October 31:

Math 431 Class Lecture Notes

- The class group of $\mathbf{Q}(\sqrt{-14})$
- The class group of $\mathbf{Q}(\sqrt{70})$

0.1 The class group of $\mathbf{Q}(\sqrt{-14})$

Let $F = \mathbf{Q}(\sqrt{-14})$. Then $\mathbf{Z}_F = \mathbf{Z}[\sqrt{-14}]$ since $-14 \equiv 2 \bmod 4$. This means that if $x + y\sqrt{-14} \in F$ then $N(x + y\sqrt{-14}) = x^2 + 14y^2$. To find the prime ideals of degree one (prime ideals such that $\mathbf{Z}_F/P \cong \mathbf{Z}/p\mathbf{Z}$) we will check the following table where we have set $y = 1$.

x	$x^2 + 14$	prime ideals
0	$14 = 2 \cdot 7$	P_2P_7
1	$15 = 3 \cdot 5$	P_3P_5
2	$18 = 2 \cdot 3^2$	$P_2(P_3')^2$
3	$23 = 23$	P_23
4	$30 = 2 \cdot 3 \cdot 5$	$P_2P_3P_5'$
5	$39 = 3 \cdot 13$	$P_3'P_{13}$
6	$50 = 2 \cdot 5^2$	$P_2(P_5)^2$
7	$63 = 3^2 \cdot 7$	$(P_3)^2P_7$

Since we can calculate the Minkowski bound to be

$$B = \frac{2}{\pi}\sqrt{|D_F|} = \frac{2}{\pi}\sqrt{56} < 6$$

we know that our class group is generated by the ideals lying over primes below six. Thus the above table might be sufficient to determine the class group.

How were the prime ideal factorizations obtained? Given our prime factorization of a given ideal's norm, we have a factorization of that ideal into prime ideals lying over those primes. This leaves the question of when those primes are the same and when they are conjugates. For example, if we have a factor of 7 in the norm of our ideal, should this be represented by P_7 or P_7'? Let our ideal in this list be $I = (m + \delta)$ since we have $y = 1$. We know that for any prime ideal, P, $\mathbf{Z}_F/P \cong \mathbf{Z}/p\mathbf{Z}$, so in P we can work mod p where p is the prime underlying our prime ideal P. Thus we know that $\delta \equiv m \bmod p$. Thus for any prime $p \in \mathbf{Z}$ if p appears in the factorization of principal ideals generated by two numbers which are not equivalent modulo p we would get $1 \in P$ which is clearly impossible. Thus if p appears only once in the factorization of the norms of the principal ideals (δ), $(1+\delta)$, ..., $(p-1+\delta)$ we know that p splits in $\mathbf{Z}_F$ or $(p) = P_p^2$. If it appears twice, then we have $(p) = P_pP_p'$. If p fails to appear at all, we know that p is inert in $\mathbf{Z}_F$.

From the above table, we now know that $(2) = P_2^2$, $(3) = P_3P_3'$, and $(5) = P_5P_5'$. Since principal ideals are trivial in the class group, this table also gives us relations between these prime ideals, namely $P_3P_5 \equiv P_2(P_3')^2 \equiv P_2P_3P_5 \equiv P_2P_5^2 \equiv 1$. We can derive from these relations that $P_3^2 \equiv P_2$, $P_3^4 \equiv 1$, $P_3^3 \equiv P_5$. Therefore our conjecture is that the class group is generated by the class $[P_3]$, and that that element has order 4; in terms of generators and relations used in finite group theory one might write

$$\mathrm{Cl}(F) =< a : a^4 = 1 >, \quad a = [P_3].$$

This is true unless P_2 is trivial. Suppose that $(a+b\delta) = P_2$. Then $N(a+b\delta) = 2 = a^2 + 14b^2$ which is clearly impossible in the integers. Thus we have $Cl_F \cong \mathbf{Z}/4\mathbf{Z}$.

0.2 The class group of $\mathbf{Q}(\sqrt{70})$

Now let $F = \mathbf{Q}(\sqrt{70})$. In this case, the Minkowski bound is $B = \frac{2}{pi}\sqrt{280} < 17$. Thus we need only look at primes below 17. Here, letting $y = 1$ we get the following table of norms. (Any norm which contains a prime larger than 13 will be disregarded and not factored.)

x	$x^2 - 70$	Prime ideals
0	-70	$P_2P_5P_7$
1	-69	
2	-66	$P_2P_3P_11$
3	-61	
4	-54	$P_2(P_3')^3$
5	-45	$P_3^2P_5$
6	-34	
7	-21	$P_3'P_7$
8	-6	P_2P_3
9	11	$P_1'1$
10	30	$P_2P_3'P_5$
11	51	
12	74	
13	99	$(P_3')^2P_11$

Here we can observe that 2, 5, and 7 ramify, 3 and 11 split and nothing is inert. Thus we have $P_2^2 \equiv P_5^2 \equiv P_7^2 \equiv 1$. However from the relations given by the table we discover that $P_2 \equiv P_3 \equiv P_3' \equiv P_7$ and also that $P_5 \equiv 1$. Thus our class group is

$$Cl_F =< [P_2] : P_2^2 = 1 >$$

unless P_2 is trivial. Suppose that there is some $(a+b\delta) = P_2$. Then $a^2-70b^2 = 2$, which looked at mod 5 tells us that in $\mathbf{Z}/5\mathbf{Z}$ 5 is a square. Since this is not true, we have $Cl_F \cong \mathbf{Z}/2\mathbf{Z}$.