Galois cohomology of algebraic groups

Holger Kammeyer (holger.kammeyer@hhu.de)

Contents

IV Galois cohomology of simple algebraic groups

I Introduction

Let L/K be a (say finite) Galois field extension. Then the Galois group $G = Gal(L/K)$ acts naturally on various objects of interest:

1.) $G \curvearrowright L$ (by K-linear automorphisms)
2.) $G \curvearrowright L^*$ (by group automorphisms)
3.) $G \curvearrowright \mu_n(L)$ ($\mu_n(L) = \{x \in L^* | x^n = 1\} \leq L^*$)
4.) $G \curvearrowright \mathbb{Z}/n\mathbb{Z}$ (trivially)
5.) $G \curvearrowright M$ (M finite (abelian) w/ trivial action)
6.) $G \curvearrowright GL_n(L)$ (on matrix entries, by group auto.)
7.) $G \curvearrowright \mathcal{G}(L) \leq GL_n(L)$ (def. by polynomials w/ K-coeff.)

Note that 1.)–6.) are special cases of 7.), i.e. G acts on the L-points of an algebraic K-group $\mathcal{G}$.

Often of interest: Given $G \curvearrowright A$, determine the G-fixed points $A^G = \{a \in A \mid \sigma . a = a \text{ for all } \sigma \in G\}$.

E.g. $\mathcal{G}(L)^G = \mathcal{G}(L) \cap GL_n(K) =: \mathcal{G}(K)$.

Idea. Study the functor $(\cdot)^G$!

Note: if A is an abelian group, it is a $\mathbb{Z}G$-module, so first consider $(\cdot)^G : \underline{\mathbb{Z}G\text{-mod}} \longrightarrow \underline{Ab}$.

<u>Lemma I.1</u> If $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact in <u>$\mathbb{Z}G$-mod</u>, then so is $0 \to A^G \to B^G \to C^G$ in <u>Ab</u>.

<u>Proof</u> Let $b \in \ker g \cap B^G$. Then there exists $a \in A$ w/ $f(a) = b$. But $f(\sigma a - a) = \sigma f(a) - f(a) = 0$ and $\ker f = 0$, hence $a \in A^G$. $\square$

So $(\cdot)^G$ is left-exact. Could it be right-exact? Let $c \in C^G$ and $b \in B$ w/ $g(b) = c$. We only know $\sigma b - b \in A$ (considering f as an inclusion $A \subseteq B$). So we get a map

$$G \to A, \quad \sigma \mapsto \sigma b - b =: a_\sigma$$

satisfying $a_{\sigma\tau} = (\sigma\tau b - b = \sigma b - b + \sigma\tau b - \sigma b =) = a_\sigma + \sigma a_\tau$, to wit a 1-cocycle $a_\sigma \in Z^1(G, A)$. Had we chosen $b + a'$ ($a' \in A$) instead of b, then a_σ would differ by the cocycle $\sigma a' - a'$, so define the 1-coboundaries as the subgroup

$$B^1(G, A) = \{ a_\sigma \in Z^1(G, A) \mid \exists\, a' \in A : a_\sigma = \sigma a' - a' \}.$$

So the obstruction to $c \in C^G$ having a preimage in B^G is given by

$$\delta(c) := [a_\sigma] \in H^1(G, A) := Z^1(G, A) / B^1(G, A),$$

meaning

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

in <u>Ab</u> is exact.

Exercise: · Show that $H^1(G,\cdot)$ is functorial and

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

is exact and natural.

· Find an example w/ $\delta \neq 0$.

Using injective resolutions, one can define right derived functors $H^i(G,\cdot)$ extending the ex. seq. So it makes sense to set $H^0(G,\cdot) := (\cdot)^G$.

Back to a possibly non-abelian A (e.g. $G \curvearrowright A = \mathcal{G}(L) \leq GL_n(L)$), we see that we need noncommutative versions of the above.

Consistency w/ the abelian case suggests we set

- $H^0(G,A) = A^G$
- $H^1(G,A) = Z^1(G,A)/\sim$ w/
  $Z^1(G,A) = \{ a_\sigma : G \to A \mid a_{\sigma\tau} = a_\sigma \cdot {}^\sigma a_\tau \}$
  and $a_\sigma \sim b_\sigma :\Leftrightarrow \exists\, a' \in A : b_\sigma = a'^{-1} \cdot a_\sigma \cdot {}^\sigma a'$

Warning: $H^1(G,A)$ is only a pointed set. But

Prop. I.2. For $A \leq_G B$, we obtain $G \curvearrowright B/A$ and

$$1 \to H^0(G,A) \to H^0(G,B) \to H^0(G,B/A) \to H^1(G,A) \to H^1(G,B)$$

is exact (preimage of a base point = image of preceding arrow).

Proof. Same as before. $\square$

Special feature: If X is a "K-object", then

$$H^1(G, \mathrm{Aut}_L X) \overset{1:1}{\longleftrightarrow} \{ Y \mid Y \cong_L X \} / \cong_K .$$

(cf. Thm. IV.3.1)

$\rightsquigarrow$ Classification strategy: first up to "$\cong_L$" (typically $L = \overline{K}$ or K_{sep}), then for each L-type X, find a convenient K-form X_0 and compute $H^1(G, \mathrm{Aut}_L X_0)$.

In our case: G simple, 1-connected lin. alg. K-group

- Classification up to "$\cong_{\overline{K}}$" via Dynkin diagrams Δ.
- Let G_0 be K-split w/ a given Dyn. diag. Δ and consider the S.E.S. of inner & outer auto.:

$$1 \to \mathrm{Ad}\, G_0 \to \mathrm{Aut}\, G_0 \rightleftarrows \mathrm{Sym}\, \Delta \to 1$$

$$\to \quad 1 \to H^1(G, \mathrm{Ad}\, G_0) \to H^1(G, \mathrm{Aut}\, G_0) \underset{s}{\overset{p}{\rightleftarrows}} H^1(G, \mathrm{Sym}\, \Delta) \to 1$$

- $\mathrm{im}\, s \overset{1:1}{\longleftrightarrow}$ K-quasisplit forms of G_0
- $p^{-1}(\alpha) \overset{1:1}{\longleftrightarrow} H^1(G, \mathrm{Ad}\, G_1)/\mathrm{Sym}\,\Delta$ where G_1 is the K-quasisplit group corresponding to $s(\alpha)$.
- Consider $1 \to Z(G_1) \to G_1 \to \mathrm{Ad}\, G_1 \to 1$

$$\rightsquigarrow \quad H^1(G, G_1) \to H^1(G, \mathrm{Ad}\, G_1) \to H^2(G, Z(G_1))$$

- Thm. (Kneser, 60s): K p-adic $\Rightarrow H^1(G, G_1) = 1$.

$\rightsquigarrow \quad H^1(G, \mathrm{Ad}\, G_1) \cong H^2(G, Z(G_1))$ computation feasible

- k: #-field $\rightsquigarrow$ local-global principle

$$H^2(\mathrm{Gal}(k), M) \hookrightarrow \prod_v H^2(\mathrm{Gal}(k_v), M)$$

for certain finite abelian M by "Poitou-Tate duality"

<u>Course outline:</u>

- Number theoretic toolbox,
- Galois cohomology of finite abelian modules,
- " " " simple algebraic groups.

II Preliminaries from algebraic number theory

(Algebraic (number) theory)

II.1 Number fields

Def. II.1.1. An algebraic number field is a finite field extension $k/\mathbb{Q}$.

- Primitive el.t thm. $\rightsquigarrow$ $k = \mathbb{Q}(a)$ for some $a \in k$ w/ (unique) minimal polynomial $f \in \mathbb{Q}[X]$ of degree $d = [k : \mathbb{Q}]$.
- The roots $\{a_1, \dots, a_d\} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$ of f are called the (Galois) conjugates of a.
- Requiring $a \mapsto a_i$ defines $\mathbb{Q}(a) \cong \mathbb{Q}(a_i)$ and any $\mathbb{Q}(a) \hookrightarrow \mathbb{C}$ must send a to some a_i, so there are exactly d embeddings $\sigma_i : k \hookrightarrow \mathbb{C}$
- Note that $\overline{\{a_1, \dots, a_d\}} = \{a_1, \dots, a_d\}$, so $\sigma_i(k) \subset \mathbb{R}$ iff $\overline{\alpha_i} = \alpha_i$. $\rightsquigarrow$

  $r_1 := \# \underbrace{\{\text{real emb. of } k\}}_{\text{"real places"}}$, $r_2 = \# \underbrace{\{\{\sigma_i, \overline{\sigma_i}\} : \sigma_i(k) \not\subset \mathbb{R}\}}_{\text{"complex places"}}$,

  $d = r_1 + 2r_2$.
- Example:
  - $\mathbb{Q}(\sqrt[3]{2})$: $r_1 = 1$, $r_2 = 1$.
  - $\mathbb{Q}(e^{2\pi i/n})$: $r_1 = 0$, $r_2 = \phi(n)/2$.

Def. II.1.2 For $\alpha \in k$, the rational numbers

$N_{k/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \cdots \sigma_d(\alpha)$ and $Tr_{k/\mathbb{Q}} = \sigma_1(\alpha) + \dots + \sigma_d(\alpha)$

are called norm and trace of α.

Let $\alpha_1, \dots, \alpha_d \in K$ and $\lambda_1, \dots, \lambda_d \in \mathbb{Q}$. Then
$\lambda_1 \alpha_1 + \dots + \lambda_d \alpha_d = 0 \iff \lambda_1 \sigma_i(\alpha_1) + \dots + \lambda_d \sigma_i(\alpha_d) = 0$
for all i. Hence
$\{\alpha_i\}$ basis of $K \iff \det(\sigma_i(\alpha_j)) \neq 0$

<u>Def. II.1.3</u> The discriminant of a basis $\{\alpha_i\} \subset K$ is
$$\operatorname{disc}\{\alpha_1, \dots, \alpha_d\} = \det(\sigma_i(\alpha_j))^2 \in \mathbb{Q}.$$

<u>Exercise:</u> • $\operatorname{discr}\{\alpha_1, \dots, \alpha_d\} = \det(\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j))$
• $K = \mathbb{Q}(a) \Rightarrow \operatorname{discr}\{1, a, \dots, a^{d-1}\} = \prod_{i<j} (\sigma_i(a) - \sigma_j(a))^2$.

Similarly, for L/K, define $\operatorname{discr}_{L/K}$ using those $\sigma_i : L \hookrightarrow \mathbb{C}$ w/ $\sigma_i|_K = \mathrm{id}_K$.

<u>II.2 Integrality in number fields</u>

Now and in the remainder, let K be a number field.

