Math 531 Tom Tucker
NOTES FROM CLASS 11/29

We had just finished proving:

Proposition 36.1. *$\ell(\mathcal{O}_L^*)$ is a full lattice in H.*

Proof. We have already seen that $\ell(\mathcal{O}_L^*)$ is a lattice in H. It is a full lattice since it generates a $\mathbb{R}$-vector space of dimension $r+s-1$, which must be equal to H (since $\dim_{\mathbb{R}} H = r+s-1$). $\square$

Theorem 36.2. *Let μ_L be the roots of unity in L as usual. There exist elements $v_1, \ldots, v_{r+s-1} \in \mathcal{O}_L^*$ such that every unit $u \in \mathcal{O}_L^*$ can be written uniquely as*

$$u = v v_1^{m_1} \cdots v_{r+s-1}^{m_{r+s-1}}$$

for $v \in \mu_L$ and $m_i \in \mathbb{Z}$.

Proof. Let $v_1, \ldots, v_{r+s-1}$ have the property that $\ell(v_1), \ldots, \ell(v_{r+s-1})$ generate $\ell(\mathcal{O}_L^*)$ as a $\mathbb{Z}$-module. Since $\ker \ell = \mu_L$, we know that every unit $u \in \mathcal{O}_L^*$ can be written as vz, where z is in the subgroup generated by the $v_1, \ldots, v_{r+s-1}$. The element z is uniquely determine by $\ell(u)$ as

$$v_1^{m_1} \cdots v_{r+s-1}^{m_{r+s-1}}$$

for some integers m_i. Then $v = zu^{-1}$ and is therefore also uniquely determined. $\square$

Let's go through this in the case of quadratic fields Let's look at the case of quadratic field first. If L is an imaginary quadratic field, then $\mathcal{O}_L$ can be thought of as a subfield of $\mathbb{C}$ and $\mathrm{N}(x) = x\bar{x} = a^2+b^2$, where $x = a+ib$. If $a^2+b^2 = 1$, then $a+bi$ lies on the unit circle. We can go a bit further and write $\mathcal{O}_L \subseteq \mathbb{Z}\omega$ where $\omega = \frac{1+\sqrt{-d}}{2}$ for some positive squarefree d. Then any norm can be written as $\frac{a^2+db^2}{4}$. In order to have

$$\frac{a^2+db^2}{4} = 1, \tag{1}$$

we must have $d \leq 4$ or $b = 0$. When $b = 0$, we must have $a^2 = 4$, so $a = \pm 2$, which gives us the obvious units ± 1. When $d = 2$, we cannot solve (1) except with $b = 0$ and $a = \pm 1$. When $d = 3$, we have 4 additional solutions

$$\frac{\pm 1 \pm \sqrt{-3}}{2}.$$

It is easy to check that that all of these are powers of ξ_6, a primitive 6-th root of unity. We've shown then that in an imaginary quadratic the only units are the roots of unity.

What about real quadratics? In this case a unit $x + \sqrt{d}y$ (d positive and squarefree) with $x, y \in \mathbb{Z}$ is solution to Pell's equation

$$x^2 - dy^2 = 1.$$

It was known in the 19th century that this has a solution other than $y = 0$ and $x = \pm 1$ and that there is a fundamental solution $u = x + y\sqrt{d}$ such that any other nontrivial (not ± 1) solution v is a power of u (so we don't need the Dirichlet unit theomre). Furthermore, we know that u is not a root of unity since the only roots of unity in $\mathbb{R}$ are ± 1. For real quadratics, then the free rank of $\mathcal{O}_L^*$ is 1.

There is an interesting example in the book with cubic fields that I will work through now. Take the ring

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

Then $|\Delta(B/\mathbb{Z})| = 3^3 11^2$. Since $11^3 \not\equiv 11 \mod 3^2$, this is a Dedekind domain. Let's try to calculate its class group. We end up with a Minkowski constant of

$$\frac{3!}{3^3}\frac{4}{\pi}\sqrt{3^3 11^2} < 17$$

so we only have to check up to 17. Let's get rid of the ramified primes first: over 3, we have

$$x^3 - 11 \equiv (x^3 - 2) \equiv (x-2)^3 \pmod 3$$

so the prime over 3 is $(3, \sqrt[3]{11} - 2)$ and $\mathrm{N}(\sqrt[3]{11} - 2) = -3$, so this ideal is generated by $\sqrt[3]{11} - 2$. Similarly at 11, we obtain

$$x^3 - 11 \equiv x^3 \pmod{11},$$

so the ideal over 11 is $(11, \sqrt[3]{11})$, which is obviously generated by $\sqrt[3]{11}$. Now, let's start checking the other primes over 2,

$$x^3 - 11 \equiv x^3 - 1 \equiv (x-1)(x^2 + x + 1) \pmod 2$$

so our primes are $(2, \sqrt[3]{11} - 1)$, which we'll call $\mathcal{P}_1$, and $(2, \sqrt[3]{11}^2 + \sqrt[3]{11} + 1)$, which we'll call $\mathcal{P}_2$.

Over 5, we get the same factorizaion

$$x^3 - 11 \equiv x^3 - 1 \equiv (x-1)(x^2 + x + 1) \pmod 5$$

so our primes are $(5, \sqrt[3]{11} - 1)$, which we'll call $\mathcal{Q}_1$, and $(5, \sqrt[3]{11}^2 + \sqrt[3]{11} + 1)$, which we'll call $\mathcal{Q}_2$.

Looking at 7, the only elements with cube roots mod 7 are ± 1, so $x^3 - 11$ is irreducible mod 7. Thus, $7B$ is irreducible and principal.

Similarly at 13, the only elements with cube roots are ± 1, 8, and 5, so $x^3 - 11$ is irreducible mod 13. Thus $13B$ is irreducible and principal.

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 $\mathrm{N}(\mathcal{Q}_2)$ exceeds the Minkowski bound, so is in the group generated by the $[\mathcal{P}_1], [\mathcal{Q}_1], [\mathcal{Q}_2]$. Now, let's look at the product $\mathcal{Q}_1\mathcal{P}_1$. We see that the norm of this ideal is 10. Since $\mathrm{N}(\theta - 1) = 10$, this ideal must be principal, since it is the only ideal with norm 10 in B. Thus, $\mathrm{Cl}(B)$ is generated by $\mathcal{Q}_1$.