Class Field Theory

David Wiedemann

Table des matières

List of Theorems

Lecture 1: Intro Mon 10 Oct

1 Motivation

Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial and a p a prime.
Look at $f_p(x) \in \mathbb{F}_p[x]$, in general, f_p is not irreducible so we can study it's factorizations.

Definition 1
We say f splits completely mod p if f_p factors into distinct linear factors.
We write $Spl(f) = \{p | f_p = \prod(x - \alpha_i)\alpha_i \neq \alpha_j \forall i \neq j\}$

Problem
Given f, describe the factorisations behaviour of f_p as a function of p.
Or at least give a rule determining $Spl(f)$.

An answer to this illposed problem is a **Reciprocity Law**.

Example
Let $f(x) = x^2 - q$ $q > 2$ prime.
Observe that

1. $f_p(x) = (x - \alpha_p)^2$, *but this happens iff* $p = 2, q$
2. $f_p(x) = (x - \alpha_p)(x + \alpha_p)$ *iff* $p \in Spl(f)$ *iff* $(\frac{q}{p}) = 1$
3. $f_p(x)$ *is irreducible iff* $(\frac{q}{p}) = -1$

To get a rule, we need to compute $\left(\frac{q}{p}\right)$, to do so, we use quadratic reciprocity.
For us, quadratic reciprocity translates to

Corollary 2

$$(\frac{q}{p}) = \begin{cases} (\frac{p}{q}) \text{ if } p \equiv 1 \mod 4 \\ -(\frac{p}{q}) \text{ if } p \equiv 3 \mod 4 \end{cases}$$

So $Spl(X^2 - q)$ is determined by congruence conditions modula $4q$.

Example
Let Φ_n be the nth cyclotomic polynomial, then

$$Spl(\Phi_n) = \{p | p \equiv 1 \mod n\}$$

What about general polynomials?
Over $\mathbb{C}$, we can always factor polynomials and so we write $K_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$

for the splitting field of K_f over $\mathbb{Q}$.
$K_f \supset \mathbb{Q}$ is a Galois extension and $\mathcal{O} = \mathcal{O}_{K_f}$ is it's ring of integers.
As $\mathcal{O}$ is a dedekind domain, we have

$$p\mathcal{O} = \prod_{i=1}^{n} \beta_i^e, \mathcal{O}/_{\beta_i} \supset \mathbb{Z}/(p) \text{ a finite extension of } \mathbb{Z}/p$$

We understand finite extensions of $\mathbb{F}_p$, there Galois group is generated by the Frobenius automorphism.
If p does not ramify ($e_p = 1 \iff p \not| D_{K_f}$) then we define the Artin-Symbol $\sigma_{\beta_i} \in Galf(K_f|\mathbb{Q})$ by

$$\sigma_{\beta_i}(\alpha) \equiv \alpha^p \mod \beta_i \forall a \in \mathcal{O}$$

<u>Fact</u> :
If $\beta_i \neq \beta_j$, then there is $\zeta \in Gal(K_f|\mathbb{Q})$ such that $\zeta(\beta_i) = \beta_j$, then $\sigma_{\beta_j} = \zeta\sigma_{\beta_i}\zeta^{-1}$.
The Artin symbol of p is $\sigma_p = C_{\mathrm{Gal}}(\sigma_{\beta_i})$.
For now we suppose $Gal(K_f|\mathbb{Q})$ is an abelian group, in this case, we can turn the Artin Symbols into a map

$$\mathbb{Q}^* \supset \Gamma_{D_{K_f}} = \langle p \not| D_{K_f} \rangle \to \mathrm{Gal}(K_f|\mathbb{Q})$$

by sending $p \to \sigma_p$

Lemma 4
If $Gal(K_f|\mathbb{Q})$ is abelian, then, up to finitely many extensions,

$$p \in Spl(f) \iff \sigma_p = 1$$

Theorem 5 (Artin Reciprocity)
For $K_f/\mathbb{Q}$ abelian, the Artin map $\sigma : \Gamma_{D_{K_f}} \to \mathrm{Gal}(K_f|\mathbb{Q})$ is surjective and it's kernel contains the "ray class group".

Here the ray class group is

$$\Gamma_a^{(ray)} = \left\{ r \in \mathbb{Q}^* | r = \frac{c}{d}(ca, d) = 1, c \equiv d \mod a \right\}$$

For a suitable a tant consists of ramified primes.
Define $\tilde{Spl}(f) = Spl(f) \setminus \{p|a\} \cup \{p \equiv 1 \mod a\}$.

Theorem 6 (Abelian polynomial theorem)
If f is abelian, then $\tilde{Spl}(f)$ can be described by congruence conditions wrt a modulus depending only on f.

Conversely, if $\tilde{Spl}(f)$ *is described by congruence conditions, then* $\mathrm{Gal}(K_f|\mathbb{Q})$ *is abelian.*

Theorem 7
Let f, g *be polynomials (monic irreducible), then*

$$K_f \subset K_g \iff Spl(g) \subset^* Spl(f)$$

This enters in the proof of the converse part of the abelian polynomail theorem.

2 Interlude : Inverse Limits

Let I be a directed ordered set ($i, j \in I \implies \exists k$ such that $i \leq k, j \leq k$)

Definition 2 (Inverse System)
A inverse system consists of data

$$\{X_i, f_{i,j} | i, j \in I, i \leq j\}$$

X_i *are objects (topological spaces, groups, etc) and the* $f_{i,j} : X_j \to X_i$ *such that* $f_{i,i} = \mathrm{Id}$ *and* $f_{j,k} \circ f_{k,i} = f_{j,i}$

Example
Take $X_i = \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}, i \leq j$.
Then, the inverse limit is defined by

$$X = \varprojlim_{i \in I} X_i = \left\{(x_i) \in \prod X_i | f_{ij}(x_j) = x_i \forall i \leq j\right\} \subset \prod_{i \in I} X_i$$

Lecture 2: Infinite galois theory

Thu 13 Oct

3 Galois Theory and profinite groups

Example
$\mathbb{F}_p \subset \mathbb{F}_{p^n} \subset \overline{\mathbb{F}_p}$.
Though the extension is infinite, we can look at $\mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$ *and it still contains the frobenius* $\phi(x) = x^p$.
Let $H = \{\phi^n | n \in \mathbb{Z}\} = \langle \phi_n \rangle \subset \mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$.
Note that $\overline{\mathbb{F}_p}^H = \mathbb{F}_p$ *BUT* $H \subsetneq \mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$

Lemma 10
Let T be a Hausdorff topological space.
The following are equivalent

- *T is an inverse limit of finite discrete spaces*
- *T is compact and every point in T has a basis of neighborhoods of subsets that are clopen*
- *T is compact and totally disconnected*

Proof (Sketch)
$1 \implies 2$ *follows from construction (exercise)*
$2 \implies 3$ *Take $x \in T$ and let C_x be the connected component of x.*
Then

$$C_x = \bigcap_{x \in U,\ clopen} U = \{x\}$$

because X is Hausdorff.
$3 \implies 1$ *Let* $I = \left\{ \text{equivalence relation } R \subset T \times T | {}^{T}\!/_{R} \text{ is finite discrete} \right\}$
.
Then, consider $\phi : T \to \varprojlim {}^{T}\!/_{R}$, one then checks this is a homeomorphism. (exercise again) $\square$

Definition 3 (Profinite space)
A profinite space is a totally disconnected, compact and Hausdorff space.

Lemma 11
Let G be a Hausdorff topological group.
Then the following are equivalent

- *G is the inverse limit of discrete finite groups*
- *G is compact and the identity in G has a basis of neighborhoods consisting of normal clopen subgroups.*
- *G is compact and totally disconnected.*

Proof
$1 \implies 3$ *see course notes*
$2 \implies 1$ *We want to show that $\phi : G \to \varprojlim {}^{G}\!/_{U}$ where the limit is taken over all normal clopen subgroups.*
$3 \implies 2$ *We take a basis for e as in the lemma above.*
We take a basis of clopen neighborhoods U and then define

$$V = \{v \in U | Uv \subset U\} \text{ and } H = \left\{h \in V | h^{-1} \in V\right\}$$

and one can show that H is a normal finite subgroup of finite index. $\square$

Definition 4 (Profinite group)
A totally disconnected compact Hausdorff topological group is called a profinite group.

