1 Overview and Review, 8/23/16

1.1 Overview

Class field theory provides a dictionary between abelian extensions of a given number field F (*i.e.* Galois extensions of F with abelian Galois group) and intrinsic data about the number field, e.g. the class group of the ring of integers, $\mathrm{Cl}(\mathcal{O}_F)$. For instance, if we let H be the union of all abelian extensions of F that are everywhere unramified, we have $\mathrm{Gal}(H/F) \cong \mathrm{Cl}(\mathcal{O}_F)$.

However, class field theory does not construct these abelian extensions, except for two classical constructions which were already known:

1. $F = \mathbb{Q}$, which has $H = \mathbb{Q}(\mu_\infty)$, where we have adjoined all the roots of unity. This is Kronecker-Weber theorem.
2. F a quadratic imaginary extension of $\mathbb{Q}$.

This is not so bad, however, since it turns out that class field theory can actually yield information about non-abelian extensions!

1.2 Topics

- Review local and global fields.
- Group and Galois cohomology.
- Local class field theory and local duality (important!).
- Global class field theory and global duality.
- Applications (Iwasawa theory).

1.3 Review

1.3.1 First Example

Let L/K be a finite Galois extension. Let $\mathfrak{P}$ be an unramified prime of L lying over $\mathfrak{p}$, so that $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_i}$ with all $e_i = 1$.

Lemma 1.3.1. *There is an element* $\mathrm{Fr}_{\mathfrak{P}}$ *of* $\mathrm{Gal}(L/K)$ *such that*

1) $\mathrm{Fr}_{\mathfrak{P}}(\mathfrak{P}) = \mathfrak{P}$*, i.e.* $\mathrm{Fr}_{\mathfrak{P}}$ *is in the decomposition group of* $\mathfrak{P}$*.*

2) $\mathrm{Fr}_{\mathfrak{P}}$ *acts on* $\mathcal{O}_L/\mathfrak{P}$ *as* $x \to x^{N(\mathfrak{p})}$*.*

Remark 1. *Note that* $\mathcal{O}_K/\mathfrak{p}$ *is a finite field of order* $N(\mathfrak{p})$*, which has the Frobenius automorphism that does precisely what 2 does. We should think of* $\mathrm{Fr}_{\mathfrak{P}}$ *as a lift of that map to* $\mathcal{O}_L/\mathfrak{P}$*.*

Proof. We will construct $\mathrm{Fr}_{\mathfrak{P}}$ explicitly. Let $\alpha \in \mathcal{O}_L$ satisfying

1. α generates $(\mathcal{O}_L/\mathfrak{P})^\times$, and
2. for all $\mathfrak{P}^o \neq \mathfrak{P}$ above $\mathfrak{p}$, $\alpha \in \mathfrak{P}^o$.

Set $F(X) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (X - \sigma\alpha) \in \mathcal{O}_K[X]$. Then $F(\alpha) = 0$, so $F(\alpha^{N(\mathfrak{p})}) = F(\alpha)^{N(\mathfrak{p})} = 0$.

Then for some σ, $\alpha^{N(\mathfrak{p})} \equiv \sigma\alpha \pmod{\mathfrak{P}}$. Then we claim that $\sigma\mathfrak{P} = \mathfrak{P}$. Otherwise, $\sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$, so $\alpha \in \sigma^{-1}\mathfrak{P}$, so $\sigma\alpha \in \mathfrak{P}$. So $\alpha^{N(\mathfrak{p})} \equiv 0 \pmod{\mathfrak{P}}$, a contradiction.

Then for all $x \in \mathcal{O}_L/\mathfrak{P}$, we can write $x = \alpha^i + b$, for some i and $b \in \mathfrak{P}$. Then

$$\sigma(x) = \sigma(\alpha^i) + \sigma(b) = \alpha^{iN(\mathfrak{p})} + \sigma(b) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}.$$

Now define $\mathrm{Fr}_{\mathfrak{P}} := \sigma$. Uniqueness is left to the reader. $\square$

Remark 2. *If* $\mathfrak{P}^o = \tau(\mathfrak{P})$ *for some* $\tau \in \mathrm{Gal}(L/K)$*,* $\mathrm{Fr}_{\mathfrak{P}^o} = \tau \mathrm{Fr}_{\mathfrak{P}} \tau^{-1}$*.*

Recall that L/K being Galois means $\mathrm{Gal}(L/K)$ acts transitively on the primes $\mathfrak{P}$ lying over $\mathfrak{p}$. So $\mathrm{Fr}_{\mathfrak{P}}$ is well-defined up to conjugation. If L/K is abelian, it is well-defined.

