Math 531 Tom Tucker
NOTES FROM CLASS 11/15

Theorem 31.1. *Let $I \subset \mathcal{O}_L$ be any fractional ideal of $\mathcal{O}_L$. Then there exists an ideal $J \subset \mathcal{O}_L$ in the same ideal class as I such that*

$$|\,\mathrm{N}_{L/\mathbb{Q}}(J))| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \mathrm{N}_{L/\mathbb{Q}}(I)\sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}.$$

Proof. Applying the previous theorem to I^{-1}, we find that there is an element $a \in I^{-1}$ such that

$$|\,\mathrm{N}_{L/\mathbb{Q}}(a)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\mathrm{N}(I)^{-1}.$$

Let $J = aI$. Since $a \in I^{-1}$, we see that

$$aI = a(I^{-1})^{-1} \subset \mathcal{O}_L.$$

We also have

$$\mathrm{N}(aI) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\mathrm{N}(I)^{-1}N(I) = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})},$$

so we are done. □

Corollary 31.2. $|\,\mathrm{Cl}(\mathcal{O}_L)|$ *is finite.*

Proof. There are finitely many ideals in $\mathcal{O}_L$ of bounded norm. □

Example 31.3. $|\,\mathrm{Cl}(\mathbb{Z}[\sqrt{-13}])| = 2$. We check the Minkowski bound and find it to be smaller than 5:

$$(1/2)(4/\pi)2\sqrt{13} < 5.$$

So we only need to check at 2 and 3. Let's see what happens at 2:

$$x^2 + 13 \equiv x^2 + 1 \pmod 2 \equiv (x+1)^2 \pmod 2.$$

Let $\mathcal{P} = (\sqrt{-13} + 1, 2)$. I claim it isn't principal. To start with, we see that 2 is irreducible in $\mathbb{Z}[\sqrt{-13}]$. If it weren't irreducible, we could write $xy = 2$ with x, y not units. Let N denote $\mathrm{N}_{\mathbb{Q}(\sqrt{-13})/\mathbb{Q}}$. This would mean that $\mathrm{N}(x)\,\mathrm{N}(y) = \mathrm{N}(2) = 4$. Since x and y are not units, we cannot have $\mathrm{N}(x)$ or $\mathrm{N}(y)$ equal to 2. But there are no a and b with $a^2 + 13b^2 = 2$, so this is impossible. Thus, the only possible generator for the ideal $\mathcal{P}$ is 2. But $2 \nmid (\sqrt{-13} + 1)$, so 2 cannot generate this ideal. In fact, we already know that $\mathcal{P}^2 = 2$, so 2 cannot generate this ideal. Hence $[\mathcal{P}] \neq 1$, where $[\mathcal{P}]$ is the ideal class of $\mathcal{P}$. Since $\mathcal{P}^2 = (2)$, we know that $[\mathcal{P}]^2 = 1$.

Let's look over 3 now:

$$x^2 + 13 \equiv x^2 + 1 \pmod 3$$

which is irreducible, so $3\mathbb{Z}[\sqrt{-13}]$ is the only prime lying over 3. Thus, $\mathrm{Cl}(\mathbb{Z}[\sqrt{-13}])$ is generated by $[\mathcal{P}]$ above and thus has order 2.

Example 31.4.

$$|\operatorname{Cl}(\mathbb{Z}[\frac{1+\sqrt{-35}}{2}])| = 2$$

Let

$$\omega = \frac{1+\sqrt{-35}}{2}.$$

Then ω has minimal polynomial $x^2 - x + 9$ The discriminant in this case is 35, so we must ramify over 5. This means that we can write the minimal polynomial as $(x - \bar{a})^2 \pmod 5$ where $\bar{a}$ is some congruence class mod 5. In fact, we calculate that $x^2 - x + 9 = (x - 3)^2 \pmod 5$. So the prime $\mathcal{P}$ lying over 5 is $(\omega - 3, 5)$. We see that 5 is irreducible in $\mathbb{Z}[\omega]$ since $xy = 5$ for x and y nonunits implies $\mathrm{N}(x)\,\mathrm{N}(y) = 25$ which implies that $\mathrm{N}(x) = 5$ (norms are always positive in imaginary quadratics). This can happen only if $\frac{a^2+35b^2}{4} = 5$ which means that $a^2 + 35b^2 = 20$, which is impossible. Since 5 is irreducible but $5\mathbb{Z}[\omega]$ is $\mathcal{P}^2$ and not prime, $\mathcal{P}$ cannot be principal. Hence $\mathbb{Z}[\omega]$ cannot have class number 1. Since $\mathcal{P}^2 = (5)$ is principal we see that $\mathcal{P}^2 = 1$. Thus, the order of $|\operatorname{Cl}(\mathbb{Z}[\frac{1+\sqrt{-35}}{2}])|$ is divisible by 2.

Now, we look at the Minkowski bound. We get $(1/2)(4/\pi)\sqrt{35}$ which is less than 5, so we need only check the primes over 2 and 3. Over 2, the polynomial becomes $x^2 + x + 1$ which is irreducible, so we need only check over 3. Over 3, our polynomial becomes $x(x - 1)$. So we have two primes $\mathcal{Q} = (\omega, 2)$ and $\mathcal{Q}' = (\omega - 1, 2)$. We know that $\mathcal{Q}'$ is the inverse of $\mathcal{Q}$ in the class group since $\mathcal{Q}\mathcal{Q}' = (2)$. Now, $\mathcal{Q}^2$ has norm equal to 9, so it must be in the same ideal class as $\mathcal{Q}$, $\mathcal{Q}'$ or (2). If $\mathcal{Q}^2$ is in the same class group as $\mathcal{Q}$, then it is $\mathcal{Q}$ is principal and the class group is trivial, which we know isn't true. If $\mathcal{Q}^2$ is in the same class group as $\mathcal{Q}'$, then $\mathcal{Q}$ has order 3 in the class group, which is impossible since we know that $\mathcal{Q}$ generates the class group and the class group has even order. Thus, we must have $\mathcal{Q}^2 = 1$ in the class group, so

$$|\operatorname{Cl}(\mathbb{Z}[\frac{1+\sqrt{-35}}{2}])| = 2.$$

Example 31.5. $|\operatorname{Cl}(\mathbb{Z}[\frac{\sqrt{-43}+1}{2}])| = 1$. Plugging into the Minkowski bound, we get

$$(1/2)(4/\pi)\sqrt{43} \leq (1/2)(4/3)7 < 5,$$

so we only need to look at 2 and 3. The minimal polynomial for

$$\omega = \frac{\sqrt{-43}+1}{2}$$

is $x^2 - x + 11$. Over 2, we get:

$$x^2 - x + 11 \equiv x^2 - x + 1 \pmod 2$$

which is irreducible, so $2\mathbb{Z}[\omega]$ is prime. Over 3, we get

$$x^2 - x + 11 \equiv x^2 - x + 2 \pmod 3$$

which has no roots (try 0,1,2) in $\mathbb{Z}/3\mathbb{Z}$, so is irreducible. Thus, $3\mathbb{Z}[\omega]$ is prime and principal. Now, we're done.

Note: it is generally easier to work in imaginary quadratics since the norms are easier to control. There are lots of real fields we can do as well, though.

Example 31.6. $|\operatorname{Cl}(\mathbb{Z}[\frac{\sqrt{13}+1}{2}])| = 1$. Plugging into Minkowski, we get

$$(1/2)\sqrt{13} < 2$$

so we must have class number 1.