Example

— $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$
— $\hat{\mathbb{Z}} = \lim_{n\in\mathbb{N}} \mathbb{Z}/N\mathbb{Z}$ *where the inverse system is given by divisibility*

Now we try to fix the fundamental theorem of Galois theory.
Let F be a field with algebraic closur $\overline{F}$.
Write $G_E = \mathrm{Gal}(\overline{F}|E)$ for a field extension $F \subset E \subset \overline{F}$.
In particular, G_F is just the absolute Galois group of F

Definition 5 (Krull Topology)
For some element $\sigma \in G_F$, define a absis of (open) neighborhoods to be

$$\{\sigma G_E | F \subset E \text{ finite normal }\}$$

Proposition 13
G_F equipped with the Krull topology is a profinite group. We have

$$G_F = \varprojlim \mathrm{Gal}(E/F)$$

where E runs over finite Galois extensions of E

Corollary 14
$G_{\mathbb{F}_p} \simeq \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \hat{\mathbb{Z}}$

Theorem 15 (Fundamental Theorem of Galois Theory (Cool version))
The assignment

$$K \to \mathrm{Gal}(\overline{F}|K)$$

is a one-to-one correspondence between extensions $F \subset K \subset \overline{F}$ and closed subgroups of G_F.
The open subgroups of G_F correspond to finite extensions of F.

Proof

1. *First, notice that an open subgroup of G_F is closed.*
2. *Finite extensions correspond to open subgroup (essentially by definition, one needs to take the normal closure)*

3. *Now, for an arbitrary field extensionf*

$$\mathrm{Gal}(\overline{F}|K) = \bigcap_i \mathrm{Gal}(\overline{F}|K_i)$$

as K_i varies over all finite subextensions of K

4. *This assignment is injective as K is the fixed field of* $\mathrm{Gal}(\overline{F}|K)$

5. *This assignment is surjective :*
Take $H \subset G_F$ a closed subgroup and let $K = \overline{F}^H$, so that $H \subset$ $\mathrm{Gal}(\overline{F}|K)$.
To see that this is in fact an equality, we take $\sigma \in \mathrm{Gal}(\overline{F}|K)$ and we show that $\sigma \in \overline{H} = H$.
Take some finite extension $K \subset L \subset \overline{F}$ so that $\sigma\,\mathrm{Gal}(\overline{F}|L)$ is a neighborhood of σ.
We need to show that

$$H \cap \sigma\,\mathrm{Gal}(\overline{F}|L) \neq \emptyset$$

To do this, we have to show $\tau \in H$ such that $\tau|_L = \sigma|_L$.

$$p : G_K \to \mathrm{Gal}(L/K)$$

□

is surjective and $p(H) \subset \mathrm{Gal}(L/K)$.
Since K is the fixed field of H, $L^{p(H)} = K$, we have $p|_H : H \to$ $\mathrm{Gal}(L/K)$ *is surjective.*

4 Local Fields

Example

$\mathbb{R}$ and $\mathbb{C}$ are local fields for us

Definition 6 (Local Field)
A local field is a topological field which is locally compact but not discrete.

Definition 7
Let F be a field. An absolute value on F is a map $|\cdot| : F \to \mathbb{R}$ such that

1. $|x| \geq 0$ *and* $|x| = 0$ *and* $|x| = 0 \iff x = 0$
2. $|xy| = |x||y|$
3. $|x + y| \leq |x| + |y|$

Example

— *$\mathbb{R}$ and $\mathbb{C}$ with euclidean norm*

— *If $\mathcal{O}$ is a DVR, $F = \frac{(}{\mathcal{O}})$, then $|x| = c^{-\nu(x)}$ with $c > 1$ defines an absolute value.*

—

Lecture 3: Local Fields

Mon 17 Oct

Remark

1. *On a local field, we get a metric $d(x, y) = |x - y|$ which induces a topology on our field F*
2. *We could define the discrete metric which induces the discrete topology, but we always exclude it*

Definition 8 (Equivalent metrics)

1. *We call $|\cdot|_1$ and $|\cdot|_2$ equivalent if they induce the same topology.*
2. *If $|x + y| \leq \max(|x|, |y|) \leq |x| + |y|$ holds, then we call $|\cdot|$ non-archimedean.*

Observe that, if $|\cdot|_1$ and $|\cdot|_2$ are equivalent absolute values, then

$$|x|_1 < 1 \implies x^n \to 0 \text{ in } |\cdot|_1 \implies x^n \to 0 \text{ in } |\cdot|_2 \implies |x|_2 < 1.$$

Proposition 19

Two absolute values $|\cdot|_1, |\cdot|_2$ are equivalent iff there is $s > 0$ such that

$$|\cdot|_1 = |\cdot|_2^s$$

Proof

The implication from right to left is easy.
Fix $y \in F^\times$ with $|y|_1 > 1$.
For any $x \in F^\times$ there is $\alpha \in \mathbb{R}$ such that

$$|x|_1 = |y|_1^\alpha$$

Take a rational approximation from above $\frac{m_i}{n_i} \to \alpha$, we get $|\frac{x^{n_1}}{y^{m_1}}|_1 < 1 \implies |\frac{x^{n_1}}{y^{m_1}}|_2 < 1$
Thus $|x|_2 \leq |y|_2^{\frac{m_i}{n_i}} \implies |x|_2 \leq |y|_2^\alpha$.
Doing the same with an approximation of α from below we get $|x|_2 = |y|_2^\alpha$.
Then

$$0 < s = \frac{\log |y|_1}{\log |y|_2} = \frac{\log |x|_1}{\log |x|_2}$$

□

Theorem 20 (Approximation Theorem)
Let $|\cdot|_1, \ldots, |\cdot|_n$ be pairwise inequivalent absolute values.
For all $a_1, \ldots, a_n \in F$ and every $\epsilon > 0$, there is $x \in F$ such that

$$|x - a_i|_i < \epsilon$$

Remark
Taking $F = \mathbb{Q}$ and p, q primes.
There are valuations v_p, v_q which induce absolute values $|\cdot|_p = p^{-v_p(\cdot)}$ which are non-archimedean and inequivalent.
A special case of the theorem above says that for each $a_1, a_2 \in \mathbb{Z}$ and all $\epsilon > 0$ there is $x \in \mathbb{Q}$ such that $|a_1 - x|_p < \epsilon$ and $|a_2 - x|_q < \epsilon$

Proof
We claim : There is $z \in F$ such that $|z|_1 > 1$ and $|z|_j < 1$ for $j = 2, \ldots, n$.
First, take $\alpha, \beta \in F$ such that

$$|\alpha|_1 < 1 \leq |\alpha|_n \text{ and } |\beta|_1 \geq 1 > |\beta|_n$$

Put $y = \frac{\beta}{\alpha}$.
The case $n = 2$ follows from this (with $z = y$).
By induction, for $n > 2$ we argue by induction. Say z' satisfies the claim for $n - 1$.
If $|z'|_n \leq 1$, take $z = (z')^m y$ for m large enough.
If $|z'|_n > 1$, look at

$$t_m = \frac{(z')^m}{1 + z'^m}$$

t_m will converge to 1 for $j = 1, n$ and 0 if not.
Take $z = t_m y$ for m large enough.
By the same argument we find $z_i \in F$ such that $|z_i|_i > 1$ and $|z_i|_j < 1$ for $j \neq i$.
Put $x = a_1 z_1^{m_1} + \ldots + a_n z_n^{m_n}$ for $m_1, \ldots, m_n \in \mathbb{N}$ large enough. Look at script here :

$$|x - a_1|_1 \leq |a_1|_1$$

□

Proposition 22
An absolute value $|\cdot|$ on a field F is non-archimedean iff $(|n|)_{n \in \mathbb{N}}$ is bounded.

Proof
" $\implies$ " $|n| = |1 + \ldots + 1| \leq \max(|1|, \ldots) = 1$
" $\impliedby$ " Say $|n| \leq N$, look at $|x + y|^l \leq \sum_{v=0}^{l} |\binom{l}{v}| \underbrace{|x|^v |y|^{l-v}}_{\leq \max(|x|,|y|)^l}$.
Taking l-th roots, we get $|x + y| \leq N^{\frac{1}{l}} (1 + l)^{\frac{N}{l}} \max(|x|, |y|)$

□

Definition 9 (Complete Field)
We call $(F, |\cdot|)$ complete if every Cauchy sequence has a limit in F.

Any valued field has a completion $(\hat{F}, |\cdot|)$.

Example
$(\mathbb{Q}, |\cdot|) \xrightarrow{completion} (\mathbb{R}, |\cdot|_\infty)$.
We can do the same for the p-adic absolute values $(\mathbb{Q}, |\cdot|_p) \xrightarrow{completion} (\mathbb{Q}_p, |\cdot|_p)$.

