CLASS FIELD THEORY

COURSE: RENÉ SCHOOF AND PETER STEVENHAGEN
NOTES: ROSS PATERSON

Disclaimer. These notes were taken live during lectures. Any errors are the fault of the transcriber and not of the lecturer.

Lecture 1 (Stevenhagen)

Recall the Fermat equation

$$x^n + y^n = z^n/\mathbb{Z}.$$

Note, an observation due to the likes of Kummer, that if we allow ourselves complex numbers then we can factorise

$$y^m = \prod_{i=1}^{m} (Z - \zeta_m^i X),$$

where $\zeta_m = e^{2\pi i/m}$. Kummer discovered that in fact we don't need to look at all of the complex numbers, but in fact we should look at 'number rings' $\mathbb{Z}[\zeta_m]$.

Algebraic Number Theory. Algebraic number theory is essentially doing arithmetic like we do for $\mathbb{Z}$, but now for number rings. These number rings live in number fields, much like $\mathbb{Z}$ lives in $\mathbb{Q}$, and in fact we end up with a diagram

$$\begin{tikzcd} K = \mathbb{Q}(\alpha) \supset \mathcal{O}_K \supseteq \mathbb{Z}[\alpha] \\ \mathbb{Q} \supset \mathbb{Z} \arrow[u, "n"] \end{tikzcd}$$

where $f = f_{\mathbb{Q}}^{\alpha} \in \mathbb{Z}[X]$ is the minimal polynomial of α. Some remarks.

- We would like to find $\mathcal{O}_K$, the ring of integers, which is free of rank $n/\mathbb{Z}$.
- $\mathcal{O}_K$ has unique prime factorisation.
- We have the class group $\mathrm{Cl}_K = I_K/P_K$, where I_K is the group of fractional ideals in $\mathcal{O}_K$ and P_K is the group of principal fractional ideals, and this is a finite abelian group.
- We have embeddings

  $$\begin{tikzcd} K \arrow[r, "\text{complex}"] \arrow[dr, "\text{real}"'] & \mathbb{C} \\ & \mathbb{R}, \arrow[u] \end{tikzcd}$$

  say we have r real embeddings and $2s$ complex ones (this is always even since for every complex embedding there is the complex conjugate embedding). Then $r + 2s + n$.
- $\mathcal{O}_K^\times = \mu_K \times \mathbb{Z}^{r+s-1}$, where μ_K is the finite group of roots of unity in K.

- The discriminant of the minimal polynomial of α, $\Delta(f)$, is related to the discriminant of the number field, Δ_K, by
$$\Delta(f) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \Delta_K.$$
- There is the Minkowski bound, which tells us that every class in Cl_K contains an integral ideal of norm at most the 'Minkowski constant' M_K, which is some explicit multiple of $\sqrt{\Delta_K}$. More precisely
$$M_K = \left(\frac{4}{\pi}\right)^s \left(\frac{n!}{n^n}\right)^2 \sqrt{\Delta_K}$$

Cyclotomic Rings. Ok so let us return to our example of cyclotomic rings. Let $K_m = \mathbb{Q}(\zeta_m)$, then the ring of integers is easy:
$$\mathcal{O}_K = \mathbb{Z}[\zeta_m].$$
There is already a natural action of $R_m = (\mathbb{Z}/m\mathbb{Z})^\times$ on this ring and field. For $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ we have the map $\varphi_a : \zeta_m \mapsto \zeta_m^a$. Thus $\mathcal{O}_K$ is a $\mathbb{Z}[R_m]$-module.

Splitting of Primes. Recall we had the diagram
$$\begin{array}{c} K = \mathbb{Q}(\alpha) \supset \mathbb{Z}[\alpha] \\ {\scriptstyle n}\Big\uparrow \\ \mathbb{Q} \supset \mathbb{Z} \end{array}$$
We want to know what 'lies above a prime $p \in \mathbb{Z}$', i.e. we want the factorisation
$$p\mathcal{O}_K = \prod_{i=1}^t \mathfrak{p}_i^{e_i}.$$
For $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, we can take $\overline{f} = f \mod p$ and look at its factorisation
$$\overline{f} = \prod_{i=1}^t \overline{g}_i^{e_i} \in \mathbb{F}_p[X],$$
and this gives the correct e_i and moreover if we choose lifts of the $\overline{g}_i$ to $\mathbb{Z}[X]$ then $\mathfrak{p}_i = \langle p, g_i(\alpha)\rangle$.