1.3.2 $\mathrm{Fr}_{\mathfrak{P}}$ of Cyclotomic Field

Let $L = \mathbb{Q}(\zeta_n)$ be the n-th cyclotomic field, $K = \mathbb{Q}$. Then $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Take p unramified in L/K, i.e. p not dividing n. Then Fr_p (we are in an abelian extension, so all $\mathrm{Fr}_{\mathfrak{P}}$ are the same). By definition, Fr_p is the σ such that $\sigma(\alpha) = \alpha^p \pmod{\mathfrak{P}}$, for all $\mathfrak{P}$ over p.

Also characterized by $\tau(\zeta_n) = \zeta_n^p$ since

$$\tau \sum a_i \zeta_n^i = (\sum a_i \zeta_n^i)^p.$$

1.3.3 $\mathrm{Fr}_{\mathfrak{P}}$ of Quadratic Field

Here, we let $L = \mathbb{Q}(\sqrt{d})$ and K as before. Then $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$, and for p unramified in L, Fr_p corresponds to 1 if p splits in L, or -1 if p is inert in L. This means that

$$\mathrm{Fr}_p = \left(\frac{d}{p}\right).$$

This connection leads us to an extremely nice proof of the quadratic reciprocity for odd primes.

Theorem 1.3.2. *Let $p \neq q$ be odd primes. Then* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Proof. Let $L = \mathbb{Q}(\zeta_p)$, $K = \mathbb{Q}$. Then $\mathrm{Gal}(L/K)$ is cyclic of order $p-1$, and so has a unique order two quotient which corresponds to a quadratic field F, where $F = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$.

Since q is unramified, we can consider Fr_q which corresponds to $q \in (\mathbb{Z}/p\mathbb{Z})^\times$. Now we simply compute this quantity in two ways.

(i) $\mathrm{Fr}_q|_F = 1 \Leftrightarrow q^{\frac{p-1}{2}} \equiv 1 \pmod p \Leftrightarrow \left(\frac{q}{p}\right) = 1$.

(ii) $\mathrm{Fr}_q|_F$ is also simply Fr_q for the quadratic extension F, hence equal to $\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right)$ by the previous example.

□

1.4 First Case of Fermat's Last Theorem

Theorem 1.4.1. *If p does not divide $|\mathrm{Cl}(\mathbb{Q}(\zeta_p))|$, then $x^p + y^p = z^p$ has no integer solutions with p not dividing xyz.*

The idea is that we can factor $\prod_i (x + \zeta_p^i y) = z^p$ in $\mathbb{Z}[\zeta_p]$. It turns out that regularity gives us that the LHS factors are p-th powers, the divisibility condition giving us that the factors are coprime.

Proof. We take $p > 5$, since we can easily prove the cases $p = 3, 5$ by looking at the equation modulo $9, 25$ respectively. Without loss of generality, assume x, y, z are coprime and p does not divide $x - y$. If $x \equiv y \pmod p$ and $x \equiv -z \pmod p$, then $-2z^p \equiv z^p \pmod p$, a contradiction. So we must have one or the other.

First, prove the coprimeness of the factors. If a prime q of $\mathbb{Z}[\zeta_p]$ divides two factors $x + \zeta_p^k y$ for $k = i, j, i \neq j$. Then $q|(\zeta_p^i - \zeta_p^j)y$. Since p does not divide y, and $q|(\zeta_p^j - \zeta_p^i)x$, so $q|(\zeta_p^i - \zeta_p^j)$, the unique prime ideal over p. (Recall that $p\mathbb{Z}[\zeta_p] = (1-\zeta_p)^{p-1}$). So $q = (1 - \zeta_p) = p$, so $p|x + y$, i.e. $x + y \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, so $x^p + y^p \equiv x + y \equiv 0 \pmod p$.

Hence, $(x + \zeta_p^i y) = J_i^p$ for some ideal J_i. But since p does not divide the class group, no element can have order p, hence J_i is principal. Then $x + \zeta_p^i y = u\alpha_i^p$ for some unit u. Dirichlet's unit theorem doesn't give us precise control over what the units look like, so we need to muck around with the following lemma.

Lemma 1.4.2. *Let u be a unit. Then $u = \zeta_p^r \epsilon$ for a unit ϵ of the maximal real subfield of the p-th cyclotomic field.*

Proof. Consider $u/\bar{u}$, an algebraic integer with norm 1 in all complex embeddings. This means $u/\bar{u}$ is a root of unity, so

$$u/\bar{u} = \pm\zeta_p^s,$$

for some s. If the sign is plus, let r be such that $2r \equiv s \pmod p$. It turns out that a minus sign gives us a contradiction.

□

So $x + \zeta_p^i y = \zeta_p^r \epsilon \alpha^p$. Conjugation gives us

$$x + \zeta_p^i y \equiv \zeta^r \epsilon \alpha$$

and

$$x + \zeta_p^{-i} y \equiv \zeta^{-r} \epsilon \alpha$$

modulo $p\mathbb{Z}[\zeta_p]$. Hence

$$\zeta_p^{-r}(x + \zeta_p^i y) \equiv \zeta^r(x + \zeta_p^{-i} y) \pmod{p\mathbb{Z}[\zeta_p]}.$$

We can conclude the proof from the following lemma.

