$$(2a+b)^2 - db^2 = \pm 4,$$

so finding units comes down to solving a slightly generalized form of Pell's equation.

The discriminant of a quadratic field is defined to be $D = (\delta - \delta')^2$. If $d \equiv 2, 3 \bmod 4$, then $D = 4d$, and if $d \equiv 1 \bmod 4$ then $D = d$.

There are only finitely many units in an imaginary quadratic field. Indeed, if $D < -4$ then the only units are ± 1, then the formulas above for the norm can be used to show that the only solutions to $N(u) = \pm 1$ are $u = \pm 1$. If $D = -4$ then a simple calculation shows that the only units are $\pm 1, \pm i$, and if $D = -3$ then the 6 units correspond to the six solutions of the equation $a^2+ab+b^2 = 1$, i.e., are $\pm 1, \pm\omega, \pm\omega^2$ where $\omega = (-1+\sqrt{-3})/2$ is a primitive cube root of unity.

0.2 Units in real quadratic fields

The situation concerning units in real quadratic field (i.e., $d > 0$) is more interesting.

Theorem 1. There are infinitely many units in $\mathbf{Z}_F$ where F is a real quadratic field, and there is a "fundamental unit" u such that all units are of the form $\pm u^k$ for $k \in \mathbf{Z}$.

The theorem basically comes down to showing that there are nontrivial solutions to Pell's equation

$$x^2 - dy^2 = \pm 1.$$

Note that if u is fundamental then so are $-u, u^{-1}, -u^{-1}$.

Challenge: See if you can prove the theorem using only elementary arguments.

This is given as a very early exercise in Neukirch's tome on algebraic number theory and class field theory; it's not clear to me what is intended, since I don't know a truly elementary proof.

It is easy to check that if you find a single unit that is nontrivial (i.e., not equal to ±1) then it is of infinite order. If a nontrivial unit u is found, then it turns out to be fairly easy to find a fundamental unit. We'll solve this problem here (i.e., how to find a fundamental unit given any nontrivial unit) and leave the problem of finding a nontrivial unit until later in the course.

The key idea is contained in the following result (and its proof).

Lemma 2. If u is a unit that is larger than 1 then

$$u > \sqrt{D-3},$$

Remark 3. Note that if u is negative, then $-u$ is positive, and that if $0 < u < 1$ then $1 < u^{-1}$. So if we can find a nontrivial unit we can easily find one that is larger than 1.

Proof. If $u = a + b\delta$ then $u' - u = b(\delta - \delta')$ and

$$(u - u')^2 = b^2(\delta - \delta')^2 = b^2 D.$$

From $(u - u')^2 = u^2 - 2uu' + u'^2$ we get

$$u^2 = b^2 D - 2uu' + u'^2 > D - 3.$$

(Since $uu' = \pm 1$, and $u'^2 < 1$.) The result follows by taking the square root. □

Since $D \geq 5$ for read quadratic fields, the result is nontrivial in all cases. It is used in the following way. Suppose that u is a nontrivial unit that we've found. Without loss of generality (i.e., by negating and reciprocating as needed) we can assume that $u > 1$. Suppose that v is a fundamental unit (that we don't know). Then $u = v^k$ for some positive integer k. (In most practical situations, we hope for $k = 1$, i.e., we hope that we have already found the fundamental unit.)

From $v > B$ for $B = \sqrt{D-3}$ we get

$$u = v^k > B^k$$

which puts an *upper bound* on k. For instance, taking logarithms and dividing by $\log(B)$ gives

$$k < \frac{\log(u)}{\log(B)}.$$

In favorable situations the number on the right hand side will be less than 2 and we are done.

Example 4. If $d = 2$, $D = 8$, it doesn't take long to find the unit $u = 1+\sqrt{2}$. One finds that

$$\frac{\log(1+\sqrt{2})}{\log(\sqrt{5})}$$

is about 1.09 so u is fundamental.

Although it seems unlikely that anyone will confront a case in this course where the bound exceeds 2, what can be done if it does? One thing is just to show that u is not a k-th power in $\mathbf{Z}_F$ for all k that are less than B. Another is to search for fundamental units $a + b\delta$ for $b \leq r$; if none are found, then a review of the proof of the lemma shows that $D - 3$ can be replaced by $r^2 D - 3$, improving the lower bound considerably.

0.3 Primes

We know that the Gaussian ring $\mathbf{Z}[i]$, and the Eisenstein ring $\mathbf{Z}[\omega]$, $\omega = e^{2\pi i/3}$, are Euclidean rings, and therefore UFD's and PID's

What do the prime elements look like? Any prime P in either of these rings divides a rational integer (i.e., an element of $\mathbf{Z}$) since $N(P) = PP'$. So P must divide a unique rational prime p, and it suffices to factor rational primes.

In $\mathbf{Z}[i]$, one finds that 2 factors as $(1+i)(1-i)$, but that $1+i$ and $1-i$ are associates. Thus there is a unique prime $P = 1+i$ dividing 2 (up to associates), and 2 is an associate of P^2. If p is a rational prime congruent to 3 mod 4, then there are no elements of norm p since the equation

$$N(P) = N(a+bi) = a^2 + b^2 = p$$

is impossible (squares of integers are congruent to 0 or 1 mod 4). Thus in this case p itself is a prime in $\mathbf{Z}[i]$. The full story is:

Theorem 5. Up to associates, the primes in $\mathbf{Z}[i]$ are as follows:

- There is a unique prime $P = 1 + i$ dividing 2.
- For each rational prime $p \equiv 3 \bmod 4$, p is prime in $\mathbf{Z}[i]$.
- For each rational prime $p \equiv 1 \bmod 4$, there are two primes P, P', in $\mathbf{Z}[i]$ dividing p; they can be obtained by writing $p = a^2 + b^2$ as a sum of two squares and setting
$$P = a + bi, \qquad P' = a - bi.$$

Proof. The only real thing left to prove is that every prime that is 1 mod 4 can be written as a sum of two squares. There are fascinating algorithmic issues involved in actually doing this for large p, and one way to do it can be based on the Euclidean algorithm in $\mathbf{Z}[i]$.

Specifically, we first observe that -1 is a square modulo p. Indeed, in the cyclic group $(\mathbf{Z}/p\mathbf{Z})^*$ and element is a square if and only if $x^{(p-1)/2} = 1$. Since
$$(-1)^{(p-1)/2} \equiv (-1)^{\text{even}} \equiv 1 \bmod p$$
there is an integer a such that $a^2 \equiv -1 \bmod p$. Thus p divides $a^2 + 1$. One now checks that $a + i$ is a nontrivial gcd with p, but that it is not divisible by p, and that $P := \gcd(p, a + i)$ is an element of norm p, so that p is the sum of two squares. □

As an exercise, the reader should work out that in the Eisenstein field $\mathbf{Q}(\omega)$ the primes consist of a prime dividing 3 (whose square is an associate of 3), rational primes that are congruent to 2 modulo 3, and conjugate pairs of primes $a + b\omega$ that divide primes congruent to 1 modulo 3.

Of course, most number rings are *not* PID's, and the clean behavior above can not be replicated for numbers, though, as we will see, it can be replicated for "ideal numbers," i.e., ideals.

For instance, one checks that in the two factorizations of 6 in $\mathbf{Z}[\sqrt{-5}]$ given by
$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$
that all of the 4 factors are irreducibles, and no two are associates of each other. So unique factorization does *not* hold.