<u>Def. II.2.1</u> The ring of integers in K is given by
$\mathcal{O}_K = \{\alpha \in K \mid f(\alpha) = 0$ for some <u>monic</u> $f \in \mathbb{Z}[x]\}$.

<u>Example:</u> $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ (Gauss's lemma)
"$\mathcal{O}_K$ is to K what $\mathbb{Z}$ is to $\mathbb{Q}$"

algebraic integers in K — rational integers

<u>Prop. II.2.2</u> Let $\alpha_1, \dots, \alpha_r \in K$. Then
$\alpha_1, \dots, \alpha_r \in \mathcal{O}_K \iff \mathbb{Z}[\alpha_1, \dots, \alpha_r]$ fin. gen. $\square$

Cor. II.2.3 $\mathcal{O}_k$ is a ring.

Proof. $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_1+\alpha_2, \alpha_1\cdot\alpha_2] = \mathbb{Z}[\alpha_1,\alpha_2]$. $\square$

Lemma II.2.4 For $\alpha \in k$, there is $\beta \in \mathcal{O}_k$, $m \in \mathbb{Z}$ such that $\alpha = \frac{\beta}{m}$.

Proof. $a_n \alpha^n + \dots + a_0 = 0$, $a_i \in \mathbb{Z}$ $\quad | \cdot a_n^{n-1}$

$\Rightarrow (a_n\alpha)^n + \dots + a_n^{n-1} \cdot a_0 = 0$, so $a_n \cdot \alpha \in \mathcal{O}_k$. $\square$

$\rightsquigarrow$ From now on, we can and will assume $k = \mathbb{Q}(a)$ w/ $a \in \mathcal{O}_k$.

Prop. II.2.5 $\mathbb{Z}[a] \subseteq \mathcal{O}_k \subseteq \underbrace{\frac{1}{\mathrm{discr}(1,\dots,a^{d-1})}}_{\in \mathcal{O}_k \cap \mathbb{Q} = \mathbb{Z}} \mathbb{Z}[a]$.

Proof. $\mathcal{O}_k \ni \alpha = \overset{\mathbb{Q}}{\overset{\cup\!\!\!\!\!\;|}{\lambda_0}} \cdot 1 + \dots + \lambda_{d-1} a^{d-1} \quad | \cdot a^i \; | \; \mathrm{Tr}_{k/\mathbb{Q}}$

$\Rightarrow \underbrace{\mathrm{Tr}_{k/\mathbb{Q}}(a^i \cdot \alpha)}_{\in \mathbb{Z}} = \sum_{j=0}^{d-1} \underbrace{\mathrm{Tr}_{k/\mathbb{Q}}(a^i \cdot a^j)}_{\det = \mathrm{discr}\{a^i\}} \cdot \lambda_j$

$\Rightarrow \lambda_j \in \frac{1}{\mathrm{discr}\{a^i\}} \mathbb{Z}$. $\square$

Cor. II.2.6 $\mathcal{O}_k$ has a $\mathbb{Z}$-basis of rank d. $\square$

Any such is called an integral basis.

Cor. II.2.7 $\mathcal{O}_k$ is noetherian.

Proof. $\mathfrak{a} \subseteq \mathcal{O}_k$ f.g. in $\underline{\mathbb{Z}\text{-mod}} \Rightarrow$ f.g. in $\underline{\mathcal{O}_k\text{-mod}}$. $\square$

Def. II.2.8 The discriminant of K is given by
$$\mathrm{discr}_K = d_K = \mathrm{discr}\{\alpha_1, \dots, \alpha_d\}$$
for an integral basis $\{\alpha_i\}$.

- Well-defined because $\det\left(T^{\{\beta_i\}}_{\{\alpha_i\}}\right) = \pm 1$.
- More generally, $d_{L/K} = (\mathrm{discr}\{\beta_i\}) \subseteq \mathcal{O}_K$.
  $\beta_i \in \mathcal{O}_L$, basis of L

Exercise: $K = \mathbb{Q}(\sqrt{D})$ for a square-free integer D

	int. base	d_K
$D \equiv 1 \ (4)$	$1, \frac{1+\sqrt{D}}{2}$	D
$D \equiv 2,3 \ (4)$	$1, \sqrt{D}$	$4D$

II.3. The arithmetic of algebraic integers

Let's consider the example $K = \mathbb{Q}(\sqrt{-5})$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. In $\mathcal{O}_K$, we have
$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$
and all these factors are irreducible, e.g.
$3 = \alpha \cdot \beta$, $\alpha, \beta \notin \mathcal{O}_K^*$. Then $N_{K/\mathbb{Q}}(\alpha) \cdot N_{K/\mathbb{Q}}(\beta) = 9$,
so $N_{K/\mathbb{Q}}(\alpha) = \pm 3$ because only units have norm ± 1.
But $N_{K/\mathbb{Q}}(x + y\sqrt{-5}) = x^2 + 5y^2 \not\equiv 3 \ (4)$, $\lightning$.

$\rightarrow$ Bad news: $\mathcal{O}_K$ is not a UFD!

<u>Kummer's remedy:</u> In an ideal world, there'd be ideal numbers $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ s.t.

$$(3) = \mathfrak{p}_1 \mathfrak{p}_2, \quad (7) = \mathfrak{p}_3 \mathfrak{p}_4, \quad (1+2\sqrt{-5}) = \mathfrak{p}_1 \mathfrak{p}_3,$$
$$(1-2\sqrt{-5}) = \mathfrak{p}_2 \mathfrak{p}_4, \quad \text{hence}$$
$$(21) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4 = \mathfrak{p}_1 \mathfrak{p}_3 \mathfrak{p}_2 \mathfrak{p}_4$$

$\rightsquigarrow$ factorization unique!

Apparently: $\mathfrak{p}_1 \mid 3$, $\mathfrak{p}_1 \mid 1+2\sqrt{-5} \Rightarrow \mathfrak{p}_1 \mid \lambda \cdot 3 + \mu \cdot (1+2\sqrt{5})$ and $\mathfrak{p}_1$ should be determined by the set of all $\alpha \in \mathcal{O}_K$ that it divides.

So set $\mathfrak{p}_1 = (3, 1+2\sqrt{-5})$, $\mathfrak{p}_2 = (3, 1-2\sqrt{-5})$, ...

<u>Thm. II.3.1</u> The ring $\mathcal{O}_K$ is

1.) noetherian,

2.) integrally closed, $\left(\begin{array}{l} \alpha \in K, f(\alpha)=0 \text{ for monic} \\ f \in \mathcal{O}_K[x] \Rightarrow \alpha \in \mathcal{O}_K \end{array} \right)$

3.) and non-zero prime ideals are maximal. $\square$

<u>Def. II.3.2</u> An int. domain w/ 1.), 2.), 3.) is called a Dedekind domain.

<u>Thm. II.3.3</u> (Dedekind) Every ideal $\mathfrak{a} \neq (0), (1)$ in a Dedekind domain $\mathcal{O}$ has a unique factorization

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

into prime ideals $\mathfrak{p}_i \subseteq \mathcal{O}$. $\square$

How do we get inverses of ideals?

Let $\mathcal{O}$ be a Dedekind domain w/ field of fractions K.

<u>Def. II.3.4</u> A fractional ideal of K is a f.g. $\mathcal{O}$-submodule $\mathfrak{a} \neq (0)$ of K.

<u>Example.</u>
- $(a) = a \cdot \mathcal{O}$ for any $a \in K^*$.
- Every (integral) ideal $\mathfrak{a} \subseteq \mathcal{O}$.

Observe: An $\mathcal{O}$-module $\mathfrak{a}$ is a fractional ideal iff there exists $0 \neq c \in \mathcal{O}$ s.t. $c \cdot \mathfrak{a} \subseteq \mathcal{O}$.

Using this, we see that for $\mathfrak{a} \neq 0$, $\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$ is a fractional ideal. If we define $\mathfrak{a} \cdot \mathfrak{b}$ as usual, then $(1) \cdot \mathfrak{a} = \mathfrak{a}$ and $\mathfrak{a} \cdot \mathfrak{a}^{-1} = (1)$:

<u>Thm. II.3.5</u> The fractional ideals form an abelian group called the ideal group J_K of K.

<u>Cor. II.3.6</u> For $\mathfrak{a} \in J_K$, we have

$$\mathfrak{a} = \prod_{0 \neq \mathfrak{p} \text{ prime}} \mathfrak{p}^{v_\mathfrak{p}}$$

with $v_\mathfrak{p} \in \mathbb{Z}$ (a.a. zero) uniquely. $\square$

So J_K is free abelian w/ basis $(\operatorname{Spec} \mathcal{O}) \setminus \{(0)\}$.

Let $P_K = \{(a) \mid a \in K^*\} \leq J_K$ be the subgroup of principal fractional ideals.

Def. II.3.7 The (ideal) class group of K is $Cl_K = J_K / P_K$.

Hence:

$$1 \longrightarrow \mathcal{O}^* \longrightarrow K^* \longrightarrow J_K \longrightarrow Cl_K \longrightarrow 1$$
$$a \longmapsto (a)$$

is exact, so $\begin{Bmatrix} Cl_K \\ \mathcal{O}^* \end{Bmatrix}$ describes the $\begin{Bmatrix} \text{gain} \\ \text{loss} \end{Bmatrix}$ when passing from numbers to ideal(number)s.

$\rightsquigarrow$ Need to study Cl_K and $\mathcal{O}^*$!

Back to $K = k$ and $\mathcal{O} = \mathcal{O}_k$.

Thm. II.3.8 (Gauß, Minkowski) Cl_k is finite. $\square$

We call $h_k = |Cl_k|$ the class number of k.

Example. · Let $D > 0$ be square-free.

Then $h_{\mathbb{Q}(\sqrt{-D})} = 1 \iff D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$

(conj.: Gauß, proof: Baker–Stark–Heegner)

· Open: Are there inf. many D w/ $h_{\mathbb{Q}(\sqrt{D})} = 1$?

Thm. II.3.9 (Dirichlet) $\mathcal{O}_k^* \cong \mu(k) \oplus \mathbb{Z}^{r_1 + r_2 - 1}$

where $\mu(k)$ is the group of roots of unity in k. $\square$

Proofs of II.3.8 and II.3.9: "Geometry of numbers".

Exercise: Show that $\mathcal{O}_K/\mathfrak{a}$ is finite for every ideal $(0)\neq\mathfrak{a}\leq\mathcal{O}_K$. Hint: First assume $\mathfrak{a}=\mathfrak{p}$ is prime. (This also proves II.3.1(3).)

Def. II.3.10 The (absolute) norm of $(0)\neq\mathfrak{a}\leq\mathcal{O}_K$ is

$$n(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|.$$

Exercise: · For $a\in\mathcal{O}_K$, we have $n((a))=|N_{K/\mathbb{Q}}(a)|$.

