October 26:

Math 431 Class Lecture Notes

- The norm of an ideal
- Decomposition of primes
- The Minkowski bound

0.1 The norm of an ideal

If mul_α is the "multiplication by α" map on a number field F that contains α, then its determinant is, by definition, the norm of α down to $\mathbf{Q}$. In addition, the absolute value of the determinant is equal to the index of the ideal (α) in $\mathbf{Z}_F$. Indeed, if α_i is a basis of $\mathbf{Z}_F$ then $\alpha\alpha_i$ is a basis for (α), and the matrix for mul_α is the same as the change of basis matrix.

We extend this idea to arbitrary ideals, by defining the norm of an ideal to be its index.

Definition 1. If I is an ideal in a number ring $\mathbf{Z}_F$ then its norm is defined to be

$$N(I) = [\mathbf{Z}_F : I].$$

The remarks above show that the norm of a principal ideal is (the absolute value of) the norm of the generator:

$$N((\alpha)) = |N(\alpha)|\,.$$

The only other crucial property of the norm that we will need is that it is multiplicative, and this will require a little work.

Theorem 2. If I and J are ideals in $\mathbf{Z}_F$ then

$$N(IJ) = N(I)N(J).$$

Proof. From the Chinese Remainder Theorem, if $I = \prod P_i^{a_i}$ then $\mathbf{Z_F}/I = \bigoplus Z_{\mathbf{F}}/P_i^{a_i}$. Thus

$$N(I) = \prod N(P_i^{a_i}).$$

So the only fact that is needed to finish the proof of the theorem is that for any prime ideal

$$N(P^a) = N(P)^a.$$

Consider the decreasing sequence of ideals

$$\mathbf{Z_F} \supset P \supset P^2 \supset \cdots \supset P^a.$$

We claim that each quotient P^k/P^{k+1} is of order $N(P) = [\mathbf{Z}_F : P]$. First we note that P^k/P^{k+1} is a vector space over the reside field $\mathbf{Z}_F/I$; indeed if $x \in P^k$ and $[a] \in \mathbf{Z}_F/I$ then $[ax]$ is a well-defined element of P^k/P^{k+1} that depends only on the class of x mod P^{k+1} and the class of a in $\mathbf{Z}_F/I$. The vector space axioms are easy to verify.

So all that we have to show is that the quotient P^k/P^{k+1} is a 1-dimensional $\mathbf{Z}_F/P$ vector space. To this end, pick any $u \in P^k - P^{k+1}$. Therefore,

$$(u) = P^K J$$

for some ideal J. Then

$$(u) + P^{k+1} = \gcd((u), P^{k+1}) = P^K.$$

Thus the $\mathbf{Z}_F$ multiples of u cover P^k/P^{k+1} and the theorem is finally proven. □

0.2 Decomposition of primes

If P is a prime ideal in a number ring $\mathbf{Z}_F$ then P contains a unique rational prime p. The field $\mathbf{Z}_F/P$ is called the residue class field of P and is sometimes denoted k_P. A little thought shows that $\mathbf{Z}_F/P$ is an extension of the field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

Definition 3. The **residue class degree** of a prime ideal P, sometimes denoted f_P, is defined to be

$$f_P := [\mathbf{Z}_F/P : \mathbf{F}_p] .$$

Thus

$$|k_P| = p^{f_P}.$$

Theorem 4. If F is a number field of degree n, p is a rational prime, and the factorization of (p) into prime ideals in $\mathbf{Z}_F$ is

$$\prod P_i^{e_i}$$

then

$$\sum e_i f_i = n$$

where f_i is the residue class degree of the prime P_i.

From now on, we will often say "the factorization of p" when "the factorization of $(p) := p\mathbf{Z}_F$ into prime ideals" is meant.

Proof. By multiplicativity of the norm, if

$$(p) = \prod P_i^{e_i}$$

then

$$N(p) = p^n = \prod_i N(P_i))^{e_i} = p^{\sum e_i f_i}$$

and the result follows by the definition of the norm. □

Definition 5. If $(p) = \prod P_i^{e_i}$ then the exponent e_i is called the **ramification index** of the prime P_i. The prime p is said to be **ramified** in $K/\mathbf{Q}$ if some exponent e_i is larger than 1.

