Math 430 Tom Tucker
Notes From Class 11/01

Let us denote $(-1)^{(q-1)/2}$ as $\epsilon(q)$.

**Proposition 17.1.** *Suppose that $p$ is odd. There are an even number of distinct primes $\mathcal{Q}$ of $\mathbb{Z}[\xi_q]$ lying over $p$ if and only if $p\mathbb{Z}[\sqrt{\epsilon(q)q}]$ factors as two distinct primes. (This is much easier to follow with a picture which I give in class.)*

*Proof.* Let $\mathfrak{m}$ be a prime in $\mathbb{Z}[\xi_q]$ such that $\mathfrak{m} \cap \mathbb{Z} = p\mathbb{Z}$. Let $G$ denote the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_q)/\mathbb{Q})$, let $E$ denote $\mathbb{Q}(\sqrt{\epsilon(q)q})$, let $G_E$ denote the part of $G$ that acts identically on $E$, and let $D$ be the part of $G$ that sends $\mathfrak{m}$ to itself. Recall that $G$ acts transitively on the set of primes of $\mathbb{Z}[\xi_q]$ lying over $p$. Thus, the number of primes lying over $p$ is equal to $[G : D]$. The index $[G : D]$ is even if and only if $D \subseteq G_E$, since $G_E$ is the unique subgroup of index 2 in $G$.

Now, let's let $\mathfrak{q}$ be a prime of $\mathbb{Z}[\sqrt{\epsilon(q)q}]$ for which $\mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z}$. The group $G_E$ acts transitively on the set of primes of $\mathbb{Z}[\xi_q]$ lying over $\mathfrak{q}$. If this set is the same as the set of all primes in $\mathbb{Z}[\xi_q]$ lying over $\mathcal{P}$, then $\mathfrak{q}$ must be the only prime in $\mathbb{Z}[\sqrt{\epsilon(q)q}]$ lying over $p$. Otherwise, there must be two primes in $\mathbb{Z}[\sqrt{\epsilon(q)q}]$ lying over $p$.

We claim that $G_E$ acts transitively on the set of all $\mathfrak{m}$ lying over $p$ if and only if $D$ is not contained in $G_E$. Note that if $D$ is not contained in $G_E$, then the $[G_E : D \cap G_E] = [G : D]$, which means that the number of primes in the $G$-orbit of $\mathfrak{m}$ is the same as the number of primes in $G_E$-orbit of $\mathfrak{m}$, which means that $G_E$ acts transitively on the $\mathfrak{m}$ lying over $p$. If $D \subseteq G_E$, then $[G : D] = 2[G_E : D]$ and $G_E$ does not act transitively on this set. □

**Corollary 17.2.** *Suppose that $p$ is odd. Then $\left(\frac{\epsilon(q)q}{p}\right) = 1$ if and only if $p$ splits into an even number of primes in $\mathbb{Z}[\xi_q]$.*

*Proof.* $\left(\frac{\epsilon(q)q}{p}\right) = 1$ if and only if $x^2 - \epsilon(q)q$ factors over $p$, which happens if and only if $p\mathbb{Z}[\sqrt{\epsilon(q)q}]$ factors as two distinct primes, since $\mathbb{Z}[\sqrt{\epsilon(q)q}]$ localized at an odd prime of $\mathbb{Z}$ is integrally closed. □

Let $T_p$ denote the number of primes lying over $p$ in $\mathbb{Z}[\xi_q]$. From what we've just seen, $(-1)^{T_P} = \left(\frac{\epsilon(q)q}{p}\right)$.

The next two proposition and corollary work for any $p$ (including 2).

**Proposition 17.3.** *The degree of the field extension $\mathbf{F}_p[\xi_q]$ is equal to $\mathrm{ord}_q(p)$ (the order of $p$ in $\mathbf{F}_q$).*

*Proof.* This is on the midterm. Hint: $\mathbf{F}_{p^n}$ contains a primitive $q$-th root of unity if and only if $q|p^n - 1$. □

**Corollary 17.4.** *Suppose that there are $T_p$ primes in $\mathbb{Z}[\xi_q]$ lying above $p$. Then $\mathrm{ord}_q(p)$ is equal to $(q-1)/T_p$.*

*Proof.* Follows immediately from the previous proposition using the fact that $T_p f_p = q - 1$ (where $f_p$ is the degree of the residue field of primes lying over $p$). □