· $n(\mathfrak{a}\cdot\mathfrak{b}) = n(\mathfrak{a})\cdot n(\mathfrak{b})$ (Hint: C.R.T.)

$\rightsquigarrow$ Obtain a homomorphism $n: J_K \longrightarrow \mathbb{R}^*_{>0}$.

II.4 Decomposition and ramification

Let p be a rational prime. Then

$$p\,\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}. \qquad (*)$$

Note that $\mathcal{O}_K/\mathfrak{p}_i$ is a finite field $\Rightarrow n(\mathfrak{p}_i)=p_i^{f_i}$.

Apply n to $(*)$: $p^d = p_1^{f_1e_1}\cdots p_r^{f_re_r}$, so $p_i=p$ and

$$f_1e_1+\cdots+f_re_r = d \quad \text{"fundamental equation"}$$

· e_i: ramification index of $\mathfrak{p}_i$ over p.

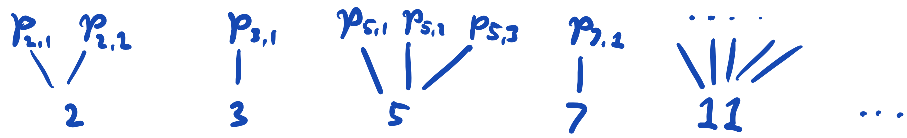
· f_i: inertia degree —— " ——.

Extreme cases: · $r=d$: "p is split".

· $r=1$, $f_1=1$: "p ramifies completely".

· $r=1$, $e_1=1$: "p is inert".

Note $p\mathcal{O}_k \subseteq \mathfrak{p}_i$ ($\Leftrightarrow \mathfrak{p}_i \mid p$) for a unique p,
"$\mathfrak{p}_i$ lies over p":



<u>Def. II.4.1</u> $\mathfrak{p}$ is called ramified in k if $e_\mathfrak{p} > 1$.
A rat. prime p " " " " " "
for some $\mathfrak{p} \mid p$.

<u>Thm. II.4.2</u> A rat. prime p is ramified in k iff $p \mid d_k$. □

<u>Cor. II.4.3</u> Almost all p are unramified. □

<u>Remark.</u> If $k/\mathbb{Q}$ is Galois and $\sigma \in \mathrm{Gal}(k/\mathbb{Q})$, then $\sigma(\mathcal{O}_k) = \mathcal{O}_k$ and

$$\sigma(\mathfrak{p}) \cap \mathbb{Z} = \sigma(\mathfrak{p} \cap \mathbb{Z}) = \sigma((p)) = (p),$$

so $\mathrm{Gal}(k/\mathbb{Q})$ permutes the prime(ideal)s over p.
It acts transitively (exercise!) and preserves e_i and f_i, so the fund. eq. takes the form

$$e \cdot f \cdot r = d.$$

$\rightsquigarrow$ If $k/\mathbb{Q}$ is cyclic of prime degree, only the above extreme cases can occur.

II.5 Valuations and completions

<u>Def. II.5.1</u> A valuation of k is a map $|\ |: k \longrightarrow \mathbb{R}$ such that for all $x, y \in k$, we have

1.) $|x| \geq 0$ and $|x| = 0 \Leftrightarrow x = 0$,

2.) $|x \cdot y| = |x| \cdot |y|$,

3.) $|x + y| \leq |x| + |y|$.

(We dismiss the trivial val. $|x| = 1$ for all $x \in k^*$.)

If $|\cdot|$ satisfies the stronger

3'.) $|x + y| \leq \max\{|x|, |y|\}$,

then $|\cdot|$ is called non-archimedean, otherwise archimedean.

<u>Examples.</u> · <u>Archimedian:</u> Let $\sigma: k \hookrightarrow \mathbb{C}$ and set $|x|_\sigma := |\sigma(x)|$.

· <u>Non-archimedean:</u> Let $\mathfrak{p}_0 \subseteq \mathcal{O}_k$ be a prime. For $x \in k^*$, write $x\mathcal{O}_k = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$ and set $|x|_{\mathfrak{p}_0} := q^{-v_{\mathfrak{p}_0}(x)}$ w/ $q = |\mathcal{O}_k/\mathfrak{p}_0| = p^{f_{\mathfrak{p}}}$ for $\mathfrak{p}_0 \cap \mathbb{Z} = (p)$.

"$\mathfrak{p}$-adic valuation"

<u>Def. II.5.2</u> $|\cdot|_1 \sim |\cdot|_2 \;:\Leftrightarrow\; \exists\, a > 0 : |\cdot|_1 = |\cdot|_2^a$

$\Leftrightarrow$ $d_i(x,y) := |y - x|_i$ define the same topologies on k.

<u>Thm. II.5.3</u> (Ostrowski) The above examples exhaust all valuations on k up to "$\sim$". $\square$

Def. II.5.4 The $\sim$-classes of (non-arch. / arch.) valuations on k are called (finite / inf.) places.

Notation: $V(k) = V_\infty(k) \cup V_f(k)$ (set of places)
Note $|V_\infty(k)| = r_1 + r_2$ because cpx. conj. emb.s define the same arch. valuation. We shall freely write $v \in V(k)$ or $\mathfrak{p} \in V(k)$.

Perks of places:

- The infinite places "complete the picture":
$$\prod_{\mathfrak{p} \in V(k)} |x|_{\mathfrak{p}} = 1 \quad \text{for all } x \in k^*.$$
- They allow for completion so that also $v \in V_f(k)$ corresponds to an embedding "$k \hookrightarrow k_v$" to a complete field k_v:

Def. II.5.5 $k \hookrightarrow k_v$ is the completion of k w.r.t. $d_v(x,y) = v(y-x)$:

$$k_v = \frac{\{\text{Cauchy seq. in } k\}}{\{\text{null seq. in } k\}}, \quad k \hookrightarrow k_v \text{ constant sequences},$$

v extends to k_v: (x_n) Cauchy $\Rightarrow (v(x_n)) \subseteq \mathbb{R}$ Cauchy.

Example: $k = \mathbb{Q}$, $v = p$, $k_v = \mathbb{Q}_p \cong \mathrm{Frac}\left(\varprojlim_k \mathbb{Z}/p^k\mathbb{Z}\right)$.
"p-adic numbers". More generally, for $\mathfrak{p} \in V_f(k)$, we call $k_{\mathfrak{p}}$ a p-adic field.

Def. II.5.6 Let $v \in V_f(k)$. Then

$$\mathcal{O}_{(v)} = \{x \in k \mid v(x) \leq 1\} \subseteq k \quad \text{and}$$
$$\mathcal{O}_v = \{x \in k_v \mid v(x) \leq 1\} \subseteq k_v$$

are called the valuation rings of the valued fields k and k_v, resp.

Note that $\mathcal{O}_{(v)} = \mathcal{O}_v \cap k$ and $\mathcal{O}_v = \overline{\mathcal{O}_{(v)}}$.

The rings $\mathcal{O}_v$ and $\mathcal{O}_{(v)}$ are PIDs w/ unique maximal ideals

$$\pi \mathcal{O}_{(v)} = \{x \in \mathcal{O}_{(v)} \mid v(x) < 1\} \quad \text{and}$$

$$\pi \mathcal{O}_v = \{x \in \mathcal{O}_v \mid v(x) < 1\},$$

so they are discrete valuation rings (DVRs).

The up to association unique elt $\pi \in \mathcal{O}_{(v)} \subset \mathcal{O}_v$ is called a uniformizer. We have a canonical iso.

$$\mathcal{O}_{(v)}/\pi \mathcal{O}_{(v)} \xrightarrow{\cong} \mathcal{O}_v/\pi \mathcal{O}_v$$

of the residue fields.

Thm. II.5.7 Let K be complete w/ valuation v and L/K algebraic. Then v extends uniquely to L. If $d = [L:K] < \infty$, then $\overline{v}(x) = \sqrt[d]{v(N_{L/K}(x))}$.

Proof. Hensel's lemma. $\square$

In particular, v_p on $\mathbb{Q}_p$ extends uniquely to $\overline{v_p}$ on $\overline{\mathbb{Q}_p}$.
Given $\sigma : k \hookrightarrow \overline{\mathbb{Q}_p}$, we obtain $v_\sigma := \overline{v_p} \circ \sigma$.
If $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, then $\overline{v_p} = \overline{v_p} \circ \tau$, so $v_\sigma = v_{\tau\circ\sigma}$.

<u>Thm. II.5.8</u> 1.) Every extension w of v_p from $\mathbb{Q}$ to k is of the form $w = v_\sigma$ for some $\sigma : k \hookrightarrow \overline{\mathbb{Q}_p}$.
2.) $v_\sigma = v_{\sigma'}$ iff there is $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$: $\sigma' = \tau\circ\sigma$. $\square$

<u>Remark</u>: This also holds for $p = \infty$ when $\mathbb{Q}_\infty = \mathbb{R}$.

Cpx. inf. places $\overset{1:1}{\longleftrightarrow}$ Conj. classes of $k \overset{\sigma}{\hookrightarrow} \mathbb{C}$, $\sigma(k) \not\subseteq \mathbb{R}$.
Real inf. places $\overset{1:1}{\longleftrightarrow}$ Embeddings $k \overset{\sigma}{\hookrightarrow} \mathbb{R}$.
Finite places over p $\overset{1:1}{\longleftrightarrow}$ Conj. classes of $k \overset{\sigma}{\hookrightarrow} \overline{\mathbb{Q}_p}$.
$\updownarrow$ 1:1
prime ideals $0 \neq \mathfrak{p} \subseteq \mathcal{O}_k$ w/ $\mathfrak{p} | p$.

Moreover $k_w = \sigma(k)\cdot\mathbb{Q}_p \subseteq \overline{\mathbb{Q}_p}$ for $w = v_\sigma$, so

$$\begin{tikzcd} k \arrow[r] & k_w \\ \mathbb{Q} \arrow[u, "\text{``global''}"'] \arrow[r] & \mathbb{Q}_p \arrow[u, "\text{``local''}"] \end{tikzcd}$$

<u>Thm. II.5.9</u> $k \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{w|p} k_w$ and $[k_w : \mathbb{Q}_p] = e_w \cdot f_w$ if $p < \infty$.

