Math 531 Tom Tucker
NOTES FROM CLASS 12/01

We were in the middle of computing the class group of the ring

\[ B = \mathbb{Z}[\sqrt[3]{11}] \]

We’ll denote \( \sqrt[3]{11} \) as \( \theta \).

Our Minkowski constant is

\[ \frac{3!}{3^3 \pi} \sqrt{3^3 11^2} < 17 \]

so we only have to check up to 17.

We found that all the primes in \( B \) lying over 3, 7, 11, and 13 were principal. Over 2, we obtained

\[ x^3 - 11 \equiv x^3 - 1 \equiv (x - 1)(x^2 + x + 1) \pmod{2} \]

so our primes are \((2, \theta - 1)\), which we’ll call \( \mathcal{P}_1 \), and \((2, \theta^2 + \theta + 1)\), which we’ll call \( \mathcal{P}_2 \).

Over 5, we get the same factorization

\[ x^3 - 11 \equiv x^3 - 1 \equiv (x - 1)(x^2 + x + 1) \pmod{5} \]

so our primes are \((5, \theta - 1)\), which we’ll call \( \mathcal{Q}_1 \), and \((5, \theta^2 + \theta + 1)\), which we’ll call \( \mathcal{Q}_2 \).

So we only have 4 primes to look at. Moreover \([\mathcal{P}_1] = [\mathcal{P}_2]^{-1}\) and \([\mathcal{Q}_1] = [\mathcal{Q}_2]^{-1}\), so the class group is generated by \([\mathcal{P}_2]\) and \([\mathcal{Q}_2]\). Let’s see if we can whittle it down a little more: we see that \( N(\mathcal{Q}_2) \) exceeds the Minkowski bound, so is in the group generated by \([\mathcal{P}_1], [\mathcal{Q}_1], [\mathcal{Q}_2]\).

Now, let’s look at the product \( \mathcal{Q}_1 \mathcal{P}_1 \). We see that the norm of this ideal is 10. Since \( N(\theta - 1) = 10 \), this ideal must be principal, since it is the only ideal with norm 10 in \( B \). Thus, \( \text{Cl}(B) \) is generated by \( \mathcal{P}_1 \).

Recall that we have \( \mathcal{P}_1 \mathcal{P}_2 = 2 \) and \( N(\mathcal{P}_1) = 2 \), \( N(\mathcal{P}_2) = 4 \). There is in fact an element with norm 4. We know that \( \theta^2 \) satisfies \((\theta^2)^3 - 11^2 = 0\), so for any \( a \in \mathbb{Z} \), we have \( N(a - \theta) = a^3 - 11^2 \). Thus, \( N(5 - \theta^2) = 4 \). Thus \( (5 - \theta^2)B \) is either \( \mathcal{P}_1^2 \) or \( \mathcal{P}_2 \). If it is equal to \( \mathcal{P}_2 \), then we are done. We now that that \( \mathcal{P}_1 \mathcal{P}_2 = 2 \), so if \((5 - \theta^2)B = \mathcal{P}_1 \), then \( 2/(5 - \theta^2) \) generates \( \mathcal{P}_1 \) and in particular \( 2/(5 - \theta^2) \in B \). To check whether or not \( 2/(5 - \theta^2) \) is in \( B \), we write out the matrix representing multiplication by \( 2/(5 - \theta^2) \) on \( 1, \theta, \theta^2 \). We end up with

\[
\begin{pmatrix}
1 & 25 & 11 & 5 \\
2 & 55 & 25 & 11 \\
121 & 55 & 25
\end{pmatrix}
\]

The entries aren’t integers, so \( 2/(5 - \theta^2) \) can’t be in \( B \) (actually we knew this as soon as we hit one noninteger entry). So we must have
2/(5 − θ^2) generates \( \mathcal{P}_1^2 \). If \( \mathcal{P}_1 \) is principal, with generator, say, \( \alpha \), then \( \alpha^2 = u(\theta^2 - 5) \) for some unit \( u \in B \). It turns out that \( v = 1 + 4\theta - 2\theta^2 \) is fundamental unit for \( B \), so every unit can be written as \( \pm v^d \) for some \( d \). In particular, the unit \( u \) can be written this way. It follows that for either \( \delta = 1 \) or \( \delta = 0 \), the element

\[ \pm v^\delta(\theta^2 - 5) \]

is a square in \( B \). We will show that this cannot be the case. If \( \pm v^\delta(\theta^2 - 5) \) is a square in \( B \), then it must be a square modulo any ideal of \( B \). In particular, we must have

\[ \pm v^\delta(\theta^2 - 5) \equiv \text{(square)} \pmod{\theta - 2}. \]