Theorem 24 (Ostrowski)
Let F be a complete valued field such that $|\cdot|$ is archimedean.
Then there is an isomorphism $\sigma : F \to \mathbb{R}$ or $\mathbb{C}$ such that $|x| = |\sigma(x)|_\infty^s \forall x \in F$

Proof
As $|\cdot|$ is archimedean, the sequence (n) is unbounded and hence $char(F) = 0$.
Hence $\mathbb{Q} \to \hat{\mathbb{Q}} \to F$ and thus $\mathbb{R} \subset F$.
Take $a \in F$, we want to find a quadratic polynomial in $\mathbb{R}[x]$ that a satisfies.
Define $f(z) = |a^2 - Tr_{\mathbb{C}|\mathbb{R}}(z)a + Nr_{\mathbb{C}|\mathbb{R}}(z)$ for $z \in \mathbb{C}$.
Note that $f : \mathbb{C} \to [0, \infty)$ and $f(z) \to \infty$ as $|z| \to \infty$.
So $m = \min_{z\in\mathbb{C}} f(z)$ is attained in $S = \{z \in \mathbb{C} | f(z) = m\}$.
We claim $m = 0$.
Take $z_0 \in S$ and suppose $m = f(z_0) > 0$, consider

$$g(x) = x^2 - Tr_{\mathbb{C}|\mathbb{R}}(z_0)x + Nr_{\mathbb{C}|\mathbb{R}}(z_0) + \epsilon \in \mathbb{R}[x]$$

Let z_1, z_1' be complex roots of g, we must have

$$z_1 z_1' = Nr_{\mathbb{C}|\mathbb{R}}(z_0) + \epsilon$$

and in particular $|z_1| > |z_0|$.
Consider $G(x) = [g(x) - \epsilon]^n - (-\epsilon)^n = \prod_{i=1}^n (x - \alpha_i)$ and assume $\alpha_1 = z_1$

$$|G(a)|^2 = \prod_{i=1}^{2n} f(\alpha_i) \geq f(z_1)|m|^{2n-1}$$

and

$$|G(a)| \leq f(z_0)^n + \epsilon^n = m^n + \epsilon^n$$

Rearranging

$$\frac{f(z_1)}{m} \leq (1 + (\frac{\epsilon}{m})^n)^2 \to 1$$

as $n \to \infty$.
Rearranging $f(z_1) \leq m = f(z_0)$ □

Definition 10
The fields $\mathbb{R}$ and $\mathbb{C}$ are called archimedean local fields.

Let $|\cdot|$ be non-archimedean

Definition 11
Let $\mathcal{O} = \{x \in F||x| \leq 1\}$ be the " valuation ring ".
Then

$$p = \{x \in F||x| < 1\}$$

is the unique maximal ideal of p.
Then $\mathcal{O}^\times = \{x \in F||x| = 1\}$ are the units and $k = \mathcal{O}/p$ is the residue field.

Definition 12 (Non-archimedean local field)
A non-archimedean local field is a complete valued field such that $|\cdot|$ is non-archimedean and k is finite.

Definition 13
The valuation v defined by $v(x) = -\log(|x|)$ is called discrete if there is a $s > 0$ such that $v(F^\times) \subset s\mathbb{Z}$.
We say v is normalized if $v(F^\times) = \mathbb{Z}$

Proposition 25
Let $(F, |\cdot|)$ be a non-archimedean valued field with completion $(\hat{F}, |\cdot|)$, then

$$\hat{\mathcal{O}}/\hat{p} \simeq \mathcal{O}/p$$

Further, if $|\cdot|$ has discrete valuation then

$$\hat{\mathcal{O}}/\hat{p}^n \simeq \mathcal{O}/p^n \text{ and } \hat{\mathcal{O}} = \lim \mathcal{O}/p^n$$

Similarly

$$\hat{\mathcal{O}}^{\times = \lim \mathcal{O}^\times / U^n}$$

for $U^n = 1 + p^n$

Lecture 4: Local fields

Thu 20 Oct

Lemma 26 (Hensel)
Let $(F, |\cdot|)$ be a non-archimedean complete valued field.
Let $f \in \mathcal{O}[x]$ and assume $f = \overline{g}\overline{h} \mod p$ with $\overline{g}$ and $\overline{h}$ coprime over $\mathcal{O}/p[x]$, thenthis factorization lifts to $\mathcal{O}$ and $\exists g, h \in \mathcal{O}[x]$ such that $g \mod p = \overline{g}$, $h \mod p = \overline{h}$ $\deg g = \deg \overline{g}$

Proof
Let $d = \deg f, m = \deg \overline{g}$.
Define g_0 to be a lift of $\overline{g}$ to $\mathcal{O}[x]$ and h_0 a lift of h with same degree.
Look at $f - g_0h_0$, take $a, b \in \mathcal{O}[x]$ such that $ag - +bh_0 \equiv 1 \mod p\mathcal{O}[x]$ and look at $ag_0 + bh_0 - 1$.
Define ω to be any element of p that divides $f - g_0h_0, ag_0 + bh_0 - 1$.
We will construct (g_n, h_n) such that $\deg g_n = m$, $\omega^n | g_n - g_{n-1}$ and $\omega^n | h_n - h_{n-1}$ such that $\omega^{n+1} | f - g_nh_n$.
Suppose we've constructed g_{n-1}, h_{n-1} we want to find $g_n = g_{n-1} + \omega^n p_m$ and $h_n = h_{n-1} + \omega^n q_m$. We'll be able to take $\deg p_m < m$.
Write

$$\begin{aligned} f - g_nh_n &\equiv (f - g_{n-1}h_{n-1}) - \omega^n(p_nh_{n-1} + q_ng_{n-1}) \mod \omega^{n+1} \\ &\equiv \omega^n\left(\frac{f - g_{n-1h_{n-1}}}{\omega^n} - p_nh_{n-1} - q_ng_{n-1}\right) \end{aligned}$$

We work with ω now, so we want

$$p_nh_0 + q_mg_0 \equiv \underbrace{\frac{f - g_{n-1}h_{n-1}}{\omega^n}}_{=f_n} \mod \omega$$

We have $bh_0 + ag_0 \equiv 1 \mod \omega$ and thus

$$(bf_n)h_0 + (af_n)g_0 \equiv f_n \mod \omega \qquad \square$$

Write $bf_n = qg_0 + p_n$ with $\deg p_n < m$.
Letting $q_n := af_n + ph_0$, all the conditions hold and we get our g_n, h_n.
The factors of the respective sequences converge in $\mathcal{O}[x]$ because the coefficieents are Cauchy and $\mathcal{O}$ is complete.

Example

1. *If $f \in \mathcal{O}[x]$ and $\overline{a} \in \mathcal{O}/p$ such that $f(a) \equiv 0 \mod p, f'(a) \in \mathcal{O}^\times$ then $\exists a \in 0, a \equiv \overline{a} \mod p$ such that $f(a) = 0$*
2. *$f \in K[x]$ such that f is irreducible $f(0) \in \mathcal{O}$ then $f \in \mathcal{O}[x]$*

Theorem 28 (Classification of non-archimedean local fields)
The non-archimedean local fields are the finite extensions of $\mathbb{Q}_p$ *and* $\mathbb{F}_p((t))$

Theorem 29
Let $(F, |\cdot|)$ *be complete valued, then* $|\cdot|$ *has a unique extension to* $\overline{F}$.
If $E/F < \infty$, *then* $|\cdot|$ *is given by*

$$|\alpha|_E = |N_{E/F}(\alpha)|_F^{\frac{1}{[E:F]}}$$

and E *is again complete for* $|\cdot|$.

Proof
We can assume that F *is non-archimedean.*
It suffices to show $\exists!$ *extension to* E *(a finite extension).*

1. *Does* $|N_{E/F}|^{\frac{1}{[E:F]}}$ *define an absolute value ?*
   Multiplicativity and $\alpha = 0 \iff |\alpha| = 0$ *is clear.*
   We want to show that $|\alpha| \leq 1 \implies |\alpha + 1| \leq 1$.
   Fix such an α *and look at the minimal polynomial of* α, *say* f.
   Then $(f(0))^{\frac{1}{[E:F]}} = N_{E|F}(\alpha)$, *thus* $|f(0)|_F \leq 1, f(0) \in \mathcal{O}_F \implies f \in \mathcal{O}_F[x]$ *thus* $f \in \mathcal{O}_F[x]$.
   Hence $f(x-1) \in \mathcal{O}_F[x]$ *which is just the minimal polynomial of* $\alpha+1$, *thus* $N(\alpha+1) \in \mathcal{O}_F \implies |\alpha+1|_E \leq 1$
2. *We show uniqueness.*
   Suppose $|\cdot|'$ *is another absolute value on* E *extending* F.
   We'll show that $\mathcal{O}_E := \left\{\alpha \in E : N_{E|F}(\alpha) \in \mathcal{O}_p\right\} \subset \mathcal{O}'_E$.
   Suppose not, take $\alpha \in \mathcal{O}_E \setminus \mathcal{O}'_E$, *thus* $\alpha^{-1} \in p'_E$.
   Let f *be the minimal polynomial of* α, $f = x^d + a_{d-1}x^{d-1} + \dots$,
   $f(\alpha) = 0 \implies 1 + a_{d-1}\alpha^{-1} + \dots a_0\alpha^{-d} = 0 \in 1 + \mathcal{O}_F p'_E = 1 + p'_E \not\ni 0$.
   Thus $\mathcal{O}_E \subset \mathcal{O}'_E$.
   Thus $|\alpha|_E \leq 1 \implies |\alpha|'_E \leq 1$.
   Hence, if both norms were inequivalent, there would exist $\alpha \in E$ *with* $|\alpha| \leq \frac{1}{100}, |\alpha|' \geq 100$, *which is impossible.*

It now suffices to show that E *is a complete valued field.*
Fact : If F *is a complete valued field,* V *is a finite dimensional vector space over* F, *then any two norms on* V *are equivalent.*
We use this with $|\cdot|_E$ *and a norm coming from a linear isomorphism with* $F^{[E:F]}$ □

We now prove the classification of local fields

Proof

Fact : On $\mathbb{Q}$*, the non-archimedean absolute values are* $|\cdot|_p$ *(up to equivalence)*

Take F *a non-archimedean local field and suppose* $\mathbb{Q} \subset F$.