<u>Bew.</u> Let $k = \mathbb{Q}(a)$ w/ min. poly. $f \in \mathbb{Q}[X]$. Then $f(X) = \prod_{v|p} f_v(X)$ over $\mathbb{Q}_p$, hence:

$$\begin{tikzcd} \mathbb{Q}_p[X]/(f) \arrow[r, "\cong\ (\text{C.R.T.})"] \arrow[d, "\cong"'] & \prod_{v|p} \mathbb{Q}_p[X]/(f_v) \arrow[d, "\cong"] \\ k \otimes_{\mathbb{Q}} \mathbb{Q}_p \arrow[r] & \prod_{v|p} k_v \end{tikzcd}$$

. $\square$

Def. II.5.10 The ring of adèles of k is $\mathbb{A}_k = \prod'_{v \in V(k)} k_w$ (almost all coord. in $\mathcal{O}_v$). The idele group is $\mathbb{I}_k = \mathbb{A}_k^*$.

We have diagonal embeddings $k \hookrightarrow \mathbb{A}_k$, $k^* \hookrightarrow \mathbb{I}_k$ w/ discrete image where $\mathbb{A}_k$ has unit nbhd. base $\prod_{v \in V(k)} U_v$ w/ $U_v \subseteq k_v$ open and $U_v = \mathcal{O}_v$ for a.a. v.
Similarly for $\mathbb{I}_k$ w/ $U_v \subseteq k_v^*$ and $U_v = \mathcal{O}_v^*$ —— " ——.
(Not the subspace top. of $\mathbb{I}_k \subseteq \mathbb{A}_k$!)

II.6 Local-global principles

Idea: • Let $p \in k[X]$. Suppose $x \in k$ satisfies $p(x) = 0$. Then, of course, $x \in k \subseteq k_v$ defines a solution $x \in k_v$ to $p(x) = 0$. If, on the other hand, we find a local solution $x_v \in k_v$ w/ $p(x_v) = 0$ for all $v \in V(k)$, does this imply that there exists a global solution $x \in k$ w/ $p(x) = 0$?

Theorem II.6.1 (Global square thm.)
Yes if $p(X) = X^2 - a$ for some $a \in k^*$. In fact, $a \in k^*$ is a global square iff it is a local square for almost all $v \in V(k)$.

Theorem II.6.2 (Hasse-Minkowski)
Let $f(X_1, \dots, X_n) = a_1 X_1^2 + \dots + a_n X_n^2$ w/ $a_i \in k$ be a quadratic form. Then there exists $0 \neq X \in k^n$ w/ $f(X) = 0$ iff there exists $0 \neq X_v \in k_v^n$ w/ $f(X_v) = 0$ for all $v \in V(k)$.

Theorem II.6.3 (Hasse norm principle)
Let $k/\mathbb{Q}$ be cyclic and $x \in \mathbb{Q}$. Then $x = N_{k/\mathbb{Q}}(y)$ for some $y \in k$ iff $x = N_{k_v/\mathbb{Q}_p}(y_v)$ for some $y_v \in k_v$ for all $v \mid p$ and $p \leq \infty$ prime.

CAUTION:

1.) II.6.1 says $k^*/(k^*)^2 \xhookrightarrow{\text{diag.}} \prod_{v \in S} k_v^*/(k_v^*)^2$ for all $S \subseteq V(k)$ finite.
Do we have $\left. k^*/(k^*)^n \hookrightarrow \prod_{v \in S} k_v^*/(k_v^*)^n \right\} (*)$ for all $n \geq 2$?
No: In $k = \mathbb{Q}(\sqrt{7})$, 16 is an 8^{th} power locally everywhere but not globally.
Thm. II.6.4 (Grunwald-Wang 1933, 1948)
$(*)$ is true except for certain "special" fields and $8 \mid n$ (and then $k_\infty \cong \mathbb{Z}/2$).

2.) II.6.2 does not generalize either:
$3X^3 + 4Y^3 + 5Z^3$ represents zero in all $\mathbb{Q}_p$ but not in $\mathbb{Q}$. [Selmer, 1951]

3.) II.6.3 does not extend to abelian extensions:
For $k = \mathbb{Q}(\sqrt{13}, \sqrt{17})$, every rational square is a local norm everywhere but 25 is not a global norm [Serre-Tate].

Local-global principles for k-isomorphism:

Thm. II.6.5 Let f and f' be quadratic forms over k such that $f \cong_{k_v} f'$ for all $v \in V(k)$. Then $f \cong_k f'$.

Proof. Pick $a \in k^*$ represented by f. Then $f - az^2$ represents zero globally, hence everywhere locally, so also $f' - az^2$ represents zero locally everywhere, hence globally by II.6.2. If the element $(x_1, \dots, x_n, z)$ representing zero has $z \neq 1$, then $f'(\frac{x_1}{z}, \dots, \frac{x_n}{z}) = a$. If $z = 0$, then f' repr. 0, so $f' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp f''$, so it repr. all of k. So $f = g + az^2$, $f' = g' + az^2$ and $f \cong_{k_v} f'$ implies $g \cong_{k_v} g'$ by the Witt cancellation thm. By induction hypothesis (the rank zero case being trivial), we have $g \cong_k g'$, so $f \cong_k f'$. $\square$

Theorem II.6.6 (Hasse principle for CSAs)
Let A be a CSA over k of degree d. Then $A \cong M_d(k)$ iff $A \otimes_k k_v \cong M_d(k_v)$ for all $v \in V(k)$.

Proof. For quaternion algebras, this follows from II.6.5 as $\left(\frac{a,b}{k}\right) \overset{1:1}{\longleftrightarrow} \langle -a, -b, ab \rangle$ (rk-3 quad. forms of discr. 1). General case: global CFT (see below). $\square$

II.7 Tate Shafarevich groups

For a Galois module $\mathrm{Gal}(k) = \mathrm{Gal}(\bar{k}/k) \curvearrowright A$ and $S \subseteq V(k)$ define the n-th Tate-Shafarevich group

$$Ш^n(k,S,A) = \ker\left(H^n(k,A) \xrightarrow{\text{diag.}} \prod_{v\notin S} H^n(k_v,A)\right)$$

$\uparrow$ cyrillic "sha"

where we write $H^n(k,\cdot) = H^n(\mathrm{Gal}(k),\cdot)$

and $\begin{matrix}\bar{k} & \to & \bar{k}_v\\ \uparrow & & \uparrow \\ k & \to & k_v\end{matrix}$ gives $\mathrm{Gal}(k_v) \to \mathrm{Gal}(k)$ (A abelian if $n>1$).

We can reformulate the local-global principles of Sec. II.6 in terms of Tate-Shafarevich groups:

- II.6.1: $Ш^1(k,S,\mu_2) = \{1\}$ for S finite.

Indeed, μ_2 is a trivial $\mathrm{Gal}(k)$-module, so $H^1(k,\mu_2) \cong \mathrm{Hom}(\mathrm{Gal}(k),\mu_2) \cong \underbrace{\{l/k \mid [l:k]\leq 2\}}_{\cong_k} \cong k^*/(k^*)^2$.

- II.6.4: $Ш^1(k,S,\mu_n) \cong \begin{cases}\mathbb{Z}/2 & \text{special case}\\ 1 & \text{otherwise}\end{cases}$.

Indeed, $1 \to \mu_n \to GL_1 \xrightarrow{(\cdot)^n} GL_1 \to 1$ (exact on $\bar{k}$), so $k^* \xrightarrow{(\cdot)^n} k^* \longrightarrow H^1(k,\mu_n) \to \underset{\overset{\|}{0}\ \text{(Hilbert 90)}}{H^1(k,GL_1)}$,

thus $H^1(k,\mu_n) \cong k^*/(k^*)^n$.

- II.6.3: $Ш^1(\mathbb{Q},\emptyset,R^{(1)}_{k/\mathbb{Q}}(GL_1)) \begin{cases} = 1 & \text{for } k/\mathbb{Q} \text{ cyclic,}\\ \neq 1 & \text{for } k=\mathbb{Q}(\sqrt{13},\sqrt{17})\end{cases}$

Indeed, $1 \to R^{(1)}_{k/\mathbb{Q}}(GL_1) \longrightarrow R_{k/\mathbb{Q}}(GL_1) \xrightarrow{\text{norm}} GL_1 \longrightarrow 1$

"norm one torus" restriction of scalars: $R_{k/\mathbb{Q}}(G)(\mathbb{Q}) \cong G(k)$

$\rightsquigarrow k^* \xrightarrow{N_{k/\mathbb{Q}}} \mathbb{Q}^* \longrightarrow H^1(\mathbb{Q},R^{(1)}_{k/\mathbb{Q}}(GL_1)) \longrightarrow H^1(\mathbb{Q},R_{k/\mathbb{Q}}(GL_1))$,

|| Shapiro

so $H^1(\mathbb{Q},R^{(1)}_{k/\mathbb{Q}}(GL_1)) \cong \mathbb{Q}^*/N_{k/\mathbb{Q}}(k^*)$ $\qquad H^1(k,GL_1) \overset{\text{H. 90}}{=} 0$

- II.6.5: $Ш^1(k,\emptyset,O(f)) = \{1\}$.

See the "special feature" in Chapter I.

• II.6.6: $Ш^1(k, \emptyset, PGL_d) = \{1\}$.

Indeed, $\mathrm{Aut}(M_d) \cong PGL_d$ by Skolem-Noether and

$$1 \to GL_1 \to GL_d \to PGL_d \to 1$$

$$\begin{tikzcd}
\rightsquigarrow H^1(k, GL_d) \arrow[r] \arrow[d, equal, "d\text{-dim. H.90}"] & H^1(k, PGL_d) \arrow[r] \arrow[d] & H^2(k, GL_1) \cong Br(k) \arrow[d, hook, "\text{Albert Brauer Hasse Noether}"] \\
0 & \prod_v H^1(k_v, PGL_d) \arrow[r] & \prod_v Br(k_v)
\end{tikzcd}$$

So if $\alpha \in Ш^1(k, \emptyset, PGL)$, then diagram chasing shows α has a preimage in $H^1(k, GL_d) = 1$ whence α is trivial.

<u>Remark.</u> There exists an accidental iso. $PGL_2 \cong_k SO_3$, explaining the correspondence of quaternion algebras and rk-3 quadr. forms w/ trivial discr.

UPSHOT:

Study local-global principles for the Galois cohomology of algebraic groups!

III Galois cohomology of finite abelian modules

III.1 Group cohomology

Recall from Chapter I that for a finite group G and a S.E.S. of (left) $\mathbb{Z}G$-modules

$$0 \to A \to B \to C \to 0,$$

we gave an ad hoc construction of an exact seq.

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

There are various ways to introduce higher cohomology groups to extend this to a L.E.S.

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta^1} H^1(G, A) \to H^1(G, B) \to$$
$$\to H^1(G, C) \to H^2(G, A) \to \cdots \quad :$$

1.) By injective resolutions:

A $\mathbb{Z}G$-module I is injective if

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[dl, dashed, "\exists"] \\ & I & \end{tikzcd},$$

or, equiv'ly., $\mathrm{Hom}_{\mathbb{Z}G}(\cdot, I)$ is exact.