Modding out by \( \theta - 2 \) is the same as setting \( \theta \) equal to 2 which gives us \( \pm v^d \) in

\[ B/(\theta - 2) \equiv \mathbb{Z}/3\mathbb{Z} \]

this is only possible if \( \pm \) is actually \(-\). Let’s try modding out by something else. How about by \( \theta + 3 \). In this case we end up with

\[ -v^\delta(\theta^2 - 5) \equiv -(1 + 4(-3)2(-3)^2)((-3)^2 - 5) \equiv -(9)^4 \pmod{\theta + 3} \]

Since \( N(\theta + 3) = 10 \), we see that \( B/(\theta + 3) \) must be

\[ \mathbb{Z}/19\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \]

so we see that \( -(9)^4 \) must be a square modulo 19. This is impossible since \(-1\) is not a square mod 10 and we are done.

Thus, \( Cl(B) \equiv \mathbb{Z}/2\mathbb{Z} \).

*****Completions

Recall that we were able prove finiteness of the class group and the Dirichlet unit theorem by embedding number fields into \( \mathbb{C} \) and \( \mathbb{R} \), in other words taking advantage of completions of the fields. It turns out we can do a similar thing at every prime \( \mathcal{P} \) of a number field. First, a definition

**Definition 37.1.** Let \( K \) be any field. An absolute value \( | \cdot | \) on \( K \) is function \( | \cdot | : K \rightarrow \mathbb{R} \) such that

1. \( |x| \geq 0 \) for every \( x \in K \) and \( |x| = 0 \) if and only if \( x = 0 \).
2. \( |xy| = |x||y| \) for every \( x, y \in K \).
3. (Triangle inequality) \( |x + y| \leq |x| + |y| \).

The book does not assume that an absolute value satisfies the triangle inequality. Here are some examples of the absolute values.
Example 37.2.  

1. Any embedding $\sigma : K \rightarrow \mathbb{C}$ induces an absolute value on $K$ by restricting the usual absolute value on $\mathbb{C}$ to $\sigma(K)$.

2. Any valuation $v$ (I’ll recall what one is) on $K$ induces an absolute value by setting $|x| = e^{-v(x)}$ for $x \neq 0$ and $|x| = 0$.

Two absolute values $| \cdot |_1$ an $| \cdot |_2$ are said to be equivalent if there exist constants $C_1$ and $C_2$ such that

$$|x|_1^{C_1} \leq |x|_2 \leq |x|_2^{C_2}.$$ 

For example if in 3. above we take $v$ to be the $p$-adic valuation on $\mathbb{Q}$, then $|x| = e^{-v(x)}$ and $|x| = p^{-v(x)}$ are equivalent.

Given an absolute value on a field, we can complete the field, with Cauchy sequences, and obtain a new field that is complete with respect to this absolute value. For example, when we complete $\mathbb{Q}$ at the usual absolute value (called a real absolute value), we obtain $\mathbb{R}$. Let’s try to remember how this went. From now on $| \cdot |$ is an absolute value satisfying 1., 2., 3. above.

Definition 37.3. A Cauchy sequence is a sequence $(x_i)_{i=1}^{\infty}$ of $x_i \in K$ with the property that for any $\epsilon > 0$ there exists $N_\epsilon$ such that for any $m, n > N_\epsilon$ $|x_m - x_n| < \epsilon$.

We define the completion $\hat{K}$ of $K$ for the absolute value $| \cdot |$ on $K$ to be the set of all Cauchy sequences on $K$ modulo the equivalence relation

$$(x_i)_{i=1}^{\infty} \sim (y_i)_{i=1}^{\infty}$$

if, for every $\epsilon > 0$ there exists $N_\epsilon$ such for all $n > \epsilon$, we have $|x_n - y_n| < \epsilon$.

The field $K$ embeds into $\hat{K}$ via constant sequences. We identify $a \in K$ with the Cauchy sequence $a, a, \ldots, a, \ldots$.

You’ve all seen this, so I’ll skip the details.

We see that $\hat{K}$ is a field. As mentioned earlier, $\mathbb{R}$ and $\mathbb{C}$ can be obtained in this way. When $|x|_p = e^{-v_p(x)}$ for $x \in \mathbb{Q}^*$, and we complete, we end up with something called the $p$-adic numbers, denoted at $\mathbb{Q}_p$.

Theorem 37.4 (Ostrowski). Every absolute value on $\mathbb{Q}$ is equivalent to the usual absolute value $| \cdot |$ or one of the $p$-adic absolute values $| \cdot |_p$.

We won’t prove this (or use it).