Moreover, for Galois extensions, $G = \mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $\{\mathfrak{p} : \mathfrak{p} \mid p\}$, and $[K : \mathbb{Q}] = e \cdot f \cdot g$, where for p a prime of $\mathbb{Z}$:

- e is the ramification index of one (all) of the primes $\mathfrak{p}$ above p;
- f is the residue field degree, i.e. the degree of the extension $\mathcal{O}_K/\mathfrak{p} =: k_{\mathfrak{p}} \supseteq \mathbb{F}_p$;
- $g = \#\{\mathfrak{p} : \mathfrak{p} \mid p\}$.

For $\mathfrak{p} \in \{\mathfrak{p} : \mathfrak{p} \mid p\}$, one takes the stabiliset $G_{\mathfrak{p}} = \mathrm{stab}_{\mathfrak{p}} \subseteq G$ and calls this the decomposition group. If the extension is unramified (i.e. $e = 1$) then this group is isomorphic via reduction to $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$, where Frob_p is the Frobenius map $x \mapsto x^p$.

Example 1. *For cyclotomic fields $G_{\mathfrak{p}} = \langle p \mod m\rangle$, and so $\mathbb{F}_p(\zeta_m)/\mathbb{F}_p$ has degree equal to the order of $p \in (\mathbb{Z}/m\mathbb{Z})^\times$*

Example 2 (Cyclotomic fields with $m = 20$)**.** *Compute for yourselves the following diagrams.*

$$\begin{array}{cccc}
 & & \mathbb{Q}(\zeta_{20}) & \\
 & \mathbb{Q}(i, \sqrt{5}) & \mathbb{Q}(\zeta_{20})^+ & \mathbb{Q}(\zeta_5) \\
\mathbb{Q}(i) = \mathbb{Q}(\zeta_4) & \mathbb{Q}(\sqrt{-5}) & \mathbb{Q}(\sqrt{5}) & \\
 & \mathbb{Q} & &
\end{array}$$

$$\begin{array}{cccc}
 & & \mathbb{Q}(\zeta_{20}) & \\
 & \mathbb{Q}(i, \sqrt{5}) & \mathbb{Q}(\zeta_{20})^+ & \mathbb{Q}(\zeta_5) \\
\mathbb{Q}(i) = \mathbb{Q}(\zeta_4) & \mathbb{Q}(\sqrt{-5}) & \mathbb{Q}(\sqrt{5}) & \\
 & \mathbb{Z}/m\mathbb{Z}^\times \& & &
\end{array}$$

Example 3 (Cyclotomic Fields)**.** *We have a correspondence*

$$(\mathbb{Z}/m\mathbb{Z})^\times \leftrightarrow \mathrm{Gal}(K_m/\mathbb{Q})$$
$$p \leftrightarrow \mathrm{Frob}_p.$$

This is actually an example of a more general mapping known as the Artin symbol. Dirichlet proved that there is equidistibution here. That is, for every $a \in \mathbb{Z}/m\mathbb{Z}^\times$ the set of primes p such that $p \equiv a \mod m$ has density $1/\varphi(m)$. This is also an example of a more general phenomenon.

Theorem 4 (Dirichlet(1840's)–Frobenius–Chebotarev(1924))**.** *Let L/K be a finite Galois extension of number fields, $G = \mathrm{Gal}(L/K)$, $C \subseteq G$ be a conjugacy class. Then*

$$\{fp \text{ of } K \ : \ \mathrm{Frob}_{\mathfrak{p}} \in C\}$$

has density (in an appropriate sense) equal to $\frac{\#C}{\#G}$.

This is a key result which is extremely important, and has many corollaries which are actually more classical at least than Chebotarev.

Corollary 5. *Let L/K be a finite Galois extension of number fields, then*

$$\{\mathfrak{p} \ : \ \mathfrak{p} \text{ splits completely in } L/K\}$$

has density $\frac{1}{[L:K]}$.

Corollary 6. *If all $p \equiv 1 \mod m$ split in $L/\mathbb{Q}$ then $L \subseteq \mathbb{Q}(\zeta_m)$.*

Theorem 7 (Kronecker–Weber(middle of the 1800's)–Hilbert)**.** *Every finite abelian extension of $\mathbb{Q}$ is cyclotomic. That is, it is contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$.*

key step of proof. If $\mathbb{Q} \subseteq L$ is totally unramified (i.e. unramified everywhere) then $\mathbb{Q} = L$. Moreover we have a map

$$\mathbb{Z}/m\mathbb{Z}^\times \to \mathrm{Gal}(L/\mathbb{Q})$$

Given by

$$p \mod m \mapsto \mathrm{Frob}_p.$$

□

Main Theorem of Class Field Theory.