The (abelian) category $\underline{\mathbb{Z}G\text{-mod}}$ has enough injectives: For every $\mathbb{Z}G$-module A, we find $0 \to A \to I$, hence also an injective resolution

$$0 \to A \to I_0 \to I_1 \to I_2 \to \cdots$$

and we define $H^i(G, A)$ as the cohomology groups $\ker d^i / \operatorname{im} d^{i-1}$ of the cochain complex

$$0 \to I_0^G \xrightarrow{d^0} I_1^G \xrightarrow{d^1} I_2^G \to \cdots$$

This is well-defined by the fund. thm. of homol. alg.. The L.E.S. then follows from the horseshoe lemma and the snake lemma. The construction is functorial: $H^i(G,\cdot)$ are the right derived functors of $(\cdot)^G$.

2.) <u>By projective resolutions:</u>

A $\mathbb{Z}G$-module P is projective if, dually,

$$\begin{tikzcd} 0 & A \arrow[l] & B \arrow[l] \\ & P \arrow[u] \arrow[ur, dashed, "\exists"'] & \end{tikzcd},$$

or, equiv'ly, $\mathrm{Hom}_{\mathbb{Z}G}(P,\cdot)$ is exact.

<u>$\mathbb{Z}G$-mod</u> has enough projectives ($\forall A \ \exists \ P \to A \to 0$), so pick a projective resolution of the trivial module $\mathbb{Z}$

$$\cdots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

and define $H^i(G,A)$ as the cohomology of

$$0 \to \mathrm{Hom}_{\mathbb{Z}G}(P_0, A) \to \mathrm{Hom}_{\mathbb{Z}G}(P_1, A) \to \mathrm{Hom}_{\mathbb{Z}G}(P_2, A) \to \cdots.$$

Observe that $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) = A^G$!

<u>Remark</u>: If BG is a connected CW complex w/ $\pi_1 BG \cong G$ and $EG := \widetilde{BG} \simeq \bullet$, then $C_*^{cw}(EG;\mathbb{Z})$ is a free (hence projective) resolution of $\mathbb{Z}$. Since $C^*_{cw}(BG;A) := \mathrm{Hom}_{\mathbb{Z}G}(C_*^{cw}(EG;\mathbb{Z}), A)$, we thus have $H^*(G,A) \cong H^*_{cw}(BG;A)$ (cohomology "w/ local coefficients" in alg. top. terminology).

3.) By homogeneous cochains (making 2.) concrete):

Let L_i be the free $\mathbb{Z}$-module w/ basis G^{i+1}. The diag. action $G \curvearrowright G^{i+1}$ endows L_i w/ the structure of a free $\mathbb{Z}G$-module and

$$\cdots \to L_2 \xrightarrow{d_2} L_1 \xrightarrow{d_1} L_0 \xrightarrow{d_0} \mathbb{Z} \to 0$$

is a free (whence projective) resolution where

$$d_i(g_0, \dots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \dots, \hat{g}_j, \dots, g_i).$$

Note that $\operatorname{Hom}_{\mathbb{Z}G}(L_i, A) \cong \{ f : G^{i+1} \to A \text{ } G\text{-equivariant} \}$ ← homogeneous cochains

4.) By (inhomogeneous) cochains:

Let X_i be the free $\mathbb{Z}G$-module w/ basis G^i. Then

$$\cdots \to X_2 \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{d_0} \mathbb{Z}$$

is a free resolution where

$$d_i(g_1, \dots, g_i) = g_1 \cdot (g_2, \dots, g_i)$$
$$+ \sum_{j=1}^{i-1} (-1)^j (g_1, \dots, g_j g_{j+1}, \dots, g_i) + (-1)^i (g_1, \dots, g_{i-1}).$$

Exercise. Show that setting

$$(g_1, \dots, g_i) \mapsto (1, g_1, g_1 g_2, \dots, g_1 \cdots g_i)$$

defines an isomorphism of $\mathbb{Z}G$-complexes $X_\bullet \cong L_\bullet$.

Exercise: Show that $Z^1(\operatorname{Hom}_{\mathbb{Z}G}(X_\bullet, A))$ and $B^1(\operatorname{Hom}_{\mathbb{Z}G}(X_\bullet, A))$ agree w/ our previous definitions of 1-cocycles and 1-coboundaries.

From 3.) and 4.) we observe that $H^*(G,A)$ is finite if G and A are.

III.2 Tate cohomology

Still let G be a finite group.

Def. III.2.1 The norm of $\mathbb{Z}G$ is the element $N_G = \sum_{g\in G} g$. The augmentation ideal is

$$I_G = \ker\left(\mathbb{Z}G \to \mathbb{Z},\ \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g\right).$$

For any $\mathbb{Z}G$-module A, let $N: A \to A,\ a \mapsto N_G \cdot a$. Then $I_G A \subseteq \ker N$ and $\operatorname{im} N \subseteq A^G = H^0(G,A)$.

Def. III.2.2 We call $A_G := H_0(G,A) := A/I_G A$ the coinvariants of A.

By the above, N induces $N^*: H_0(G,A) \to H^0(G,A)$.

Def. III.2.3 Set $\hat{H}_0(G,A) := \ker N^*$, $\hat{H}^0(G,A) := \operatorname{coker} N^*$.

Observe that $(\cdot)_G \cong \mathbb{Z} \otimes_{\mathbb{Z}G} (\cdot)$ are nat. isomorphic, hence $(\cdot)_G$ is right exact. Dually to III.1.1), we define $H_i(G,\cdot)$ as the left derived functors of $(\cdot)_G$. Similarly to III.1.2), $H_i(G,A)$ is also the algebraic homology of $P_\bullet \otimes_{\mathbb{Z}G} A$ for a projective resolution $P_\bullet \to \mathbb{Z}$. by right $\mathbb{Z}G$-modules.

Example: If A is trivial, then $H_1(G,A) = G_{ab} \otimes_{\mathbb{Z}} A$.

Def. III.2.4 We define the Tate cohomology groups as

$$\hat{H}^n(G,A) = H^n(G,A) \qquad \text{for } n \geq 1$$
$$\hat{H}^0(G,A) = A^G/NA \qquad \text{(see above)}$$
$$\hat{H}^{-1}(G,A) = \hat{H}_0(G,A) = {}^{\ker N}/I_G A \qquad \text{(— " —)}$$
$$\hat{H}^{-n}(G,A) = H_{n-1}(G,A) \qquad \text{for } n \geq 2.$$

Thm III.2.5 $0 \to A \to B \to C \to 0$ in $\mathbb{Z}G$-mod induces

$$\cdots \to \hat{H}^{-2}(G,C) \to \hat{H}^{-1}(G,A) \to \hat{H}^{-1}(G,B) \to \hat{H}^{-1}(G,C) \to$$
$$\to \hat{H}^0(G,A) \to \hat{H}^0(G,B) \to \hat{H}^0(G,C) \to \hat{H}^1(G,A) \to \cdots.$$

III.3 Cup products

Still let G be finite and let $K^i(G,A) = \mathrm{Hom}_{\mathbb{Z}G}(L_i, A)$ be the cochain complex of homogeneous cochains. For $\mathbb{Z}G$-modules A and B, we obtain a left $\mathbb{Z}G$-module structure on $A \otimes B := A \otimes_{\mathbb{Z}} B$ setting $g \cdot (a \otimes b) = (ga) \otimes (gb)$.

Def. III.3.1 The cup product on homogeneous cochains is the bilinear map defined by

$$K^p(G,A) \times K^q(G,B) \xrightarrow{\cup} K^{p+q}(G, A \otimes B)$$
$$a \cup b\,(g_0, \dots, g_{p+q}) = a(g_0, \dots, g_p) \otimes b(g_p, \dots, g_{p+q}).$$

Thm. III.3.2 We have an induced bilinear cup product

$$H^p(G, A) \times H^q(G, B) \longrightarrow H^{p+q}(G, A \otimes B).$$

Proof. Well-defined because an easy calculation gives

$$d(a \cup b) = (da) \cup b + (-1)^p (a \cup db). \qquad \square$$

Remark. • For $a \in H^0(G, A) = A^G$, $b \in H^q(G, B)$, we have $a \cup b = f_*(b)$ where f_* is induced from $B \to A \otimes B$, $x \mapsto a \otimes x$. So for $p = q = 0$, we have $\cup : A^G \times B^G \longrightarrow (A \otimes B)^G$, $(a, b) \mapsto a \otimes b$.

• A bilinear map $A \times B \xrightarrow{\varphi} C$ factors as

$$\begin{tikzcd} A \otimes B \arrow[dr, dashed, "\overline{\varphi}"] & \\ A \times B \arrow[u] \arrow[r, "\varphi"] & C \end{tikzcd},$$

so that we have an induced cup product

$$H^p(G, A) \times H^q(G, B) \longrightarrow H^{p+q}(G, C).$$

• We also have a cup product

$$\hat{H}^p(G, A) \times \hat{H}^q(G, B) \longrightarrow \hat{H}^{p+q}(G, C)$$

associated w/ any pairing $A \times B \xrightarrow{\varphi} C$, $p, q \in \mathbb{Z}$, constructed using the extension $X_{-1-n} = \mathbb{Z}[G^{n+1}]$ of $X_\bullet$ w/

$$d_{-n}(g_0, \dots, g_{n-1}) = \sum_{g \in G} \sum_{i=0}^{n} (-1)^i (g_0, \dots, g_{i-1}, g, g_i, \dots, g_{n-1}).$$

for $n \geq 1$ and $d_0(g_0) = \sum_{g \in G} g$. For $p = q = 0$, it is the pairing $A^G/NA \times B^G/NB \longrightarrow C^G/NC$ induced by φ. For $p, q > 0$, it agrees w/ the previous cup product.

III.4 Cohomology of profinite groups

Def. III.4.1 A topological group G is called profinite if $G = \varprojlim G_i$ for an inverse system of finite groups $(G_i)_{i \in I}$.

Thm. III.4.2 G is profinite iff G is compact and totally disconnected.