We know $|\cdot|_{\mathbb{Q}} = |\cdot|_p$ *for some* p *and thus* $\mathbb{Q}_p \subset F$.

Local compactness implies that $F/\mathbb{Q}_p < \infty$.

Assume $\mathrm{char} F = p > 0$*, thus* $\mathbb{F}_p \subset F$*, take* $t \in F$ *with* $|t| < 1$.

We claim that t *is transcendental, if not* $\exists N$ *such that* $t^N = 1 \implies |t| = 1$.

Thus $\mathbb{F}_p((t)) \subset F \implies F/\mathbb{F}_p((t)) < \infty$. □

Theorem 30

Let F *be a non-archimedean local field and* $\omega \in F^\times$ *a uniformizer for* $\mathcal{O}$.

Then $\mathcal{O}^\times \times \omega^{\mathbb{Z}} \to F^\times$ *is an isomorphism.*

Consider $1 \to \mathcal{O}^\times \to F^\times \to \mathbb{Z} \to 0$*, this ses splits with* $s : \mathbb{Z} \to F^\times$ *sending* n *to* ω^n.

Theorem 31

Let F *be a non-archimedean local field, then* $\mathcal{O}^\times \subset F^\times$ *is compact open and* $F^\times$ *is locally compact.*

Proof

Look at $F^\times \to \{(a,b) : ab = 1\} \subset F^2$ *sending* $a \to (a, \frac{1}{a})$.

We get everything just by topological considerations. □

Recall $U^n = 0$ if $n = 0$ and $1 + p^n$ if $n \geq 1$.
Then $\mathcal{O}^\times = \bigcup_{a \mod p \neq 0} a + p$.
All these p are open compact and thus $\mathcal{O}^\times$ is too.
Take $\alpha \in F^\times$, then $\alpha\mathcal{O}^\times$ is a compact open neighborhood of α.

Lemma 32

Let F *be a non-archimedean local field.*

The maps $x \to x^m$ *with* m *an integers sends* $U^m \to U^{n+v(m)}$ *and induces an isomorphism for* m *large enough (depending on* m*)*

Proof

Take $a \in U^n, a = 1 + \omega^n b$*, then* $a^m = 1 + m\omega^n b + \omega^{2n} c$ *for some* $c \in \mathcal{O}$.

$$= 1 + \omega^{v(m)}\omega^n b + \omega^{2n} c \in 1 + \omega^{v(m)+m}\mathcal{O}$$

for $n \geq v(M)$.

We show injectivity.

There exist finitely many n*-th roots of unity in* F.

For $n >> 1$, $U^n \ni$ *an* m*-th root of unity* $\neq 1$

To show surjectivity, take $a \in \mathcal{O}^\times$, we want to find $x \in \mathcal{O}$ such that

$$(1 + x\omega^n)^m = 1 + a\omega^{n+v(m)}$$

Thus $1 + b\omega^{v(m)}x\omega^n + \omega^{2n}f(x) = 1 + a\omega^{n+v(m)}$ where $m = b\omega^{v(m)}$.
$x + \omega^{n-v(m)}f(x) = a$ when $n > v(m)$.
Modulo ω, this becomes $x = a$.
By Hensel, this lifts to a solution $x \in \mathcal{O}$ because $(x-a)' = 1 \neq 0$. □

Corollary 33
Let F be non-archimedean local, then $(F^\times)^m \subset F^\times$ is an open subgroup.

$$\bigcap_m (F^\times)^m = \{1\}$$

Proof
It suffices to show $1 \in (F^\times)^m$ has an open neighborhood, indeed, take U^m a large enough n.
For the second part, take $a \in \bigcap_m (F^\times)^m$, $v(a) \in m\mathbb{Z}\forall m \implies v(a) = 0$ and we know that $a \in U^n$ for all n.
Thus $a - 1 \in \bigcap_i p^i = 0$ □

Lecture 5: Cohomology a la Tate

Mon 24 Oct

If F is a non-archimedean local field with normalized valuation v_f and E/F is a finite extension of degree n, then E is again a non-archimedean local field with respect to a unique absolute value extending $|\cdot|_F$.
The valuation associated to $|\cdot|_E$ is w_E and

$$|x|_E = |N_{E|F}(x)|^{\frac{1}{n}}$$

We have $\mathbb{Z} = v_F(F^\times) \subset w_e(E^\times) \subset \frac{1}{n}\mathbb{Z}$.
We have an extension of residue fields k_E/k_F

Definition 14
We define $e = e(E|F) = [\omega_E(E^\times) : v_F(F^\times)]$ and $f = f(E|F) = [k_E : k_F]$.

Proposition 34
Let $E|F$ be a finite extension of non-archimedean local fields.
Then $[E : F] = n = e \cdot f$

Remark
$n \geq e \cdot f$ holds in great generality (we don't need it to be a local field) but equality needs completeness.

Proof

Let ϖ_E *be a generator of* $p_E \subset \mathcal{O}_E$*.*
Choose $\omega_1, \dots, \omega_f \in \mathcal{O}_E^\times$ *such that they reduce to a basis of* k_E *over* k_F*.*
We claim that $\{\omega_j \varpi_E^i | j = 1, \dots, f \text{ and } i = 0, \dots, e-1\}$ *is linearly independent.*
Take

$$S = \sum_{i=0}^{e-1} \underbrace{\sum_{j=1}^{f} a_{ij}\, \omega_j \varpi_E^i}_{=S_i}$$

□

Suppose $S = 0$ *with the coefficents not all zero.*
Let $\alpha_i = \min_{j\in[f],a_{ij}\neq 0} v_F(a_{ij})$*.*
Then notice that $\varpi_F^{-\alpha_i} S_i$ *has at least one coefficient in* $\mathcal{O}_F^\times$*.*
Reducing $\mod p_E$ *gives a linear in* k_E $\sum_{j=1}^f \tilde{a_{ij}}\omega_j$ *and thus at least one of the* $\tilde{a_{ij}} \neq 0$*.*
Thus $S_i \neq 0$ *and even more* $w_E(S_i) \in v_F(F^\times)$*.*
Since $S = 0$ *there must be* $0 \leq i, j \leq e-1$ *with* $i \neq j$ *such that* $w_E(S_i \varpi_E^i) = w_E(S_j \varpi_E^j)$*.*
Thus $w_E(\varpi_E^i) \in w_E(\varpi_E^j) + \mathbb{Z}$*.*
But this can only happen if $i = j$*.*
Now, define $M = \sum_{i=0}^{e-1} \underbrace{\sum_{j=1}^{f} \mathcal{O}_F\omega_j\, \varpi_E^i}_{=N}$ *an* $\mathcal{O}_F$ *module.*
We claim that $M = \mathcal{O}_E$*.*
We start with some observations $\mathcal{O}_E = N + \varpi_E\mathcal{O}_E = N + \varpi_E N + \varpi_E^2 N + \ldots + \varpi_E^e \mathcal{O}_E = M + p_F\mathcal{O}_E$*.*
Thus $\mathcal{O}_E = M + p_F^v\mathcal{O}_E$ *for* $v \geq 1$ *and thus* M *is dense in* $\mathcal{O}_E$*.*
But M *is also closed*

Definition 15
If E/F *is a finite extension, then it is called unramified if* $[k_E : k_F] = n$ *(ie.* $e = 1$ *).*
A non-finite extension is called unramified if k_E/k_F *is separable and* E *is a union of finite unramified extensions.*

Proposition 36
Let E/F *and* F'/F *be two finite extensions of non-archimedean local fields and let* $E' = EF'$ *. Then*

— *E/F unramified, then E'/F' is unramified*
— *subextensions of unramified extensions are unramified*
— *compositions of unramified extensions are unramified.*

Proof
The second and third property follow from the first one, so we only show the first one.
k_E/k_F *is generated by* $\overline{\alpha}$.
We can lift $\overline{\alpha}$ *to* $\alpha \in \mathcal{O}_E$ *and take the minimal polynomial* $f \in \mathcal{O}_F[x]$ *for* α *over* F.
We compute $[k_E : k_F] \leq \deg(\overline{f}) = \deg f = [F(\alpha) : F] \leq [E : F] = [k_E : k_F]$.
Thus $E = F(\alpha)$ *and* $\overline{f}$ *is the minimal polynomial of* $\overline{\alpha}$ *and* $E = F'(\alpha)$.
Consider the minimal polynomial $g \in \mathcal{O}_{F'}[x]$ *of* α *over* F'.
Note that $\overline{g}$ *is irreducible by Hensel's lemma (and* $\overline{g}$ *has no multiple roots as* $\overline{g}|\overline{f}$*).*
Now $[k_E : k_{F'}] \leq [E' : F'] = \deg g = \deg \overline{g} - [k_{F'}(\overline{\alpha}) : k_{F'}] \leq [k_{E'} : k_{F'}]$ $\square$

Why are unramified extensions so nice ?