Lemma 1.4.3. *If $\alpha = a_0 + \cdots + a_{p-1}\zeta_p^{p-1}$, $a_i \in \mathbb{Z}$ not all zero, and if $\alpha \in m\mathbb{Z}[\zeta_p], m \in \mathbb{Z}$, then $m | a_i$ for all i.*

□

2 Review of Local Fields, 8/25/16

2.1 Locla Fields Facts

Let K be a field, then absolute value on K is a map to $\mathbb{R}^{\geq 0}$ that is multiplicative, satisfies the triangle inequality and is positive semi-definite. Includes for instance the p-adic norm, archimedean absolute values.

Definition 2.1.1. *Absolute value is <u>non-archimedean</u> if $|x + y| \leq \max(|x|, |y|)$.*

In non-archimedean fields, we talk about valuations, i.e. maps $v : K \to \mathbb{R} \cup \{\infty\}$ which is additive, i.e. $v(x + y) \geq \min(v(x), v(y))$ and $v(0) = \infty$. For instance, $v(p^n \frac{a}{b}) = n$.

Definition 2.1.2. *Given a non-archimedean valuation, let*

$$\mathcal{O}_v = \{x \in k | |x| \leq 1\}$$
$$\mathfrak{m}_v = \{x \in k | |x| < 1\}$$
$$\mathcal{O}_v^{\times} = \{x \in k | |x| = 1\}$$

Lemma 2.1.3. $|\cdot|_v$ *is discrete if and only if* $\mathfrak{m}_v$ *is principal.*

For example, $\mathbb{Q}_p, |\cdot|_p$ is discrete, and $|\mathbb{Q}_p \setminus 0| = p^{\mathbb{Z}}$. However, $\overline{\mathbb{Q}_p}$ with $|\cdot|_p$ is non-discrete, since $|p^{1/n}| = p^{-1/n} \to 1$.

Remark 3. *Any* $|\cdot|$ *on* k *topologizes* k*.*

Lemma 2.1.4. *If* $|\cdot|, |\cdot|^{\mathfrak{p}}$ *are absolute values on* k*, then TFAE:*

(1) they define the same topology

(2) $\mathcal{O}_{|\cdot|} = \mathcal{O}_{|\cdot|^{\mathfrak{p}}}$

(3) $|x| = (|x|^{\mathfrak{p}})^r$*, some* $r \in R$*.*

Theorem 2.1.5 (Ostrowski)**.** *The only absolute values on* $\mathbb{Q}$ *are the usual one and the* p*-adic ones.*

Theorem 2.1.6 (Weak Approximation)**.** *Let* $|\cdot|_1, ..., |\cdot|_n$ *be pairwise inequivalent absolute values on* k*. Then*

$$k \hookrightarrow \prod_{i=1}^{n} k_{|\cdot|_i}$$

is dense, where the subscripts indicate completions with respect to those absolute values.

Proof. First, we claim that there exists $a \in k$ with $|a|_1 > 1$ and $|a|_i < 1$ for the other i. Work by induction. This is clearly true for $n = 1$. For $n = 2$, if $|\cdot|_1 \ncong |\cdot|_2$ then there are b, c such that $|b|_1 < 1, |b|_2 \geq 1$, $|c|_1 \geq 1, |c|_2 < 1$. Then let $a = b/c$. By indcution, there's $b \in k$ such that $|b|_1 > 1, |b|_i < 1$ and (by $n = 2$ case), $|c| > 1, |c|_n < 1$. If $|b|_n < 1$, we're done. If $|b|_n = 1$, set $a = cb^m$ for m large enough. Otherwise, set $a = cb^m/(1 + b^m)$. Done.

Next, we show that for any $\epsilon > 0$, there is an $\alpha \in k$ such that $|a - 1|_1 < \epsilon$ and $|a|_i < \epsilon$. Take a as above, i.e. $\alpha^m/(1 + \alpha^m)$ for $m >> 0$.

Let $x_1, ..., x_n \in k$. For each i, choose $|\alpha_i - 1|_i$ very small, $|\alpha_i|_{j \neq i}$ very small, and set $x = \sum x_i \alpha_i$. $\square$

2.2 Hensel's Lemma

Let $\mathcal{O}$ be a complete discrete valuation ring (e.g. any local ring). We want to discuss Hensel's lemma.