Proof "$\Rightarrow$": $\varprojlim G_i \leq \prod_{i \in I} G_i$ closed.
"$\Leftarrow$": (trickier) $G \cong \varprojlim_N G/N$ w/ $N \trianglelefteq G$ open.
Here $[G:N] < \infty$ because G is compact. $\square$

Examples. • Finite groups

• $\mathrm{Gal}(k) = \mathrm{Gal}(\bar{k}/k) \cong \varprojlim_{\ell/k \text{ finite Galois}} \mathrm{Gal}(\ell/k) = \varprojlim_{\substack{N \trianglelefteq \mathrm{Gal}(k) \\ \text{closed, finite index}}} \mathrm{Gal}(k)/N$

• For M discrete torsion abelian, the Pontryagin dual $M^* = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$ is profinite w/ the compact-open topology. Indeed,

$$M^* = \mathrm{Hom}(\varinjlim_{N \leq M \text{ finite}} N, \mathbb{Q}/\mathbb{Z}) = \varprojlim_{N \leq M \text{ finite}} \mathrm{Hom}(N, \mathbb{Q}/\mathbb{Z}).$$

In fact, $(\cdot)^*$ is an antiequivalence between discr. tors. ab. gps and abelian profinite groups.
(For G abelian profinite, $\mathrm{Hom}_{\text{cont.}}(G, \mathbb{Q}/\mathbb{Z})$ is discr. tors. ab. CAUTION: For $M = \mathbb{Z}$, we have $M^* = \mathbb{Q}/\mathbb{Z} \cong \underbrace{\bigoplus_p \mathbb{Z}(p^\infty)}_{\text{Prüfer p-group } \varinjlim_n \mathbb{Z}/p^n}$, so $M^{**} \cong \prod_p \mathbb{Z}_p \cong \underbrace{\hat{\mathbb{Z}}}_{\varprojlim_n \mathbb{Z}/n}$.)

- For all $v \in V_f(k)$, the groups $\mathcal{O}_v$ and $\mathcal{O}_v^*$ are profinite (in particular $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$).

Until further notice, let G be a profinite group.

<u>Def. III.4.3</u> A discrete G-module is a discrete abelian group A w/ a continuous action $G \curvearrowright A$.

This means for all $a \in A$, the orbit map $G \to A$, $g \mapsto g \cdot a$ is continuous ($\Leftrightarrow$ $G_a = \{g \in G \mid ga = a\}$ is open).

<u>Examples w/ $G = \mathrm{Gal}(k)$:</u> • $A = \bar{k}^*$. For $a \in \bar{k}^*$, we have $G_a = \mathrm{Gal}(\bar{k}/k(a))$ is closed and has finite index by infinite Galois theory, so G_a is open.

- $A = \mu_n(\bar{k})$ (an invariant submodule of $\bar{k}^*$)

- The trivial discrete G-module M (e.g. $M = \mathbb{Z}/n$, to be distinguished from $\mu_n(\bar{k})$.)
- The previous examples $\bar{k}^*$, $\mu_n(\bar{k})$, $\mathbb{Z}/n$ are examples of commutative affine group schemes over k (cf. Chapter IV): GL_1, μ_n, $\mathbb{Z}/n$ (constant) and $(\sigma : \bar{k} \to \bar{k}) \in G$ acts functorially.
- Let M be a finite commutative group scheme over k. Then the Cartier dual of M is $M' = \mathrm{Hom}(M, GL_1)$ w/ G-action given by $\sigma.f(m) = \sigma.f(\sigma^{-1}.m)$.

For instance $(\mu_n)' = \mathrm{Hom}(\mu_n, GL_1) = \mathrm{Hom}(\mu_n, \mu_n)$
$= \{ (\cdot)^k \mid k = 0, \dots, n-1 \}$ and $\sigma(\sigma^{-1} z)^k = z^k$,
so $G \curvearrowright (\mu_n)'$ is trivial which means $\mu_n' = \mathbb{Z}/n$, $(\mathbb{Z}/n)' = \mu_n$.

Let $\underline{G\text{-mod}^\delta}$ be the category of discrete G-modules. Then $\underline{G\text{-mod}^\delta}$ has enough injectives (take $0 \to A \to I$ in $\mathbb{Z}G$-mod, then $0 \to A \to \operatorname{colim}_{U \leq_o G} I^U$), hence:

<u>Def. III.4.4</u> For a discrete G-module A, we define $H^i(G, A)$ as the right derived functors of $(\cdot)^G$.

However, $\underline{G\text{-mod}^\delta}$ does NOT have enough projectives. (Note that the $\mathbb{Z}G$-module $\mathbb{Z}G$ is not discrete because the stabilizer of $1 \in \mathbb{Z}G$ is trivial.)
For explicit computations, we therefore define more generally $K^i(G, A) = \{ f : G^i \to A \ \underset{(\Leftrightarrow \text{ loc. const.})}{\text{continuous}} \}$.
and $d^i(f) = f \circ d_i$ w/ d_i as in III.1.4).

<u>Theorem III.4.5</u> For every discrete G-module A, we have $H^i(G, A) = H^i(K^\bullet(G, A))$. $\square$

<u>Prop. III.4.6</u> Let (G_i) be an inverse system of (pro-)finite groups and (A_i) be an inductive system of discrete G_i-modules s.t.
$$\begin{tikzcd} G_j \arrow[r] \arrow[d, "\cdot a"'] & G_i \arrow[d, "\cdot a"] \\ A_j & A_i \arrow[l] \end{tikzcd}$$
for all $a \in A_i$. Set $G = \varprojlim_i G_i$ and $A = \varinjlim_i A_i$.
Then $H^q(G, A) = \varinjlim_i H^q(G_i, A_i)$.

Proof. Even stronger, we have that the colimit map

$$\varinjlim_i K^\bullet(G_i, A_i) \longrightarrow K^\bullet(G, A)$$

is an isomorphism. $\square$

Cor. III.4.7. $H^q(G, A) = \varinjlim_{U \trianglelefteq_o G} H^q(G/U, A^U)$.

Proof. $G = \varprojlim G/U$ as discussed above and $A = \varinjlim A^U$ because $a \in A$ lies in A^{G_a}. $\square$

Cor. III.4.8 $H^q(G, A)$ is torsion abelian for $q \geq 1$.

Proof. Follows from III.4.7 and the fact that for finite G, $H \leq G$ and $q \geq 1$, the homomorphism

$$\mathrm{cores}_H \circ \mathrm{res}_H : H^q(G, A) \longrightarrow H^q(G, A)$$

is multiplication w/ $[G:H]$ (apply to $H = \{1\}$).
(see "Oberseminar Algebra und Geometrie".) $\square$

III.5 Galois cohomology

In this section, let $G = \mathrm{Gal}(k)$ and $A \in \underline{G\text{-mod}^\delta}$.
Given an extension k_1/k and an alg. closure $\overline{k}_1/k$, we can find

$$\begin{array}{ccc} \overline{k} & \xrightarrow{j} & \overline{k}_1 \\ \uparrow & & \uparrow \\ k & \xrightarrow{i} & k_1 \end{array}$$

inducing $f: \mathrm{Gal}(k_1) \longrightarrow \mathrm{Gal}(k)$. Replacing j w/ j'

gives $f'(\sigma) = j'^{-1} \circ \sigma \circ j' = j'^{-1} \circ (j \circ j^{-1}) \circ \sigma \circ (j \circ j^{-1}) \circ j'$

$$= (j'^{-1} \circ j) \circ j^{-1} \circ \sigma \circ j \circ (j^{-1} \circ j')$$
$$= \tau^{-1} \circ f(\sigma) \circ \tau$$

w/ $\tau = j^{-1} \circ j' \in Gal(k)$.

<u>Prop. III.5.1</u> Let $\tau \in G$. Then $\sigma \mapsto \tau^{-1}\sigma\tau$ and $a \mapsto \tau a$ induce an automorphism Φ_τ of $H^q(G, A)$ and $\Phi_\tau = id$.

(Functoriality: $f: G' \to G$, $g: A \to A'$ (additive) w/ $g(f(\sigma').a) = \sigma'.g(a)$ induce $H^q(G, A) \to H^q(G', A')$.)

<u>Proof</u> Can be checked on the cocycle description of $H^1(G, A)$. General case by homological algebra. □

Hence the induced homomorphism
$$H^q(Gal(k), A) \longrightarrow H^q(Gal(k_1), A)$$
is independent of j. In particular, for $k_1 = k$ we conclude that any two algebraic closures $\bar{k}, \bar{k}_1$ give canonically isomorphic
$$H^q(Gal(k), A) \cong H^q(Gal(k_1), A),$$
so we may write
$$H^q(k, A) := H^q(Gal(k), A)$$
the q-th Galois cohomology of k w/ coeff. in A.

If A is a commutative affine group scheme over k and k_1/k is any field extension, then $f: \mathrm{Gal}(k_1) \to \mathrm{Gal}(k)$ and $g: A(\bar{k}) \to A(\bar{k}_1)$ satisfy $g(f(\sigma).a) = \sigma.g(a)$, hence we obtain

$$\begin{array}{ccc} H^q(\mathrm{Gal}(k), A(\bar{k})) & \longrightarrow & H^q(\mathrm{Gal}(k_1), A(\bar{k}_1)) \\ \| & & \| \\ H^q(k, A) & \longrightarrow & H^q(k_1, A) \end{array}$$

well-defined and functorial in k, i.e. A defines

$$H^q(\cdot, A): \underline{\text{field ext.}/k} \longrightarrow \underline{\text{ab. groups}}$$

<u>Examples</u>. 1.) $A = \mathbb{G}_a$, the additive group scheme over k w/ $\mathbb{G}_a(\bar{k}) = (\bar{k}, +)$:

<u>Thm. III.5.2</u>. $\hat{H}^q(K, \mathbb{G}_a) = 0$ for all K/k and all $q \in \mathbb{Z}$.

<u>Proof</u>. Every finite Galois extension L/K has a normal basis, i.e. $L = \bigoplus_{\sigma \in \mathrm{Gal}(L/K)} K\sigma(x)$ for some $x \in L$. This means L is $\mathrm{Gal}(L/K)$-induced (Def.: A is G-induced if $A \cong \bigoplus_{g \in G} gD$ for some $D \leq A$.) A G-induced module A has trivial cohomology because $\mathrm{Hom}_{\mathbb{Z}G}(X_\cdot, A) \cong \mathrm{Hom}_{\mathbb{Z}}(X_\cdot, D)$ w/ $X_\cdot$ as in III.3 is exact since each X_q is $\mathbb{Z}$-free.

Hence $H^q(K, \mathbb{G}_a) \cong \varinjlim_{L/K \text{ fin. Gal.}} H^q(\mathrm{Gal}(L/K), L) = 0$

by III.4.7 (which provides isos of the complexes). $\square$

2.) $A = \mathbb{G}_m = GL_1$, the multiplicative group scheme over k w/ $\mathbb{G}_m(\bar{k}) = (\bar{k}^*, \cdot)$:

Thm. III.5.3. ("Hilbert 90") $H^1(k, \mathbb{G}_m) = 0$.