— If $E|F$ is unramified, then there is a morphism of galois groups $Gal(E/F) \to Gal(k_E|k_F)$ sending $\sigma \to \overline{\sigma}$ by defining $\overline{\sigma}(x + p_E) = \sigma(x) + p_E$ and this is an isomorphism.
  As $\mathrm{Gal}(k_E|k_F)$ is generated by the frobenius, sending $\overline{x} \to \overline{x}^{q_F}$ where $\#k_F = q_F$.

Definition 16
The automorphism $\phi_{E|F} \in \mathrm{Gal}(E|F)$ *that induces the frobenius via the isomorphism above is called the frobenius automorphism.*

Theorem 37
If $L \supset E \supset F$ *are unramified finite extensions of* F*, we have*

$$\phi_{E|F} = \phi_{L|F}|_E$$

and $\phi_{L|F}^{[E:F]} = \phi_{L|E}$

Interlude : Relevance to the classical situation

If $L|K$ is a finite extension of algbraic number fields and $p \in \mathcal{O}_K$.
Then this prime induces a normalized valuation v_p on K.
Let k_p be the completion and write $p\mathcal{O}_L = \beta_1^{e_1} \dots \beta_r^{e_r}$.
Then, we get valuations $\omega_{\beta_i} = \frac{1}{e_i} v_{\beta_i}$ extending v_p.
Completing with respect to these different valuations, we get L_i's for every i.
Then $f_j = f(L_j/K_p), e_i = e(L_i|K_p)$ and one has $\sum_{i=1}^r e_i f_i = n$.

If $L|K$ is a Galois extension, we obtain maps $L_\beta \to L_{\sigma\beta}$.

In particular, if $\sigma\beta = \sigma$, then $L_\beta \xrightarrow{\sigma} L_\beta$ defines an element in $\mathrm{Gal}(L_\beta/K_p)$.
And we get a morphism $G(\beta) = \{\sigma \in \mathrm{Gal}(L/K) | \sigma\beta = \beta\} \to \mathrm{Gal}(L_\beta|K_p)$.
If p is unramified, then this is an isomorphism and we can pull back the frobenius.

Lecture 6: Cohomology of groups

Thu 27 Oct

5 Cohomology of finite groups

Let G be a finite group.

Definition 17
A G-module A is an abelian group on which G acts

1. $1_G \cdot a = a$
2. $\sigma(a+b) = \sigma a + \sigma b$
3. $(\sigma\zeta)a = \sigma(\zeta a)$

Example

1. $\mathbb{Z}[G]$
2. *If $G = \mathrm{Gal}(L/K)$, then G acts on $L^\times$ and on L.*

The group ring has additional structure, there is a map.

$$\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$$

sending $\sum_{\sigma\in G} n_\sigma \sigma \to \sum_{\sigma \in G} n_\sigma$ called augmentation.
We call $I_G = \ker \epsilon$ the augmentation ideal.
There is the norm element $N_G = \sum_{\sigma\in G} \sigma$.
This gives rise to a map $\mu : \mathbb{Z} \to \mathbb{Z}[G]$ sending $n \mapsto n \times N_G$.
As any element acts trivially oon the norm, the image of μ is an ideal and we can form $J_G = {}^{\mathbb{Z}[G]}\!/_{\mathbb{Z}N_G}$.
We get two short exact sequences

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

and

$$0 \to \mathbb{Z} \xrightarrow{\mu} \mathbb{Z} \to J_G \to 0$$

Lemma 39

— *As a group, I_G is the free abelian group generated by $\sigma - 1$ as σ runs over $G \setminus 1$.*
— *As a group, J_G is the free abelian group generated by $\sigma \mod \mathbb{Z}N_G$*

as σ runs over $G \setminus 1$

— *We have* $\mathbb{Z}[G] \simeq I_G \oplus \mathbb{Z} \simeq J_G \oplus \mathbb{Z}$.

Proof

$$x = \sum_{\sigma \in G} n_\sigma \sigma = \sum_{1 \neq \sigma \in G} n_\sigma(\sigma - 1) + (\sum_{\sigma \in G} n_\sigma) 1_G = \sum_{1 \neq \sigma \in G} (n_\sigma - n_1)\sigma + n_1 N_G$$

□

Lemma 40

$I_G = Ann(\mathbb{Z}N_G)$ *and* $\mathbb{Z}N_G = Ann(I_G)$

Proof

$x = \sum_{\sigma \in G} n_\sigma \sigma \in \mathbb{Z}[G]$, *if* x *is in the annihilator,*

$$xN_G = \sum_\sigma n_\sigma \sigma N_G = \sum_\sigma n_\sigma N_G \implies (\sum_{\sigma \in G} n_\sigma) = 0$$

□

Definition 18 (Fixed module)

$A^G = \{a \in A | \sigma a = a \forall \sigma \in G\}$.

We also write

$$_{N_G}A = \{a \in A | N_G a = 0\}$$

and

$$I_G A = \left\{ \sum n_\sigma (\sigma a_\sigma - a_\sigma) | a_\sigma \in A, n_\sigma \in \mathbb{Z} \right\}$$

Definition 19

If A, B *are two* G*-modules, then we can turn* $\hom_{\mathbb{Z}}(A, B) (= \hom(A, B))$ *into a* G*-module by letting*

$$\sigma f = \sigma \circ f \circ \sigma^{-1}$$

In particular,

$$\hom_G(A, B) = \hom(A, B)^G$$

Definition 20

If A, B *are as before, then* $A \otimes B$ *is a* G*-module by* $\sigma(a \otimes b) = \sigma a \otimes \sigma b$

Remark

In general,

$$(A \otimes B)^G \neq A^G \otimes B^G$$

Remark

Given two G-homomorphisms $A \xrightarrow{h} A', B \xrightarrow{g} B'$, we get

$$(h, g) : \hom(A', B) \to \hom(A, B')$$

by pre/post-composition and

$$h \otimes g : A \otimes B \to A' \otimes B'$$

Definition 21 (Resolution)

Let G be a finite group. A complete free resolution of the (trivial) G-module $\mathbb{Z}$ is an exact sequence

$$\xleftarrow{d_{-2}} X_{-2} \xleftarrow{d_{-1}} X_{-1} \xleftarrow{d_0} X_0 \xleftarrow{d_1} X_1 \dots$$

of free G-modules X_q such that

$$X_0 \xrightarrow{\epsilon} \mathbb{Z} \xrightarrow{\mu} X_{-1}$$

is exact and fits into the above exact sequence.
All the maps are G-homomorphisms.

We define the following standard resolution

— $X_0 = X_{-1} = \mathbb{Z}[G]$

— $X_q = \bigoplus_{(\sigma_1, \dots, \sigma_q) \in G^q} \mathbb{Z}[G] \cdot (\sigma_1, \dots, \sigma_q) = X_{-q-1}$

To define our G-homomorphisms d_q, it suffices to define them on the generators.
We define $d_0(1) = N_G$ and $d_1(\sigma) = \sigma - 1$.
For $q > 1$, define

$$\begin{aligned} d(q)(\sigma_1, \dots, \sigma_q) = \sigma_1(\sigma_2, \dots, \sigma_q) \\ &+ \sum_{i=1}^{q-1} (-1)^i (\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma_{i+1}, \dots, \sigma_q) \\ &+ (-1)^q (\sigma_1, \dots, \sigma_{q-1}) \end{aligned}$$

Furthermore $d_{-1}(1) = \sigma_{\sigma \in G}[\sigma^{-1}(\sigma) - (\sigma)]$ and

$$\begin{aligned} d_{-q-1}(\sigma_1, \dots, \sigma_q) = \sum_{\sigma \in G} \sigma^{-1}(\sigma, \sigma_1) \\ &+ \sum_{\sigma \in G} \sum_{i=1}^{q} (-1)^i (\sigma_1, \dots, \sigma_{i-1}, \sigma_1 \sigma, \sigma^{-1}, \sigma_{i+1}, \dots, \sigma_q) \\ &+ \sum_{\sigma \in G} (-1)^{q+1} (\sigma_1, \dots, \sigma_q, \sigma) \end{aligned}$$

Lemma 43
This is a complete free resolution of $\mathbb{Z}$.

