MATH 6370, LECTURE 9
APRIL 06

GORDAN SAVIN

We shall now state a simplified version of the main theorem in global class field theory. Let $[F:\mathbb{Q}]=n$ be a number field, and A the ring of algebraic integers in F. We shall assume that A is a principal ideal domain, in fact, we shall assume a stronger condition, that the ideals are principal in the narrow sense. More precisely, let $\sigma_1,\dots,\sigma_r$ be all real embeddings of F. An element $\alpha\in F^\times$ is called totally positive if $\sigma_i(\alpha)>0$ for all real embeddings. For $F=\mathbb{Q}$, totally positive means simply positive. If F has no real embeddings then there are no conditions, and in this case all non-zero elements are totally positive. We say that a non-zero ideal $I\subset A$ is principal in the narrow sense if $I=(\alpha)$ for a totally positive α. For example, $A=\mathbb{Z}$, then all non-zero ideals are generated by positive integers.

The narrow class group is the group of classes of ideals modulo narrow principal ideals. In general, this group may be larger than the usual groups of classes of ideals. To understand the difference, consider the homomorphism $A^\times\to\mu_2^r$ given by

$$\gamma\mapsto(\text{sign}\sigma_1(\gamma),\dots,(\text{sign}\sigma_r(\gamma)).$$

Let A^+ be the kernel of the above homomorphism. This is the group of all totally positive units. Observe that $\mathbb{Z}^+$ is trivial.

If this homomorphism is surjective then every non-zero principal ideal $I=(\beta)$ is generated by a totally positive element. Indeed, there exists $\gamma\in A^\times$ such that

$$(\text{sign}\sigma_1(\gamma),\dots,(\text{sign}\sigma_r(\gamma))=(\text{sign}\sigma_1(\beta),\dots,(\text{sign}\sigma_r(\beta)).$$

Then $\alpha=\beta\gamma$ is totally positive, and $I=(\alpha)$.

Exercise: The ring of integers in $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{6})$ are both (usual) PIDs. Decide if they are PIDs in the narrow sense.

So assume that A is PID in the narrow sense. In particular, every non-zero ideal is generated by a totally positive element, unique up to multiplying by an element in A^+. The global class field theorem in this case says the following. For every non-zero ideal $I\subset A$ there exists an abelian extension E of F iwhose Galois group is

$$G(E/F)\cong(A/I)^\times/A^+.$$

Any abelian extension of F is contained in such E. If $F=\mathbb{Q}$, and $I=(m)$, then E is the cyclotomic filed with the Galois group $(\mathbb{Z}/m\mathbb{Z})^\times$. Let $P\subseteq A$ be a prime ideal. Let $P\cap\mathbb{Z}=(p)$. Then A/P is a finite field of characteristic p consisting of q elements. Let B be the ring of integers in E. Assume that P is unramified in B. That means that we have a factorization $BP=Q_1\cdot\ldots\cdot Q_g$ into pairwise different prime ideals in B. Let $Q\subset B$ be any of these ideals. Then $Q\cap A=P$ and B/Q is a finite field extension of A/P. Recall that the

Frobenius Fr_P is an element in $G(E/F)$ such that

$$\mathrm{Fr}_P(x) \equiv x^q \pmod{Q}$$

for all $x \in B$. Write $P = (\pi)$ for a totally positive element π in A. The set of maximal ideals containing I is finite. Assume that P is not one of them. Then $I + P = A$ (why?) hence there exists $i \in I$ and $a \in A$ such that $i + \pi a = 1$. It follows that π is invertible modulo I, thus it gives an element, denoted by the same letter π in $(A/I)^\times$. The extension E, corresponding to I, is unramified at P and

$$\mathrm{Fr}_P \mapsto \pi \in (A/I)^\times/A^+$$

under the isomorphism $G(E/F) \cong (A/I)^\times/A^+$. Note that this is well defined. This is Artin's reciprocity map. The field E is called a ray class field.

As I varies, the isomorphisms $G(E/F) \cong (A/I)^\times/A^+$ are compatible as follows. If $J \subseteq I$ are two ideals and K and E the corresponding ray class fields, then $K \supseteq E \supseteq F$ and the surjection

$$G(K/F) \to G(E/F)$$

obtained by restricting to E elements in $G(K/F)$, corresponds to the natural map

$$(A/J)^\times/A^+ \to (A/I)^\times/A^+.$$

Now is perhaps the right moment to introduce Galois groups of fields that are composites of infinitely many (finite) Galois extensions, for example, all abelian extensions of a number field. The following example is a good way to start. Let $F_n = \mathbb{Q}(\mu_{p^n})$ the abelian extension of $\mathbb{Q}$ obtained by adjoining the roots of one of order p^n. As n grows we get an increasing sequence of fields (sometimes called a tower of extensions)

$$F_1 \subset F_2 \subset \ldots \subset F = \cup_{n=1}^\infty F_n = \mathbb{Q}(\mu_{p^\infty}).$$

Let $G_n = G(F_n/\mathbb{Q})$. The above sequence of inclusions gives a (so-called, for obvious reasons) inverse system of surjections

$$G_1 \leftarrow G_2 \leftarrow \ldots.$$

Note that an automorphism σ of F is the same as a sequence of $\sigma_n \in G_n$ such that the restriction of σ_n to F_{n-1} is σ_{n-1}. In other words the group of automorphims of F is the set of $\sigma = (\sigma_1, \sigma_2, \ldots)$, where $\sigma_n \in G_n$, and $\sigma_n \mapsto \sigma_{n-1}$ by the surjective maps. This set is called the inverse (or projective) limit of the groups G_n and denoted by

$$G = \varprojlim G_n.$$

For the example at hand, $G_n \cong (\mathbb{Z}/n\mathbb{Z})^\times$ and $G = \mathbb{Z}_p^\times$ the group of units in the p-adic completion of $\mathbb{Z}$. Thus $\mathbb{Z}_p^\times$ is the Galois group of the maximal abelian extension of $\mathbb{Q}$ ramified at p only. For different primes these fields are (linearly) independent, see the previous lecture, so the Galois group of the maximal abelian extension of $\mathbb{Q}$ is the product of $\mathbb{Z}_p^\times$ over all primes p.