**Theorem 17.5.** *(Quadratic reciprocity for odd primes) Let $p$ and $q$ be odd primes, $p \neq q$. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

*Proof.* Let $\mathrm{ord}_q(p)$ denote the order of $p \pmod q$. We see that

$$\begin{aligned}\left(\frac{\epsilon(q)q}{p}\right) &= (-1)^{T_p} \quad \text{(Corollary 17.2)} \\ &= (-1)^{\frac{q-1}{\mathrm{ord}_q(p)}} \quad \text{(Corollary 17.4)} \\ &= \left(\frac{p}{q}\right) \quad \text{(Property (iv))}.\end{aligned}$$

Thus,

$$\left(\frac{p}{q}\right) = \left(\frac{\epsilon(q)q}{p}\right) = \left(\frac{-1^{(q-1)/2}}{p}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right).$$

Multiplying $\left(\frac{p}{q}\right)$ by $\left(\frac{q}{p}\right)$ then finishes the proof. □

********** Now, let's move on to the class group. Recall that for any integral domain $R$, we have notion of invertible ideals (recall that it is a fractional ideal with an inverse) and that we have an exact sequence

$$0 \longrightarrow \mathrm{Pri}(R) \longrightarrow \mathrm{Inv}(R) \longrightarrow \mathrm{Pic}(R) \longrightarrow 0.$$

where $\mathrm{Pri}(R)$ is the set of principal ideals of $R$, $\mathrm{Inv}(R)$ is set of invertible ideals of $R$, and the group law is multiplication of fractional ideals. When $R$ is Dedekind, we call $\mathrm{Pic}(R)$ the class group of $R$ and denote it as $\mathrm{Cl}(R)$. When $R$ is the integral closure $\mathcal{O}_L$ of $\mathbb{Z}$ in some number field $L$, we often write $\mathrm{Cl}(L)$ for $\mathrm{Cl}(\mathcal{O}_L)$. We also write $\Delta(L)$ for $\Delta(\mathcal{O}_L/\mathbb{Z})$. We want to prove the following.

**Theorem 17.6.** *Let $L$ be a number field. Then $\mathrm{Cl}(L)$ is finite.*

We've already shown this $\mathbb{Z}[i]$. We showed that $\mathrm{Cl}(\mathbb{Z}[i]) = 1$, i.e. that it is a principal ideal domain. On the other hand, we've seen that $\mathrm{Pic}(\mathbb{Z}[\sqrt{19}]) \neq 1$ (this ring isn't Dedekind, but later we'll see Dedekind rings with nontrivial class groups.

How did we show that $\mathrm{Cl}(\mathbb{Z}[i]) = 1$? We took advantage of the fact that $\mathbb{Z}[i]$ forms a sublattice of $\mathbb{C}$. We'll try to do that in general.

Here is the idea... If we have a number field $L$ of degree $n$ over $\mathbb{Q}$, then we have $n$ different embeddings of $L$ into $\mathbb{C}$. They can be obtained by fixing one embedding $L \longrightarrow \mathbb{C}$ and then conjugating this embedding by elements in the cosets of $H_L$ in $\mathrm{Gal}(M/\mathbb{Q})$ for $M$ some Galois extension of $\mathbb{Q}$ containing $L$. We'll use these to make $B$ a full lattice in $\mathbb{R}^n$. What is a full lattice?

**Definition 17.7.** A lattice $\mathcal{L} \subset \mathbb{R}^n$ is a free $\mathbb{Z}$-module whose rank as a $\mathbb{Z}$-module is the equal to the dimension of the $\mathbb{R}$-vector space generated by $\mathcal{L}$. A full lattice $\mathcal{L} \subset \mathbb{R}^n$ is a free $\mathbb{Z}$-module of rank $n$ that generates $\mathbb{R}^n$ as a $\mathbb{R}$-vector space.

**Example 17.8.**
(1) $\mathbb{Z}[\theta]$ where $\theta^2 = 3$ is *not* a full lattice of $\mathbb{R}^2$ under the embedding $1 \mapsto 1$ and $\theta \mapsto \sqrt{3}$, since it generates an $\mathbb{R}$-vector space of dimension 1.
(2) $\mathbb{Z}[i]$ is full lattice in $\mathbb{R}^2$ where $\mathbb{R}^2$ is $\mathbb{C}$ considered as an $\mathbb{R}$-vector space with basis $1, i$ over $\mathbb{R}$.

