October 29:

Math 431 Class Lecture Notes

- Finiteness of the class group
- Computing a class group
- The Minkowski bound

0.1 Finiteness of the class group

The Minkowski bound says that every ideal I in a number ring $\mathbf{Z}_F$ contains an element α such that

$$|N(\alpha)| \leq C_F N(I)$$

where C_F depends only on the signature (r_1, r_2), degree n, and discriminant D_F of F:

$$C_F = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|D_F|}.$$

It is an interesting exercise to show that

$$N(I) = \gcd(\{|N(\alpha)| \ : \alpha \in I\}).$$

Thus the term $C_F\sqrt{|D_F|}$ measures how far off we can be in comparing $N(I)$ with the smallest possible $N(\alpha)$, for $\alpha \in I$. If the class group is trivial then of course one can find α with $|N(\alpha)| = N(I)$. Thus it is plausible that this result says something about the class group.

Theorem 1. The class group $\mathrm{Cl}(F)$ of a number field is finite.

Proof. We show that any class contains an ideal of norm at most C_F. To see this, let I be an ideal in $\mathbf{Z}_F$, and denote its class by $[I]$. Then I is invertible so there is an ideal I' such that $II' = (\beta)$ for some β. Now apply the Minkowski bound to I' to obtain an element α such that

$$|N(\alpha)| \leq C_F \cdot N(I).$$

Since $(\alpha) \subset I'$, $(\alpha) = I'J$ for some J. This implies that $I(\alpha) = II'J = (\beta)J$. Thus I and J are in the same ideal class. However

$$N(J) = \frac{N((\alpha))}{N(I')} = \frac{|N(\alpha)|}{N(I')} \leq C_F.$$

There are finitely many rational primes less than $N(J)$, and hence finitely many prime ideals P in $\mathbf{Z}_F$ of norm less than a given bound, and hence finitely many ideals of norm less than $C_F\sqrt{|D|}$. Since every ideal class has a representative in a finite set, the ideal class group is finite. □

0.2 Computing a class group

Let $F = \mathbf{Q}(\sqrt{-15})$. Then we know that $\mathbf{Z}_F = \mathbf{Z}[\delta]$ where $\delta = (1+\sqrt{-15})/2$, $D_F = -15$, and $N(x + y\delta) = x^2 + xy + 4y^2$. From the proof of the finiteness of the class number using the Minkowski bound we know that every ideal class contains an ideal of norm at most

$$\frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{15} < 4.$$

It turns out that class groups can be computed by computing sufficiently many norms, and then drawing suitable inferences!

So we start by computing $N(x + \delta) = x^2 + x + 4$ for $0 \leq x < 12$. (Since $N(-x + \delta) = N(x - 1 - \delta)$ it is unnecessary to compute this function for negative x.)

x	x^2+x+4	$(x+\delta)$
0	$4 = 2^2$	P_2^2
1	$6 = 2 \cdot 3$	$P_2' P_3$
2	$10 = 2 \cdot 5$	$P_2 P_5$
3	$16 = 2^4$	$P_2'^4$
4	$24 = 2^3 \cdot 3$	$P_2^3 P_3$
5	$34 = 2 \cdot 17$	$P_2' P_{17}$
6	$46 = 2 \cdot 23$	$P_2 P_{23}$
7	$60 = 2^2 \cdot 3 \cdot 5$	$P_2'^2 P_3 P_5$
8	$74 = 2 \cdot 37$	$P_2 P_{37}$
9	$94 \cdot 47$	$P_2' P_{47}$
10	$114 = 2 \cdot 3 \cdot 19$	$P_2 P_3 P_{19}$
11	$119 = 2^3 \cdot 17$	$P_2'^3 P_{17}'$
12	$160 = 2^5 \cdot 5$	$P_2^5 P_5$

After computing the norm we factor the resulting integer; the idea is that this gives us lots of information about the factorization of the principal ideal $(x+\delta)$ into prime ideals.

For instance, the factorization $N(2+\delta) = 6 = 2 \cdot 3$ tells us that the factorization of the principal ideal $(2+\delta)$ must involve a prime ideal of norm 2 and a prime ideal of norm 3.

If P is a prime ideal of degree 1 lying over a rational prime p, then the residue field $\mathbf{Z}_F/P$ is equal to $\mathbf{Z}/p\mathbf{Z}$, and δ is congruent to an integer modulo P. If $\delta \equiv a \bmod P$ then $N(a-\delta)$ is divisible by p. Thus any prime of degree 1 "occurs" sooner or later in the factorization table above.

On the other hand, $\delta \bmod P$ generates $\mathbf{Z}_F/P$ as an extension of $\mathbf{Z}/p\mathbf{Z}$, so if $\delta \equiv a \bmod P$ then this extension is of degree 1. Thus a rational prime occurs in a factorization of $(x+\delta)$ if and only if the corresponding prime ideal is of degree 1.

(Warning: this relies on the fact that the ring of integers has a power basis, i.e., that $\mathbf{Z}_F = \mathbf{Z}[\delta]$, so in fields of higher degree this sort of argument might not hold for primes dividing the index of $\mathbf{Z}[\alpha]$ in $\mathbf{Z}_F$.)

Next, we note that a prime ideal P occurs in the factorization of $(x+\delta)$ and $(x'+\delta)$ if and only if $x \equiv x' \bmod p$. Indeed, if $x+\delta \in P$ and $x'+\delta \in P$ then

$$x + \delta - x' - \delta = x - x' \in P \cap \mathbf{Z} = (p).$$

These remarks enables us to make many inferences from the table of norms. First, 2 splits, 3 and 5 are ramified, and 7 is inert. Next, we can factor each principal ideal into prime ideals as indicated.

What do the factorizations tell us about the class group? From the equations

$$(2) = P_2 P_2', \ (3) = P_3^2, \ (5) = P_5^2$$

we see that the primes P_2 and P_2' are inverses in the class group, and that the classes of P_3 and P_5 have order 2. From the factorization $(1+\delta) = P_2' P_3$, $(2+\delta) = P_2 P_5$ we see that P_2 and P_2' have order 2 (so that $[P_2] = [P_2']$ and that $[P_3] = [P_2] = [P_5]$. In fact, the only class groups that are consistent with all of the above information are: the trivial group (every ideal is principal), or the group of order 2, in which, for instance, $[P_2]$ is the nontrivial element.

Morally speaking, we are sure that the latter is probably true. To verify this, it suffices to show that P_2 is nontrivial. If P_2 were principal, say $P_2 = (x + y\delta)$, then there would be an element of order 2:

$$N(x + y\delta) = x^2 + xy + 4y^2 = N(P_2) = 2.$$

This equation is unsolvable in integers x, y (e.g., implies $(2x+y)^2 + 15y^2 = 8$). So we conclude that $Cl(F)$ is of order 2.