Proof. As above, it is enough to show that $H^1(\mathrm{Gal}(L/k), L^*) = 0$ for every finite Galois extension L/k. Set $G := \mathrm{Gal}(L/k)$. Let $\sigma \mapsto a_\sigma$ be a cocycle in $Z^1(G, L^*)$. By Dedekind's theorem, $G \subseteq \mathrm{Hom}_k(L, L)$ is linearly independent over L, hence we find $x \in L^*$ such that $b := \sum_{\sigma \in G} a_\sigma \cdot \sigma(x) \neq 0$. For all $\tau \in G$, we conclude

$$\tau(b) = \sum_{\sigma \in G} {}^{\tau}a_\sigma \cdot \tau\sigma(x) = \sum_{\sigma \in G} a_{\tau\sigma} \cdot a_\tau^{-1} \tau\sigma(x) =$$

$$= a_\tau^{-1} \sum_{\sigma \in G} a_\sigma \sigma(x) = a_\tau^{-1} \cdot b,$$

so $a_\tau = b \cdot \tau(b)^{-1} = \tau(b^{-1}) \cdot (b^{-1})^{-1}$ is a coboundary. $\square$

Exercise. Show that if $\mathrm{Gal}(L/k) = \langle \sigma \rangle$ is cyclic then for every $x \in L^*$ w/ $N_{L/k}(x) = 1$, there exists $c \in L^*$ such that $x = \frac{\sigma(c)}{c}$. (Hilbert's original Thm. 90)
(Hint: Use that $\hat{H}^{-1}(G, A) \cong \hat{H}^1(G, A)$ for cyclic G.)

Def. III.5.4 The abelian group $H^2(k, \mathbb{G}_m)$ is called the **Brauer group** $\mathrm{Br}(k)$ of k.

3.) $A = \mu_n$, the finite abelian group scheme of n-th roots of unity:

<u>Thm. III.5.5</u> $\quad H^1(k, \mu_n) \cong k^*/(k^*)^n$.

<u>Proof</u> $\quad 1 \to \mu_n \to G_m \xrightarrow{(\cdot)^n} G_m \to 1$, meaning

$1 \to \mu_n(\bar{k}) \to \bar{k}^* \xrightarrow{(\cdot)^n} \bar{k}^* \to 1$ is exact, gives

$$k^* \xrightarrow{(\cdot)^n} k^* \xrightarrow{\delta^0} H^1(k, \mu_n) \to H^1(k, G_m) \overset{H.90}{=} 0$$

hence $\quad H^1(k, \mu_n) \cong \operatorname{coker}(k^* \xrightarrow{(\cdot)^n} k^*) = k^*/(k^*)^n$. $\quad \square$

<u>Thm. III.5.6</u> $\quad H^2(k, \mu_n) \cong Br(k)[n]$, the subgroup of $Br(k)$ of elements whose order divides n.

<u>Proof</u>

$0 = H^1(k, G_m) \xrightarrow{\delta^1} H^2(k, \mu_n) \to H^2(k, G_m) \xrightarrow{(\cdot)^n} H^2(k, G_m)$,

hence $\quad H^2(k, \mu_n) \cong \ker(Br(k) \xrightarrow{(\cdot)^n} Br(k)) = Br(k)[n]$. $\square$

<u>Cor. III.5.7</u> If k contains a primitive n-th root of unity, then $H^1(k, \mathbb{Z}/n) = k^*/(k^*)^n$ and $H^2(k, \mathbb{Z}/n) \cong Br(k)[n]$.

<u>Proof</u>. In that case $\mu_n(\bar{k}) \subseteq k^*$, so that $\mu_n \cong \mathbb{Z}/n$ is a trivial $Gal(k)$-module. $\square$

4.) "Hilbert 90" has the following noncommutative generalization (for any field K).

<u>Thm III.5.8</u> $\quad H^1(K, GL_n) = 0$.

Proof. As before, for a cocycle $\sigma \mapsto a_\sigma$, form $b = \sum_{\sigma \in G} a_\sigma \cdot \sigma(x)$ and check that $\tau(b) = a_\tau^{-1} \cdot b$.
Then show that $x \in GL_n(L)$ for L/K finite Galois can be so chosen that b is invertible. $\square$

III.6 The Brauer group and local duality

Recall that every CSA A over a (say perfect) field K is of the form $A \cong M_n(D_A)$ for a uniquely determined division algebra D_A over K.
Define $A \sim B \;:\Leftrightarrow\; D_A \cong D_B$, then "$\otimes_K$" endows the set of equivalence classes of CSAs over K w/ a well-defined structure of an abelian group $CSA(K)$.

Thm. III.6.1 $CSA(K) \cong Br(K)$.

Proof. $\mathrm{Aut}(M_n(\bar{K})) \cong PGL_n(\bar{K})$ by Skolem-Noether,

$$1 \to GL_1 \to GL_n \to PGL_n \to 1$$

$$\rightsquigarrow \quad \underset{\substack{\| \text{ III.5.7} \\ 0}}{H^1(K, GL_n)} \longrightarrow H^1(K, PGL_n) \xrightarrow{\delta_n^1} H^2(K, GL_1)$$

This defines $CSA(K) \to Br(K)$ which gives the iso.

$$A \mapsto \delta^1_{\sqrt{\dim_K A}}([A])$$ $\square$

Examples 1.) If $K = \bar{K}$, then $Br(K) = 0$.
2.) If K is finite, then $Br(K) = 0$ by

III.6.1 and Wedderburn's thm. that every finite skew field is a field. (Proof from the BOOK).

3.) $Br(\mathbb{R}) \cong \mathbb{Z}/2$ because the only central division algebras over $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{H}$.

4.) If $K/\mathbb{Q}_p$ has finite degree, then $Br(K) \cong \mathbb{Q}/\mathbb{Z}$:
(Recall from Oberseminar on class field theory)
If K_{ur}/K is the maximal unramified extension, then $Gal(K_{ur}/K) \cong \hat{\mathbb{Z}}$, so for each n there exists a unique unramified ext. L_n/K and for all L/K w/ $[L:K]=n$, we have
$H^2(L/K, \mathbb{G}_m) = H^2(L_n/K, \mathbb{G}_m) \leq H^2(K, \mathbb{G}_m)$.
Hence $Br(K) = \operatorname{colim}_n H^2(L_n/K, \mathbb{G}_m)$ and
$inv_{L_n/K}: H^2(L_n/K, \mathbb{G}_m) \xrightarrow{\cong} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, so $Br(K) \cong \mathbb{Q}/\mathbb{Z}$. □

<u>Cor. III.6.2</u> $H^1(K, \mu_n) \cong K^*/(K^*)^n$ is finite and so is $H^2(K, \mu_n) \cong (\mathbb{Q}/\mathbb{Z})[n] \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$. □

A spectral sequence argument then implies that actually $H^i(K, M)$ is finite for every finite commutative $Gal(K)$-module M.

5.) From global class field theory, we have
<u>Thm. III.6.3</u> (Albert - Brauer - Hasse - Noether)
$$1 \to Br(k) \to \bigoplus_{v \in V(k)} Br(k_v) \to \mathbb{Q}/\mathbb{Z} \to 1. \quad \square$$

Again let $K/\mathbb{Q}_p$ be a p-adic field and let M be a finite commutative group scheme over K (equivalently, a finite commutative (discrete) $\mathrm{Gal}(K)$-module). Evaluation gives a pairing of $\mathrm{Gal}(K)$-modules $M \times M' \longrightarrow \mathbb{G}_m$ inducing a cup product

$$H^i(K, M) \times H^{2-i}(K, M') \longrightarrow \mathrm{Br}(K) = \mathbb{Q}/\mathbb{Z}.$$

Thm. III.6.4 (Local Tate duality) For $i = 0, 1, 2$,

$$H^i(K, M) \times H^{2-i}(K, M') \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing of finite abelian groups.

Proof. One checks that the functor

$$\begin{aligned} (\underline{\mathrm{Gal}(K)\text{-}\mathrm{mod}^{\delta}_{\mathrm{finite}}})^{op} &\longrightarrow \underline{\text{ab. groups}} \\ A &\longmapsto H^2(K, A)^* \end{aligned}$$

is represented by $\mu(\bar{K}) = \mathrm{colim}_n\, \mu_n(K)$, i.e. $H^2(K, A)^* \cong \mathrm{Hom}_{\mathrm{Gal}(K)}(A, \mu)$ naturally in A.
Since $\mathrm{Hom}_{\mathrm{Gal}(K)}(M, \mu) = \mathrm{Hom}_{\mathrm{Gal}(K)}(M, \mathbb{G}_m) = H^0(K, M')$, this shows $H^2(K, M)^* \cong H^0(K, M')$ and this iso. is implemented by the cup product.
This shows the case $i=2$. For $i=0$, replace M by M'.
For $i=1$, verify that $H^1(K, M) \to H^1(K, M')^*$ is inj. $\square$

III.7 Unramified cohomology

Still let $K/\mathbb{Q}_p$ be a finite extension.

Def. III.7.1 We call $A \in \underline{\mathrm{Gal}(K)\text{-mod}^{\delta}}$ unramified if $\mathrm{Gal}(\bar{K}/K_{ur})$ acts trivially on A. In that case, we set $H^i_{ur}(K, A) = H^i(\mathrm{Gal}(K_{ur}/K), A)$.

Prop. III.7.2 Suppose A is finite and unramified. Then $H^0_{ur}(K, A) = H^0(K, A)$ and $H^i_{ur}(K, A) = 0$ for $i \geq 2$. For $i = 1$, $H^1_{ur}(K, A) \leq H^1(K, A)$ is a (possibly nontrivial, possibly proper) subgroup.

Proof $H^0_{ur}(K, A) = A^{\mathrm{Gal}(K_{ur}/K)} = A^{\mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/K_{ur})}$ $= A^{\mathrm{Gal}(\bar{K}/K)} = H^0(K, A)$. That $H^i_{ur}(K, A) = 0$ for $i \geq 2$ follows from $cd(\hat{\mathbb{Z}}) = 1$ [cohomological dimension, use $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ and $H^2(\mathbb{Z}/p^n, \mathbb{Z}/p) \overset{\text{period.}}{\cong} \hat{H}^0(\mathbb{Z}/p^n, \mathbb{Z}/p)$ $\cong H^0(\mathbb{Z}/p^n, \mathbb{Z}/p) \cong \mathbb{Z}/p$, so $H^2(\mathbb{Z}_p, \mathbb{Z}/p) \overset{\text{III.4.6}}{\cong}$ $\cong \varinjlim_n H^2(\mathbb{Z}/p^n; \mathbb{Z}/p) = 0$ because the transition maps are $\mathbb{Z}/p \xrightarrow{\cdot p} \mathbb{Z}/p$, hence are trivial. For G pro-p, $cd_p(G) \leq n$ if $H^{n+1}(G, \mathbb{Z}/p) = 0$, so $cd_p(\mathbb{Z}_p) \leq 1$. But $H^1(\mathbb{Z}_p, \mathbb{Z}/p) = \mathrm{Hom}_c(\mathbb{Z}_p, \mathbb{Z}/p) = \mathrm{Hom}(\mathbb{Z}_p/p\mathbb{Z}_p, \mathbb{Z}/p)$ $= \mathbb{Z}/p$, so $cd_p(\mathbb{Z}_p) = 1$ whence $cd(\hat{\mathbb{Z}}) = \sup_p cd_p(\mathbb{Z}_p) = 1$.]
Lastly, $0 \to H^1_{ur}(K, A) \to H^1(K, A)$ by inf-res. $\square$

With respect to local Tate duality (III.6.4) we have:

- If A is finite unramified, then so is A'.
- We have $H^i_{nr}(K,A)^\perp = H^{2-i}_{nr}(K,A')$ for $i=0,1,2$.