Theorem 8 (CFT)**.** *Let K be a number field, and L/K be an abelian extension. Then L is a class field, i.e. it is contained in a ray class field modulo some modulus $\mathfrak{m}$.*

Of course there are plenty of words here that need to be defined and understood, but the point is as follows: There is a 'ray class group modulo $\mathfrak{m}$' $\mathrm{Cl}_\mathfrak{m}$ generated by some set of primes $\mathfrak{p} \nmid \mathfrak{m}$ and such that

$$\mathrm{Cl}_\mathfrak{m} \to \mathrm{Gal}(L/K)$$
$$[\mathfrak{p}] \mapsto \mathrm{Frob}_\mathfrak{p}.$$

By the end of this week you should hopefully see this as no more complicated than $\mathbb{Z}/m\mathbb{Z}^\times$! Let us see the definition.

Definition 9. A modulus of a number field K is a formal pair $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where $\mathfrak{m}_0 \subseteq \mathcal{O}_K$ is a nonzero ideal and $\mathfrak{m}_\infty$ is a collection of real embeddings of K. We define the associated ray class group as follows.

$$\mathrm{Cl}_\mathfrak{m} = I(\mathfrak{m})/R_\mathfrak{m},$$

where $I(\mathfrak{m})$ is the group generated by the fractional ideals of K which are coprime to $\mathfrak{m}$ and $R_\mathfrak{m} = \langle \alpha\mathcal{O}_K \;:\; \alpha \equiv 1 \mod \mathfrak{m}\rangle$, where $\alpha \equiv 1 \mod \mathfrak{m}$ means that both for $\mathfrak{p} \mid \mathfrak{m}_0$ we have $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m}_0)$ and for $\sigma \in \mathfrak{m}_\infty$ we have $\sigma(\alpha) > 0$.

Example 10 (Ray class groups for $\mathbb{Q}$)**.** *For $K = \mathbb{Q}$ what do we get? Consider $\mathfrak{m} = \langle m\rangle$, then*

$$\mathrm{Cl}_\mathfrak{m} = (\mathbb{Z}/m\mathbb{Z})^\times / \langle \pm 1\rangle .$$

If we add the infinite place and consider $\mathfrak{m} = \langle m\rangle \cdot \infty$ then

$$\mathrm{Cl}_\mathfrak{m} = \mathbb{Z}/m\mathbb{Z}^\times.$$

So we've already seen these!

Since the set of principal ideals coprime to $\mathfrak{m}$, call it $P(\mathfrak{m})$, lies between $I(\mathfrak{m})$ and $R_\mathfrak{m}$, we have a map

$$\mathrm{Cl}_\mathfrak{m} \to \mathrm{Cl}_K.$$

In fact this map is surjective, and moreover we obtain a sequence

$$1 \longrightarrow (\mathcal{O}_K/\mathfrak{m})^\times / \mathrm{im}(\mathcal{O}_K^\times) \longrightarrow \mathrm{Cl}_\mathfrak{m} \longrightarrow \mathrm{Cl}_K \longrightarrow 0,$$

where $(\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times = (\mathcal{O}_K/\mathfrak{m}_0)^\times \times \prod_{\sigma \in \mathfrak{m}_\infty} \langle -1\rangle$.

Every $\mathfrak{m}$ gives rise to an analogue of the cyclotomic fields, called the ray class field modulo $\mathfrak{m}$, which we denote by $H_\mathfrak{m}$.

Consider the sets enumerated by $n \in \mathbb{Z}_{>0}$

$$S_n := \left\{p \;:\; p = x^2 + ny^2\right\}.$$

Then we know

$$S_1 = \{p \ : \ p = x^2 + y^2\} = \{p \equiv 1 \mod 4\}$$

which has density 1/2. Moreover similar results are easy enough for $n = 2, 3, 4$. This is seen by considering the factorisation of p in $\mathbb{Z}[\sqrt{-n}]$. However when we get to $n = 5$ there is a problem: the class group of $\mathbb{Z}[\sqrt{-5}]$ is $\mathbb{Z}/2\mathbb{Z}$ (not trivial), so factoring the prime p as an ideal doesn't help so much.

Definition 11. For $\mathfrak{m} = 1$ the field $H = H_{\mathfrak{m}}$ is called the Hilbert class field, and $\mathrm{Cl}_K = \mathrm{Cl}_{\mathfrak{m}} \cong \mathrm{Gal}(H/K)$.