It turns out that only finitely many primes can be ramified.

Theorem 6. The prime p is ramified in F if and only if p divides the discriminant.

The proof of this theorem is somewhat difficult (though one direction is easier than the other), and will be deferred to when (and if) we return to the constructive aspects of the problem of finding $\mathbf{Z}_F$.

Example 7. The discriminant of $f(x) = x^3 + x + 1$ is -31. Therefore if α is a root of f and $F = \mathbf{Q}(\alpha)$ then $\mathbf{Z}_F = \mathbf{Z}[\alpha]$. By the above theorem, 31 is the only ramified prime and it can be verified that

$$(31) = P^2 Q$$

where $P = (31, \alpha - 14)$, $Q = (31, \alpha - 3)$.

In a cubic field there are two possible factorizations for ramified primes

$$(p) = P^2 Q, \quad (p) = P^3$$

where all primes are of residue class degree 1. There are three possible factorizations of unramified primes

$$(p) = P_1 P_2 P_3, \quad (p) = PQ, \quad (p) = R$$

corresponding to the three different partitions of 3.

Example 8. In $\mathbf{Z}[i]$ there are three types of primes:

$$\begin{aligned} (2) &= P^2, & P &= (1+i), e_P = 2, f_P = 1 \\ (p) &= PP', & P &= (a+bi), e_P = f_P = 1 \\ (p) &= Q, & e_Q &= 1, f_Q = 2 \end{aligned}$$

In favorable circumstances (true in any event for all but finitely many primes) the decomposition of a rational prime p in $\mathbf{Q}(\alpha)$ can be detected from the factorization of m_α modulo p.

Theorem 9. Suppose that $F = \mathbf{Q}(\alpha)$ is a number field, where α is an algebraic integer. If p is a rational prime and the index $[\mathbf{Z}_F : \mathbf{Z}[\alpha]]$ is prime to p, then the factorization of the ideal (p) exactly mirrors the factorization of the polynomial m_α modulo p. More precisely. if

$$\mathrm{m}_\alpha \equiv \prod f_i^{e_i} \bmod p$$

where the f_i are distinct monic irreducible polynomials in $\mathbf{F}_p[x]$ then

$$(p) = \prod P_i^{e_i}$$

where $P_i = (p, f_i(\alpha))$ are prime ideals of residue class degree $\deg(f_i)$.

This will be proved next time.

0.3 The Minkowski Bound

Later we will prove the following result, using the geometry of numbers.

Theorem 10. (Minkowski Bound) Let F be a number field with discriminant D_F and degree n over $\mathbf{Q}$. Then every ideal I in $\mathbf{Z}_F$ contains an element α such that

$$|N(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|D_F|} N(I).$$

The idea of the proof is to embed the integers $\mathbf{Z}_F$ into $\mathbf{R}^n$ as a lattice, and use the fact that every sufficiently large sphere has two contain two points of a lattice.

Recall the the ideal class group $\mathrm{Cl}(F)$ is the set of equivalence classes of ideals under the relation $I \sim J$ when there are elements α and β of $\mathbf{Z}_F$ such that

$$\alpha I = \beta J.$$

Alternatively, the ideal class group can be more simply described as the quotient

$$\frac{\text{fractional ideals}}{\text{principal fractional ideals}}$$

where a fractional ideal is a Z_F submodule of F of rank n. One shows that fractional ideals can be represented in the form

$$\prod P_i^{a_i}$$

where the exponents are arbitrary integers (positive, zero, or negative). And the "principal ideals" in the denominator refer to principal ideals of elements of F. (If x is in F, then $x = a/b$ where $a, b \in \mathbf{Z}_F$, and $(x) = (a)(b)^{-1}$.)

The most important theorem about the class group is that it is finite.

Theorem 11. Cl_F is finite.

In addition, the group is trivial if and only if the ring of integers is a PID, which is in turn equivalent to being a UFD.

Theorem 12. The following are equivalent:

- The group $\mathrm{Cl}(F)$ is trivial.
- $\mathbf{Z}_F$ is a PID.
- $\mathbf{Z}_F$ is a UFD.