On the other hand, we can send $\mathbb{Z}[\theta]$ where $\theta^2 = 3$ into $\mathbb{R}^2$ in such a way that it is a full lattice in the following way. Let $\phi : 1 \mapsto (1, 1)$ and $\phi : \theta :\longrightarrow (\sqrt{3}, -\sqrt{3})$. In this case, we must generate $\mathbb{R}^2$ as an $\mathbb{R}^2$ vector space since $(1, 1)$ and $(\sqrt{3}, -\sqrt{3})$ are linearly independent.

There are two different types of embeddings of $L$ into $\mathbb{C}$. There are the real ones and the complex ones. An embedding $\sigma : L \longrightarrow \mathbb{C}$ is real if $\overline{\sigma(y)} = \sigma(y)$ for every $y \in L$ (the bar here denotes complex conjugation) and is complex otherwise. How can we tell which is which?

Suppose we have a number field $L$. We can write $L \cong \mathbb{Q}[X]/f(X)$ for some monic irreducible polynomial $L$ with integer coefficients. Then by the Chinese remainder theorem $\mathbb{R}[X]/f(X) \cong \bigoplus_{i=1}^{m} \mathbb{R}[X]/f_i(X)$ where the $f_i$ have coefficients in $\mathbb{R}$, are irreducible over $\mathbb{R}$, and $f_1 \dots f_m = g$ (note that the $f_i$ are distinct since $L$ is separable over $\mathbb{Q}$). We also know that each $f_i$ is of degree 1 or 2. When $f_i$ has degree 1, then $\mathbb{R}[X]/f_i(X)$ is isomorphic to $\mathbb{R}$ and when $f_i$ has degree 2, then $\mathbb{R}[X]/f_i(X)$ is isomorphic to $\mathbb{C}$. Since $\mathbb{Q}$ has a natural embedding into $\mathbb{R}$, we obtain a natural embedding of

$$j : L \cong \mathbb{Q}[X]/f(X) \longrightarrow \bigoplus_{i=1}^{m} \mathbb{R}[X]/f_i(X).$$

Composing $j$ with projection onto the $i$-th factor of

$$\bigoplus_{i=1}^{m} \mathbb{R}[X]/f_i(X)$$

then gives a map from $L \longrightarrow \mathbb{R}$ or $L \longrightarrow \mathbb{C}$. In fact, when $\deg f_i = 2$ and $\mathbb{R}[X]/f_i(X)$ is $\mathbb{C}$ we get two embeddings by composing with conjugation. The image of $L$ is the same for these two embeddings, so we will want to link these two in some way...

Let's order the embeddings $\sigma_1, \ldots, \sigma_n$ ($n = [L : \mathbb{Q}]$) in the following way. We let $\sigma_1, \ldots, \sigma_r$ be real embeddings. The remaining embeddings come in pairs as explained above, so for $i = r+1, r+3, \ldots$, we let $\sigma_i$ be a complex embedding and let $\sigma_{i+1} = \overline{\sigma_{i+1}}$. We let $s$ be the number of complex embeddings. We have $r + 2s = n$.

Now, we can embed $\mathcal{O}_L$ into $\mathbb{R}^n$ by letting

$$\begin{aligned} h(y) &= (\sigma_1(y), \ldots, \sigma_r(y), \\ &\quad \Re(\sigma_{r+1}(y)), \Im(\sigma_{r+1}(y)), \ldots, \Re(\sigma_{r+2(s-1)}(y)), \Im(\sigma_{r+2(s-1)}(y))) \\ &= \big(\sigma_1(y), \ldots, \sigma_r(y), \\ &\quad \frac{\sigma_{r+1}(y) + \sigma_{r+2}(y)}{2}, \frac{\sigma_{r+1}(y) - \sigma_{r+2}(y)}{2i}, \ldots, \\ &\quad \frac{\sigma_{r+2(s-1)}(y) + \sigma_{r+2(s-1)}(y)}{2}, \frac{\sigma_{r+2(s-1)}(y) - \sigma_{r+2(s-1)+1}(y)}{2i}\big). \end{aligned} \tag{1}$$

Let us also denote as $h_i$ the map $h : \mathcal{O}_L \longrightarrow \mathbb{R}$ given by composing $h$ with projection $p_i$ onto the $i$-th coordinate of $\mathbb{R}^n$.

We will continue to use $h$ and $h_i$ as defined above. We will also continue to let $s$ and $r$ be as above and to let $n = r + 2s$ be the degree $[L : \mathbb{Q}]$.