November 12:

Math 431 Class Lecture Notes

- ## 0.1 The class number of $\mathbf{Q}(\sqrt[3]{6})$

- Finding the ring of integers
- Finding the class number of a cubic field

0.2 The class number of $\mathbf{Q}(\sqrt[3]{6})$

In discussing the infamous group quiz, it was determined that there was a typo in the second problem, and the the problem on the class number of $\mathbf{Q}(\sqrt[3]{6})$ should perhaps have included a hint about the ring of integers. (Later, it was also revealed that the peaceful drunken rooks puzzle actually was well-posed, and that the puzzle is available commercially.)

Let $F = \mathbf{Q}(\sqrt[3]{6})$. Then, for $\alpha = \sqrt[3]{6}$, $m_\alpha = f$, and $f = x^3 - 6$, we know that $\mathrm{disc}(f) = \mathrm{disc}(1, \alpha, \alpha^2) = [\mathbf{Z}_F : \mathbf{Z}[\alpha]]^2 \cdot D_F$. From the formula for the discriminant of a cubic we also know $\mathrm{disc}(1, \alpha, \alpha^2) = -27 \cdot 6^2 = -3^5 \cdot 2^2$.

Therefore $\mathbf{Z}[\alpha]$ is of index $1, 2, 3, 6, 9, 18$ in $\mathbf{Z}_F$ (all of the integers whose square divides the discriminant). In fact, $\mathbf{Z}_F = \mathbf{Z}[\alpha]$ but to prove this gracefully it is easiest to use results on algebraic integers.

0.3 Finding the ring of integers

Let R be a ring such that

$$\mathbf{Z}[\alpha] \subset R \subset \mathbf{Z}_F.$$

The basic idea is to start with $R = \mathbf{Z}[\alpha]$ and gradually enlarge R until we (provably) have reached $\mathbf{Z}_F$. The tools needed to do this are loosely summarized as follows.

Theorem 1. a) the primes of $\mathbf{Z}[\alpha]$ are of the form $P = (p, g(\alpha))$, where $g \in \mathbf{F}_p[x]$ is irreducible and $g \mid f \bmod p$).

b) If P is a prime ideal in R then there is an $x \in F - R$ such that $xP \subset R$.

c) The question of whether or not $xP \subset P$ is true is independent of which x is chosen in part b).

d) If $xP \subset P$ then x is an algebraic integer, and R can be enlarged, and the prime ideals can be recomputed.

e) If xP is not a subset of P, then we say that x is a "certificate of invertibility" for P. If all prime ideals in R have certificates of invertibility then $R = \mathbf{Z}_F$.

The only prime ideals that are not invertible are those lying over primes p such that p^2 divides the discriminant of α. Thus there are finitely many prime ideals in play at any given time, and since the discriminant of R goes down every time it is enlarged, the algorithm implicit in the above results clearly terminates.

In the example of current we start with let $R = \mathbf{Z}[\alpha]$, where $\alpha = \sqrt[3]{6}$. Then we only have to worry about $p = 2$ and $p = 3$ and the only prime ideals above those primes are $P_2 = (2, \alpha)$ and $P_3 = (3, \alpha)$. We want to find certificates of invertibility for those ideals; if we fail then we can enlarge R.

Consider P_2. We need $2x$ and αx to be in R. The former implies that $x = y/2$, where $y = A + B\alpha + C\alpha^2$. From

$$y\alpha = 6C + A\alpha + B\alpha^2$$

we see that $x = \alpha^2/2$ works just fine. Then $x\alpha = 3 \notin P_2$ so x is a certificate of invertibility of P_2.

Similar arguments show that for P_3 we can also use $x = \alpha^2/3$, and that xP_3 is not contained in P_3. Thus P_3 is invertible as well, and we conclude that $\mathbf{Z}[\alpha] = \mathbf{Z}[\sqrt[3]{6}$ is the full ring of integers $\mathbf{Z}_F$.

0.4 Finding the class number of a cubic field

Now we can return to our regularly scheduled program of computing the class group. We know that

$$N(\alpha - x) = -f(x)$$

for integers x, and this enables us to compute a table of norms.

x	$x^2 - 6$	prime ideals
0	-6 $= -2 \cdot 3$	P_2P_3
1	-5 $= -5$	P_5
2	2 $= 2$	P_2
3	21 $= 3 \cdot 7$	P_3P_7
-1	-7 $= -7$	P_7'
-2	-14 $= -2 \cdot 7$	P_2P_7''

We can calculate the Minkowski bound to be

$$B = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|D_F|} = \frac{6}{3^3}\left(\frac{4}{\pi}\right)\sqrt{3^5 \cdot 2^2} < 9$$

so we know that every element of the class group contains an ideal of norm less than 9, and, in particular, that the class group is generated by prime ideals of norm less than 9.

By the above table,

$$(7) = P_7P_7'P"_7, \quad (5) = P_5Q_5, \quad (3) = P_3^3, \quad (2) = P_2^3.$$

By the $x = -1$ table entry, we know that one of the P_7's is principal. Similarly, we know that P_2 and P_5 are principal (by the $x = 2$ and $x = 1$ entries). So, P_3 is principal (by $x = 0$), and consequently, both of the other P_7's are principal. Therefore, $h = 1$ and we have a PID.

Note that in fact, we did not have to use the result from the previous section about the ring of integers. Namely, the norm calculations are valid no matter what the ring of integers actually is; e.g., if an element has prime norm then it generates a prime ideal of degree 1 in $\mathbf{Z}_F$; finally, since we found that the class number was 1, we didn't have to prove that any ideals were non-principal and didn't need to fully calculate the "norm form."

We also remark that the norm table could be used to find a nontrivial unit, by finding a principal ideal that was trivial, as a principal ideal. A famous theorem due to Dirichlet that we will cover next week says that the units of a number field F consist of roots of unity, together with s independent elements, where $s = r_1 + r_2 - 1$, i.e.,

$$\mathbf{Z}_F^* \simeq U \times \mathbf{Z}^s$$

where U is a finite group. For the cubic field above, $r_1 + r_2 - 1 = 1$ and there is a "fundamental unit" of infinite order, much as in the case of real quadratic fields.