Proof
Nope. $\square$

Now, we are ready to define the (Tate) cohomology groups!
Define $A_q = \hom_G(X_q, A)$ (and call an element $x : X_q \to A$ in A_q a q-cochain).
We get a complex

$$\dots \xrightarrow{\partial_{-2}} A_{-2} \xrightarrow{\partial_{-1}} A_{-1} \xrightarrow{\partial_0} A_0 \xrightarrow{\partial_1} A_1 \to \dots$$

which is not necessarily exact but $\partial_{q+1} \circ \partial_q = 0$.
Now $Z_q = \ker \partial_{q+1}$ are the q-cocycles, $R_q = \operatorname{Im} \partial_q$ are q-coboundaries.
The qth cohomology group of the G-module A is the quotient $H^q(G, A) = {}^{Z_q}\!/\!_{R_q}$

Lecture 7: group cohomology

Mon 31 Oct

We'll write $A_q = \hom_G(X_q, A)$.
Recall $A_q = A_{-q-1} \simeq \{x : G \times \ldots \times G \to A\}$.
The maps ∂_q are given by
— $\partial_0 x = N_G x$ for $x \in A_{-1} = A$
— $[\partial_1 x](\sigma) = \sigma x - x$
— $\partial_{-1} x = \sum_{\sigma \in G} (\sigma^{-1} x(\sigma) - x(\sigma)) \in A$
— For $q \geq 1$,

$$\partial_q x(\sigma_1, \ldots, \sigma_q) = \sigma_1 x(\sigma_2, \ldots, \sigma_q) + \sum_{i=1}^{q-1} (-1)^i x(\sigma_1, \ldots, \sigma_i \sigma_{i+1}, \ldots, \sigma_q) + (-1)^q x(\sigma_1, \ldots, \sigma_{q-1})$$

— And

$$\partial_{-q-1} x(\sigma_1, \ldots, \sigma_q) = \sum_{\sigma \in G} [\sigma^{-1} x(\sigma, \sigma_1, \ldots, \sigma_q) + \sum_{i=1}^{q} (-1)^i x(\sigma_1, \ldots, \sigma_{i-1}, \sigma_i \sigma) + \ldots]$$

In low degree, we can compute these groups

1. $$H^{-1}(G, A) = {}^{\ker \partial_0}\!/\!_{\operatorname{Im} \partial_{-1}} = {}^{{}_{N_G}A}\!/\!_{I_G A}$$

2. $$H^0(G, A) = \frac{\ker \partial_1}{\operatorname{Im} \partial_0} = {}^{A^G}\!/\!_{N_G A}$$

3. Looking at 1-cocycles, we see that they are maps $x : G \to A$ with

$$\partial_2 x = 0 \iff x(\sigma\tau) = \sigma x(\tau) + x(\sigma)$$

If G operates trivialy on A, then these are just $\hom(G, A) = H^1(G, A)$.
In particular, if $A = {}^{\mathbb{Q}}\!/_{\mathbb{Z}} = \hom(G, {}^{\mathbb{Q}}\!/_{\mathbb{Z}}) = \chi(G)$ is the "character group".

In general, given an exact sequence $0 \to A \to B \to C \to 0$, then $0 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G, A)$ is exact.
The group $H^2(G, A)$ has the following interpretation, extensions $\hat{G}$ of a G module A by G are uniquely determined by a G-module structure on A and a class $x(\sigma, \tau)$ of "factor systems".
These factor systems are uniquely determined by elements in $H^2(G, A)$.
We have interpretations of $q = -1, 0, 1, 2$, later we will see what $q = -2$ does (under some mild assumptions).

5.1 The exact sequence of Cohomology

Given A, B two G-modules and $f : A \to B$ some G-hom, then this induces a map $\overline{f_q} : H^q(G, A) \to H^q(G, B)$ sending $[c] \to [f_q c]$.
We observe that $f_\bullet$ is indeed a chain-map.

Theorem 44
Let $0 \to A \to B \to C \to 0$ be exact.
Then there is a canonical homomorphism $\delta_q : H^q(G, C) \to H^{q+1}(G, A)$

Lecture 8: maps in cohomology

Mon 07 Nov

Theorem 45
Let A be a G-module, $H \subset G$ normal, then

$$0 \to H^1({}^G\!/_H, A^H) \xrightarrow{inf} H^1(G, A) \xrightarrow{res} H^1(H, A)$$

Proof
If $x : {}^G\!/_H \to A^H$ is a 1-cocyle, assume $inf(x) = \sigma a - a$ is a coboundary.
But then $(\sigma\tau a - a = \sigma a - a \forall \tau \in H)$ thus $a \in A^H$.
We check exactness at $H^1(G, A)$.
It is clear that $res \circ inf = 0$.
For the other inclusion, if $x : G \to A$ is a 1-cocycle such that $x(\tau) = \tau a - a$ with $a \in A$ for all $\tau \in H$.
Let $p : G \to A$ be defined by sending $\sigma \mapsto \sigma a - a$.
Put $x' = x - p$ and observe $x'(\tau) = 0$ for $\tau \in H, [x] = [x'] \in H^1(G, A)$.
Compute $x'(\sigma\tau) = x'(\sigma) + \sigma x'(\tau) = x'(\sigma)$ and $x'(\tau\sigma) = x'(\tau) + \tau x'(\sigma)$.
So we define $y : {}^G\!/_H \to A$ by $y(\sigma H) = x'(\sigma)$ □

Theorem 46
Let A be a G-module and $H \subset G$ normal.
Suppose $H^1(H,A) = 0$ for $i = 1, \ldots, q-1$, then

$$0 \to H^q({}^{G}\!/_{H}, A^H) \xrightarrow{inf} H^q(G,A) \xrightarrow{res} H^q(H,A)$$

is exact.

Proof
By induction on q , the case $q = 1$ follows from the above.
Consider

$$0 \to A \to \mathbb{Z}[G] \otimes A \to J_G \otimes A \to 0$$

We have that $0 \to A^H \to B^H \to C^H \to 0$ is exact because $H^1(H,A) = 0$.
We get a map of diagrams induced by connecting homomorphisms from

$$0 \to H^{q-1}({}^{G}\!/_{H}, C^H) \to H^{q-1}(G,C) \to H^{q-1}(H,C)$$

to

$$0 \to H^q({}^{G}\!/_{H}, A^H) \to$$

□

Lecture 9: stuff

Thu 10 Nov

Recall $H^q(G,A)$ are torsion groups, so there is a decomposiiton $\bigoplus_p H^q(G,A)_p$.

Theorem 47
Let A be a G-module and G_p a p-Sylow subgroup of G, then

$$Res_q H^q(G,A)_p \to H^q(G_p, A)$$

is injective and $Cores_q : H^q(G_p, A) \to H^q(G,A)_p$ is surjective.

Proof
$[G : G_p]$ is coprime to p, so

$$H^q(G,A)_p \xrightarrow{cores \circ Res} H^q(G,A)_p$$

is an automorphism as $coRes \circ Res$ is just multiplication by $[G : G_p]$.
So restriction is injective.
Orders of elements in $H^q(G_p, A)$ are powers of p so $cores(H^q(G_p, A)) \subset H^q(G,A)_p$.
Surjectivity follows as above. □

Corollary 48
Let G_p be a p-Sylow group for G.
Suppose that $H^q(G_p, A) = 0$, then $H^q(G, A) = 0$.

Proof
Because $Res : H^q(G, A) \to H^q(G_p, A)$ is injective. $\square$

Definition 22
Let G be a finite group, $H \subset G$ a subgroup. Then a G-module A is called ${}^{G}\!/_{H}$-induced if it has a representation

$$A = \bigoplus_{\sigma \in {}^{G}\!/_{H}} \sigma D$$

where $D \subset A$ is an H-module.

Theorem 49 (Shapiro's lemma)
Suppose $A = \bigoplus_{\sigma \in {}^{G}\!/_{H}} \sigma D$ is ${}^{G}\!/_{H}$-induced, then

$$H^q(G, A) = H^q(H, D)$$

Proof
Write ${}^{G}\!/_{H} = \{[\sigma_1], \dots, [\sigma_m]\}$.
For $q = 0$, we consider the map

$$A^G /_{N_G A} \xrightarrow{Res} A^H /_{N_H A} \xrightarrow{\pi} D^H /_{N_H D}$$

where π is induced by the projection onto $[e]D$.
This is an isomorphism with inverse sending $\nu : d + N_H D \mapsto \sum_{i=1}^m \sigma_i d + N_G A$.
One verifies that $\pi \circ Res \circ \nu = \mathrm{Id} = \nu \circ \pi \circ Res$.
For the general case, we want to shift dimensions

$$A^q = \begin{cases} J_G \otimes \ldots \otimes J_G \otimes A \text{ if } q \geq 0 \\ I_G \otimes \ldots \otimes I_G \otimes A \text{ if } q < 0 \end{cases}$$

,

$$D_*^q = \begin{cases} J_G \otimes \ldots \otimes J_G \otimes D \text{ if } q \geq 0 \\ I_G \otimes \ldots \otimes I_G \otimes D \text{ if } q < 0 \end{cases}$$

and

$$D^q = \begin{cases} J_H \otimes \ldots \otimes J_H \otimes D \text{ if } q \geq 0 \\ I_H \otimes \ldots \otimes I_H \otimes D \text{ if } q < 0 \end{cases}$$