Theorem 2.2.1 (Version 1)**.** *Let $f(x) \in \mathcal{O}[X]$. Let $a_0 \in \mathcal{O}$ be such that $|f(a_0)| < |f^{\mathfrak{p}}(a_0)|^2$. Then there is a root $a \in \mathcal{O}$ of f such that $|a - a_0| < |f(a_0)/f^{\mathfrak{p}}(a_0)^2|$.*

Proof. Literally Newton's method. □

For example, if $\mathcal{O} = \mathbb{Z}_5$ and $f(X) = X^3 + X + 3$, then $f(1) \equiv 0 \pmod 5$, $f^{\mathfrak{p}}(1) \equiv 4 \pmod 5$. Then we can let $a_1 = a_0 - f(a_0)/f^{\mathfrak{p}}(a_0) \equiv 6 \pmod 2 5$.

Important Example. If $\mathcal{O} = \mathbb{Z}/p\mathbb{Z}$, and $f(X) = X^p - X$, then for any $a \in \mathbb{F}_p$, $f(a) \equiv 0 \pmod p$, and $f^{\mathfrak{p}}(a) \equiv -1 \pmod p$. Then there exists an $a* \in \mathbb{Z}/p\mathbb{Z}$ such that $a* \equiv a \pmod p$, $f(a) = 0$. Hence we can conclude that the p-th roots of unity are contained in $\mathbb{Q}_p$ and reduction mod p is a group isomorphism from $\mu_{p-1}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{F}_p^\times$. The inverse of this map is called the Teichmuller lift.

In general, if $\mathcal{O}$ is a discrete valuation ring, with finite residue field k, then $\mu_{|k|-1}(\mathcal{O}) \cong k^\times$.

Theorem 2.2.2 (Version 2)**.** *Let $\mathcal{O}$ be a DVR with residue field $k = \mathcal{O}/\mathfrak{m}$. Let $f(X) \in \mathcal{O}[X]$. If $\bar{f}(X) \in k[X]$ factors as $g_0(X)h_0(X)$ with g_0, h_0 monic and coprime, then $f(X) = g(X)h(X)$ for unique monic $g, h \in \mathcal{O}[X]$ such that $g \equiv g_0, h \equiv h_0 \pmod{\mathfrak{m}}$.*

2.3 Extension of Valuations

Proposition 2.3.1. *Let k be complete with respect to a discrete $|\cdot|_v$. Let L/K be a finite separable extension. Then $|\cdot|_v$ extends uniquely to L, L is complete with respect to this extension, and for every $\alpha \in L$, $|\alpha|_v := |N_{L/K}(\alpha)|^{1/[L:K]}$.*

Proof. If both were an extension, then since all norms on a finite dimensional vector space over a complete field are equivalent, they define the same topology and so the exponent must be equal.

To prove existence, note that there is a unique maximal ideal $\mathfrak{m}_L$ of $\mathcal{O}_L$ above that of $\mathcal{O}_k$. You can define a valuation upstairs by defining one on the maximal ideal, then normalize. □

Remark 4. *The formula is forced by existence of uniqueness. If L/K is a Galois extension, $|\sigma(\cdot)|$ is another absolute value, so $|\sigma(\cdot)| = |\cdot|$ by uniqueness, and take the product over all elements of the Galois group.*

Suppose k is complete with respect to the discrete, non-archimedean valuation. Let L/K be a finite separable extension. Let v_k be the normalized valuation on k, i.e. $v : k \twoheadrightarrow \mathbb{Z}$. Let π_k be the generator of the maximal ideal of $\mathcal{O}_k$ (a uniformizing element). Let $w : L \to \mathbb{R}$ be the unique extension of v_k to L.

Definition 2.3.2. *Let* $e_{L/K} = [w(L^\times) : v_k(k^\times)]$*, i.e.* $\pi_k \mathcal{O}_L = \pi_L^{e_{L/K}}$*, be the* *ramification degree. Let* $f_{L/K} = [k_L : k_k]$ *be the degree of the residue field extension be called the* *inertial degree.*

Example. If $L = \mathbb{Q}_p(\sqrt{p})$, $e_{L/K} = 2, f_{L/K} = 1$.

Example. Let $L = \mathbb{Q}_p(\zeta)$ where $\zeta^{p^2-1} = 1$, and $\zeta^{p-1} \neq 1$. Then $e_{L/K} = 1, f_{L/K} = 2$. Minimal polynomial is $(X - \zeta)(X - \zeta^p)$.

Definition 2.3.3 (Purist's). *A local field is a field with nontrivial absolute value inducing a locally compact topology on* k*.*

Definition 2.3.4. *Namely, it is either* $\mathbb{R}, \mathbb{C}$ *in the archimedean case, or in the non-archimedean case, a finite extension of* $\mathbb{Q}_p$ *or* $\mathbb{F}_p((T))$*.*

Note that k is complete with respect to non-archimedean absolute value if and only if the residue field is finite and $\mathcal{O}_K$ is compact.