Note $A^[]q = \bigoplus_{i=1}^{m} \sigma_i D^q_*$.
Compute that

$$J_G = J_H \oplus K_1 \text{ for } K_1 = \bigoplus_{\tau \in H} \tau \left(\sum_{i=2}^{m} \mathbb{Z}\sigma_i \right)$$
$$I_G = I_H \oplus K_{-1} \text{ for } K_{-1} = \bigoplus_{\tau \in H} \tau \left(\sum_{i=2}^{m} \mathbb{Z}(\sigma_i - 1) \right)$$

So $D^q_* = D^q \oplus C^q$ *where* C^q *is* H*-induced.*
We get the diagram

$$H^0(G, A^q) \xrightarrow{Res_0} H^0(H, A^q) \xrightarrow{\pi} H^0(H, D^q_*) \xrightarrow{p} H^0(H, D^q)$$

and then something happens... □

5.2 The cup-product

Let A, B be G-modules, there is a map

$$A^G \times B^G \to (A \otimes B)^G$$

and $N_G A \times N_G B \to N_G(A \otimes B)$.
We get an induced map

$$H^0(G, A) \times H^0(G, B) \xrightarrow{\cup} H^0(G, A \otimes B)$$

We call this the cup product.

Definition 23
There is a unique family of billinear maps

$$\cup : H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B)$$

called the cup product, satisfying

1. *For* $p = q = 0$ *it is the cup product defined above*
2. $H^p(G, A'') \times H^q(G, B) \to H^{p+q}(G, A'' \otimes B) \xrightarrow{\delta} H^{p+q+1}(G, A \otimes B)$
   and

   $$H^p(G, A^H) \times H^q(G, B) \xrightarrow{(\delta,1)} H^{p+1}(G, A) \times H^q(G, B) \xrightarrow{\cup} H^{p+q+1}(G, A \otimes B)$$

   where
   $$0 \to A \to A' \to A'' \to 0$$
   is exact and
   $$0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$$
   is too

3. *If* $0 \to B \to B' \to B'' \to 0$ *and* $0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$ *is exact, then*

$$H^p(G,A) \times H^q(G,B'') \xrightarrow{\cup} H^{p+q}(G,A \otimes B'') \xrightarrow{(-1)^p \delta} H^{p+q+1}(G,A \otimes B)$$

and

$$H^p(G,A) \times H^q(G,B'') \xrightarrow{(1,\delta)} H^p(G,A) \times H^{q+1}(G,B) \xrightarrow{\cup} H^{p+q+1}(G,A \otimes B)$$

Proof (Existence of the cup product)
Nope. □

Theorem 50
Let $f : A \to A', g : B \to B'$, *we have*

$$\overline{f}[a] \cup \overline{g}[b] = \overline{f \otimes g}([a] \cup [b])$$

Theorem 51
Let A, B *be* G*-modules,* $H \subset G$ *a subgroup.*
If $[a] \in H^p(G,A), [b] \in H^q(G,B), [c] \in H^q(H,B)$, *then*

$$Res([a] \cup [b]) = (Res[a]) \cup (Res[b])$$

and

$$Cores(Res[a] \cup [c]) = [a] \cup cores[c]$$

Theorem 52
Take $[a] \in H^p(G,A), [b] \in H^q(G,B), [c] \in H^r(G,C)$.
Then
— $([a] \cup [b]) \cup [c] = [a] \cup ([b] \cup [c])$
— $[a] \cup [b] = (-1)^{pq}[b] \cup [a]$

Lemma 53
$[a_1] \cup [b_{-1}] \in H^0(G, A \otimes B)$ *is given by*

$$\sum_{\tau \in G} a_1(\tau) \otimes \tau b_{-1}$$

Lecture 10: stuff

Mon 14 Nov

Proof

Consider

$$0 \to A \xrightarrow{i} A \otimes \mathbb{Z}[G] \to A'' \to 0$$

and

$$0 \to A \otimes B \xrightarrow{i'} A' \otimes B \to A'' \otimes B \to 0$$

two exact sequences.
Note $H^1(G, A') = 0$, *so* $i(a_1) = \partial a_0'$.
Put $a_0'' = j(a_0')$.
By definition of δ *we have* $[a_1] = \delta(a_0'')$.
Now we can compute

$$\begin{aligned}
[a_1] \cup [b_{-1}] &= \delta[a_0''] \cup [b_{-1}] \\
&= \delta([a_0''] \cup b_{-1}) \\
&= \delta([a_0'' \otimes b_{-1}]) \\
&= [\partial_0(a_0' \otimes b_{-1})] \\
&= [N_G(a_0' \otimes b_{-1})] \\
&= [\sum_{\tau \in G} a_1(\tau) \otimes \tau b_{-1}] + [a_0' \otimes N_G b_{-1}]
\end{aligned}$$

□

Lemma 54

$$[a_1] \cup [\sigma] = [z_{-1}] \in H^{-1}(G, A)$$

We can take $z_{-1} = a_1(\sigma)$

Proof

There is an isomorphism $H^{-1}(G, A) \simeq H^0(G, A \otimes I_G)$.
It suffices to show that $\delta([a_1] \cup [\sigma]) = \delta([a_1(\sigma)])$.
First, note that $\delta[a_1(\sigma)] = [x_0]$ *for* $x_0 = \sum_{\tau \in G} \tau a_1(\sigma) \otimes \tau$.
Recall that we have $\delta[\sigma] = [\sigma - 1] \in H^{-1}(G, I_G)$, *so*

$$\delta([a_1] \cup [\sigma]) = ([a_1] \cup \delta[\sigma]) = -[a_1] \cup [\sigma - 1] = [y_0]$$

We will use that a_1 *is a crossed homomorphism, we get*

$$\begin{aligned}
y_0 &= -\sum_{\tau \in G} a_1(\tau) \otimes \tau(\sigma - 1) \\
&= \sum_{\tau \in G} a_1(\tau) \otimes \tau - \sum_{\tau \in G} a_1(\tau) \otimes \tau\sigma
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\tau \in G} a_1(\tau) \otimes \tau - \sum_{\tau in G} a_1(\tau\sigma) \otimes \tau\sigma + \sum_{\tau \in G} \tau a_1(\sigma) \otimes \tau\sigma \\
&= \sum_{\tau \in G} \tau a_1(\sigma) \otimes \tau\sigma
\end{aligned}
$$

where we used that $a_1(\tau) = a_1(\tau\sigma) - \tau a_1(\sigma)$.
Finally, we can look at

$$y_0 - x_0 = \sum_{\tau \in G} (\tau a_1(\sigma) \otimes \tau(\sigma - 1)) = N_G(a_1(\sigma) \otimes (\sigma - 1))$$

hence $[x_1] = [y_0]$ □

Theorem 55

$$[a_2] \cup [\sigma] = \left[\sum_{\tau \in G} a_2(\tau, \sigma) \right] \in H^0(G, A)$$

Proof
As before, $A' = \mathbb{Z}[G] \otimes A$ and $0 \to A \to A' \to A'' \to 0$ exact.
Then $a_2 = \partial a_1', a_2(\tau, \sigma) = \tau a_1'(\sigma) - a_1'(\tau\sigma) + a_1'(\tau)$.
Then $[a_2] \cup [\sigma] = \delta([a_1''] \cup [\sigma]) = [\sum_\tau \tau a_1'(\sigma)] = [\sum_{\tau \in G} a_2(\tau, \sigma)] + [\sum_{\tau \in G} a_1'(\tau, \sigma) - \sum_{\tau \in G} a_1'(\tau)]$ □

5.3 Cohomology of (finite) cyclic groups

Let G be a cyclic group of order n with generator σ.
Now $\mathbb{Z}[G] = \bigoplus_{i=0}^{n-1} \mathbb{Z}\sigma^i$, $N_G = 1 + \sigma + \ldots + \sigma^{n-1}$ and

$$\sigma^k - 1 = (\sigma - 1)(\sigma^{k-1} + \ldots + \sigma + 1)$$

In particular $I_G = \mathbb{Z}[G](\sigma - 1) = (\sigma - 1)\mathbb{Z}[G]$ is a principal ideal.

Theorem 56 (Cohomology of cyclic groups)
In the situation before, $H^q(G, A) \simeq H^{q+2}(G, A)$.

Proof
It suffices to prove the result for $q = -1$ and then it follows by dimension shifting as

$$H^q(G, A) \simeq H^{-1}(G, A^{q+1}) \simeq H^1(G, A^{q+1}) \simeq H^{q+2}(G, A)$$

Let Z_1 be the set of 1-cocycles. These are crossed homomorphisms

$$x(\sigma^k) = \sigma x(\sigma^{k-1}) + x(\sigma) = \ldots = \sum_{i=0}^{k-1} \sigma^i x(\sigma)$$

Observe that x is fully determined by its value on σ.
Compute $N_G x(\sigma) = x(\sigma^n) = x(1) = 0$, hence $x(\sigma) \in {}_{N_G}A$.
We can define $Z_1 \to Z_{-1} = {}_{N_G}A$ sending $x \to x(\sigma)$, this is an isomorphism.
Since it respects coboundaries, it descends to an isomorphism of cohomology groups.
If $x \in R_1$, $x(\sigma^k) = \sigma^k a - a$ for some $a \in A$, $\iff$ $x(\sigma) \in I_G A = R_{-1}$. $\square$

Given an exact sequence $0 \to A \to B \to C \to 0$ of G-modules

$$H^{-1}(G,A) \to H^{-1}(G,B) \to H^{-1}(G,C) \xrightarrow{\delta} H^0(G,A) \to H^0(G,B) \to H_0(G,C) \to H^1(G,A) \simeq H^{-1}(G,A)$$

Definition 24 (Herbrand quotient)
Let A be an abelian group and f, g two endomorphisms of A such that $f \circ g = g \circ f = 0$.
Then the Herbrand quotient is defined by

$$q_{f,g}(A) = \frac{[\ker f : \operatorname{Im} g]}{[\ker g : \operatorname{Im} f]}$$

An important special case of this is $f = D = \sigma - 1, g = N = 1 + \sigma + \ldots + \sigma^{n-1}$ with A a G-module.
Clearly, $D \circ N = N \circ D = 0$, then $q_{D,N}(A) = \frac{\# H^0(G,A)}{\# H^{-1}(G,A)}$.
If the context is clear, we write $q_{D,N}(A) = h(A)$.

Theorem 57
Let G be a cyclic group and $0 \to A \to B \to C \to 0$ be an exact sequence of G-modules, then $h(B) = h(A)h(C)$.

Proof
Look at the exact hexagon and call the maps $f_1, f_2, f_3, f_4, f_5, f_6$.
Define $F_i = \# \operatorname{Im} f_i$.
And now, "combinatorics"... $\square$

Lecture 11: herbrand quotients

Thu 17 Nov

Theorem 58
If G is cyclic of order n.
If A is finite, then $q_{f,g}(A) = 1$.
If A is a submodule of B with finite index, then $h(B) = h(A)$.

Proof
If $f : A \to A$, then

$$\# A = \# \ker f \# \operatorname{Im} f = \# \ker g \# \operatorname{Im} g$$

for finite A. $\square$

Lemma 59
Let f, g be commuting endomorphisms of A, then

$$q_{0,g\circ f} = q_{0,g}(A) q_{0,f}(A)$$

Theorem 60
Let G be a cyclic group of order p and let A be a G-module.
Suppose that $q_{0,p}(A)$ is defined, then $q_{0,p}(A^G)$ and $h(A)$ are defined and

$$h(A)^{p-1} = \frac{q_{0,p}(A^G)^p}{q_{0,p}(A)}$$

Proof
Let σ be a generator of G and $D = \sigma - 1$, then $0 \to A^G \to A \xrightarrow{D} I_G A \to 0$ is exact.
We have $q_{0,p}(A) = q_{0,p}(A^G) q_{0,p}(I_G A)$.
We have to compute $q_{0,p}(I_G A)$.
Recall that $\mathbb{Z} N_G = \mathbb{Z} \sum_{i=0}^{p-1} \sigma^i$ annihilates $I_G A$.
Thus, we can view $I_G A$ as a $\mathbb{Z}[G]/\mathbb{Z}N_G$-module.
But we have ring isomorphisms

$$\mathbb{Z}[G]/\mathbb{Z}N_G \simeq \mathbb{Z}[x]/(1 + x + \ldots + x^{p-1}) \simeq \mathbb{Z}[\zeta]$$

In $\mathbb{Z}[\zeta]$, we know that $p = (\zeta - 1)^{p-1} \cdot e$ for a unit $e \in \mathbb{Z}[\zeta]^\times$ and $p = (\sigma - 1)^{p-1} \cdot \epsilon$ for a unit $\epsilon \in \mathbb{Z}[G]/\mathbb{Z}N_G$.
In particular multiplication by ϵ is an automorphism of $I_G A$ and $q_{0,\epsilon}(I_G A) = 1$.
We have

$$q_{0,p}(I_G A) = q_{0,D^{p-1}}(I_G A) q_{0,\epsilon}(I_G A) = q_{0,D}(I_G A)^{p-1}$$

Theorem 61 (Chevalley)
Let G be a cyclic group of order p and let A be a G-module, then

$$h(A) = p^{\frac{p\beta-\alpha}{p-1}}$$

where α is the rank of A and β is the rank of A^G.

Proof
Write $A = A_0 \oplus A_1$ where A_1 is torsion free.
Then $rankA = rankA_1 = \alpha$ and $A^G = A_0^G \oplus A_1^G$, thus $rankA^G = rankA_1^G = \beta$.
We get

$$h(A)^{p-1} = h(A_1)^{p-1} = \frac{q_{0,p}(A_1^G)^p}{q_{0,p}(A_1)} = p^{p\beta-\alpha}$$

□

5.4 A theorem of Tate

G no longer is necessarily is cyclic.

Theorem 62
Let A be a G-module.
Suppose there is $q_0 \in \mathbb{Z}$ such that

$$H^{q_0}(H, A) = H^{q_0+1}(H, A) = 0$$

for all subgroups $H \subset G$.
Then A has trivial cohomology.

Remark
This is clear for G cyclic.

Proof
We can assume $q_0 = 1$ by dimension shifting.
We need to show that if $H_1(H, A) = H^2(H, A) = 0$ then $H^0(H, A) = H^3(H, A) = 0$.
We prove this by induction on $\#G$.
If $\#G = 1$ there is nothing to prove.
By induction hypothesis, we can assume $H^0(H, A) = H^3(H, A) = 0$ for all proper subgroups $H \subsetneq G$.
We can assume that G is a p-group.
There is a normal subgroup $H \subset G$ such that G/H is cyclic of power p.
By induction hypothesis, we have $H^i(H, A) = 0$ for $i = 0, 1, 2, 3$.

Now, we know that

$$0 \to H^q(G/H, A^H) \xrightarrow{inf} H^q(G, A) \xrightarrow{res} H^q(H, A)$$

In our case, $H^q(H, A) = 0$ hence inflation is an isomorphism.
Now, $H^1(G, A) = 0 \implies H^1(G/H, A^H) = 0 \implies H^3(G/H, A^H) = 0 \implies H^3(G, A) = 0$ because G/H is cyclic.
Similarly, $H^2(G, A) = 0 \implies H^2(G/H, A^H) \implies H^0(G/H, A^H) = 0$.
We conclude by observing that

$$A^G = N_{G|H} A^H = N_{G|H} N_H A = N_G A$$ □

Lecture 12: Tate's theorem

Mon 21 Nov

Theorem 64
Let a be a G-module and assume that for each subgroup $H \subset G$, we have

1. $H^{-1}(H, A) = 0$
2. $H^0(H, A)$ *is cyclic of order* $\#H$

Let $[a_0]$ be a generator of $H^0(G, A)$, then $[a_0] \cup \cdot$ is an isomorphism for all $q \in \mathbb{Z}$.

Proof
The inclusion $i : A \to A \oplus \mathbb{Z}[G]$ induces an isomorphism $\overline{i} : H^q(H, A) \to H^q(H, B)$ because $0 \to A \to A \oplus \mathbb{Z}[G] \to \mathbb{Z}[G] \to 0$ is exact and the last term has trivial cohomologgy.
Consider $f : \mathbb{Z} \to B$ sending $n \to a_0 \cdot n + N_G N$.
This map induces a homomorphism $\overline{f} : H^q(H, \mathbb{Z}) \to H^q(H, B)$ which fits into the diagram $H^q(G, \mathbb{Z}) \xrightarrow{[a_0]\cup} H^q(G, A) \to H^q(G, B)$ which is equal to the map $\overline{f}$.
To see that the compositions do agree, notice that for $q = 0$, we have that $z_q \in \mathbb{Z}$ gets sent to $[a_0 \otimes z_q] = [z_q a_0]$ which gets sent to $bqa_0 + N_G A$.
It now suffices to show that $\overline{f}$ is an isomorphism.
Look at

$$0 \to \mathbb{Z} \xrightarrow{f} B \to C \to 0$$

The corresponding long exact sequence of cohomology groupsthen is

$$H^{-1}(H, B) \to H^{-1}(H, C) \xrightarrow{\delta} H^0(H, Z) \xrightarrow{\overline{f}} H^0(H, B) \to H^0(H, C) \to H^1(H, \mathbb{Z})$$

We know that $H^{-1}(H, B) = H^1(H, \mathbb{Z}) = 0$ and we want to show that $H^{-1}(H, C) = H^0(H, C) = 0$.
We want to show that $H^q(H, C) = 0 \forall q$, as this will show that $\overline{f}$ is an isomorphism. □