Exercise. (i) Show that μ_n is unramified if $p \nmid n$.
(ii) Show that then $H^1_{nr}(K,\mu_n) \cong \mathcal{O}_K^* / (\mathcal{O}_K^*)^n$.
(Hint: use that $\mathcal{O}_K^{nr*} \leq K_{nr}^*$ has $H^1_{nr}(K, \mathcal{O}_K^{nr*}) = 0$.)

III.8 Poitou-Tate duality

Let M be a finite $\mathrm{Gal}(k)$-module.

Goal: Find a local-global principle informing about the diagonal maps $\beta_i : H^i(k,M) \longrightarrow \prod_{v\in V(k)} H^i(k_v, M)$.

Convention: If $i=0$ and $v \in V_\infty(k)$, then in this section $H^i(k_v, M)$ shall mean $\hat{H}^0(k_v,M)$, so $H^0(k_v,M)=0$ for v complex and $H^0(k_v,M) \cong M^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})} / N_{\mathrm{Gal}(\mathbb{C}/\mathbb{R})} M$ for v real.

Prop. III.8.1 The module M is unramified outside finitely many $v \in V(k)$ (as $\mathrm{Gal}(k_v)$-module).

Proof. The subgroup $G = \{\sigma \in \mathrm{Gal}(k) \mid \sigma.m = m$ for all $m \in M\} \leq \mathrm{Gal}(k)$ is open, hence of finite index and the corresponding field extension l/k is unramified at all $v \nmid \mathrm{discr}_{l/k}$. So $\mathrm{Gal}(k_v^{nr}) \leq \mathrm{Gal}(l_w) \leq \mathrm{Gal}(l)$ acts trivially for any $w \mid v \nmid \mathrm{discr}_{l/k}$. $\square$

__Def. III.8.2__ We define $P^i(k,M)$ as the restricted product
$$P^i(k,M) = \prod_{v\in V(k)}{}' H^i(k_v,M) \quad \text{w.r.t.} \quad H^i_{ur}(k_v,M).$$

Hence III.7.2 implies

- $P^0(k,M) = \prod_v H^0(k_v,M)$ is compact,
- $P^2(k,M) = \bigoplus_v H^2(k_v,M) = \coprod_v H^2(k_v,M)$ is discrete,
- $P^1(k,M) = \prod_v{}' H^1(k_v,M) = \amalg_v H^1(k_v,M)$ is locally compact (notation "$\amalg$" suggested by Tate).

Moreover $P^i(k,M) = \bigoplus_{v \text{ real}} H^i(k_v,M)$ for $i\geq 3$ because $cd(Gal(k_v)) = 2$ for v finite. [Indeed,
$$cd(Gal(k_v)) \leq \underbrace{cd(Gal(k_v^{ur}))}_{\leq 1 \text{ "because" } Br(k_v^{ur})=0} + \underbrace{cd(Gal(k_v^{ur}/k_v))}_{\leq 1 \text{ as above}} \leq 2$$
and $H^2(k_v,\mu_n) \cong \mathbb{Z}/n\mathbb{Z}$ by III.6.2.]

__Prop. III.8.3__ The diagonal map
$$\beta^i = \beta^i_M : H^i(k,M) \longrightarrow \prod_{v\in V(k)} H^i(k_v,M)$$
has image in $P^i(k,M)$.

__Proof.__ Let $\alpha\in H^i(k,M)$. Pick l/k finite Galois w/ $\alpha\in H^i(l/k,M)$ and $Gal(l) \curvearrowright M$ trivially.
If v is unramified in l/k and $w\mid v$ is any place of l, then
$$\begin{tikzcd} H^i(l/k,M) \arrow[d] & \leq H^i(k,M) \arrow[r] & H^i(k_v,M) \\ H^i(l_w/k_v,M) \arrow[r] & H^i(k_v^{ur}/k_v,M) \arrow[ur] & \end{tikzcd}$$
shows that α maps to $H^i_{ur}(k_v,M)$ for a.a. v. $\square$

Prop. III.8.4 ("Real local duality") Let M_0 be a finite $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-module. Then cup product defines a perfect pairing of finite abelian 2-groups

$$\hat{H}^i(\mathbb{R}, M_0) \times \hat{H}^{2-i}(\mathbb{R}, M_0') \longrightarrow \mathrm{Br}\,\mathbb{R} \cong \mathbb{Z}/2\mathbb{Z}. \quad \square$$

Prop. III.8.5 Tate local duality induces isos $P^0(k, M)^* \cong P^2(k, M')$ and $P^1(k, M)^* \cong P^1(k, M')$.

Proof. For $i = 0, 1, 2$, we have $P^i(k, M)^* = \left(\prod_v{}' H^i(k_v, M)\right)^* \cong \prod{}' H^i(k_v, M)^*$ restricted w.r.t. $\left(H^i(k_v, M)/H^i_{ur}(k_v, M)\right)^*$. Hence by III.6.4 & III.8.4,

$P^i(k, M)^* \cong \prod{}' H^{2-i}(k_v, M')$ restricted w.r.t.

$\left(H^i(k_v, M)/H^i_{ur}(k_v, M)\right)^* \cong H^i_{ur}(k_v, M)^{\perp} = H^{2-i}_{nr}(k_v, M'). \quad \square$

Correspondingly, let $\gamma_i : P^i(k, M) \longrightarrow H^{2-i}(k, M')^*$ be the dual of $\beta^{2-i}_{M'} : H^{2-i}(k, M') \longrightarrow P^{2-i}(k, M')$ and recall that we have $\ker \beta^i_M = Ш^i(k, \emptyset, M) =: Ш^i(k, M)$ (see Sec. II.7).

Thm. III.8.6 (Poitou-Tate)

(i) For $i \geq 3$, we have $H^i(k, M) \cong \bigoplus_{v \text{ real}} H^i(k_v, M)$.

(ii) The Tate-Shafarevich groups $Ш^1(k, M')$ and $Ш^2(k, M)$ are finite and dual to each other.

(iii) We have a 9-term exact sequence

$$
\begin{tikzcd}
0 \arrow[r] & H^0(k,M) \arrow[r, "\beta^0"] & \prod\limits_v H^0(k_v,M) \arrow[r, "\gamma^0"] & H^2(k,M')^* \arrow[dll, "\delta^1"'] \\
 & H^1(k,M) \arrow[r, "\beta^1"] & \prod\limits_v{}' H^1(k_v,M) \arrow[r, "\gamma^1"] & H^1(k,M')^* \arrow[dll, "\delta^2"'] \\
 & H^2(k,M) \arrow[r, "\beta^2"] & \coprod\limits_v H^2(k_v,M) \arrow[r, "\gamma^2"] & H^0(k,M')^* \arrow[r] & 0.
\end{tikzcd}
$$

$\square$

The boundary map δ^1 arises as

$$H^2(k,M')^* \longrightarrow \operatorname{coker}(\gamma^0) = \operatorname{coker}(\beta^{2\,*}_{M'}) = (\ker(\beta^2_{M'}))^* =$$

$$= (Ш^2(k,M'))^* \overset{(ii)}{=} Ш^1(k,M) \leq H^1(k,M)$$

and similarly for δ^2.

<u>Example</u> $\cdot$ $k=\mathbb{Q}$, $M=\mathbb{Z}/2$: (Recall $\mathbb{Z}/2' \cong \mu_2 \cong \mathbb{Z}/2$.)

$$
\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/2 \arrow[r] & \prod\limits_{p\leq\infty} \mathbb{Z}/2 \arrow[r] & \mathrm{Br}(\mathbb{Q})[2]^* \arrow[dll, "0"'] \\
 & \mathbb{Q}^*/(\mathbb{Q}^*)^2 \arrow[r] & I_{\mathbb{Q}}/I_{\mathbb{Q}}^2 \arrow[r] & \left(\mathbb{Q}^*/(\mathbb{Q}^*)^2\right)^* \arrow[dll, "0"'] \\
 & \mathrm{Br}(\mathbb{Q})[2] \arrow[r] & \bigoplus\limits_{p\leq\infty} \mathbb{Z}/2 \arrow[r] & \mathbb{Z}/2^* \arrow[r] & 0.
\end{tikzcd}
$$

II.6.1

II.6.6 $(d=2)$

- Recall from Thm. II.6.4 that $\mathbb{Z}/2 \cong Ш^1(\mathbb{Q}(\sqrt{7}),\mu_8) \cong Ш^2(\mathbb{Q}(\sqrt{7}),\mathbb{Z}/8)$, so for $k=\mathbb{Q}(\sqrt{7})$, the first boundary map is non-trivial if $M=\mu_8$ and the second boundary map is non-trivial if $M=\mathbb{Z}/8$.

Note that the dual of the P.-T. seq for M is the P.-T. seq. for M'. Note also that topologically, the P.-T. seq. is of the form

$$\begin{aligned} 0 &\to \text{finite} \to \text{compact} \to \text{compact} \\ &\to \text{discrete} \to \text{loc. cpt.} \to \text{compact} \\ &\to \text{discrete} \to \text{discrete} \to \text{finite} \to 0 . \end{aligned}$$

IV Galois cohomology of simple algebraic groups

IV.1 Noncommutative cohomology

Let G be a profinite group.

Def. IV.1.1 A **G-set** is a discrete top. space A w/ a continuous G-action. If A carries moreover a group structure preserved by the action ($^\sigma(ab) = {}^\sigma a\, {}^\sigma b$ for $a, b \in A$, $\sigma \in G$), then we call A a **G-group**.

Observe that a G-group w/ abelian G is just a discrete G-module as in Def. III.4.3.

Proceed as in Chapter I:

- For a G-set E, set $H^0(G, E) = E^G$.
- For a G-group A, set $Z^1(G, A) = \{a : G \to A \mid a_{\sigma\tau} = a_\sigma {}^\sigma a_\tau \text{ for all } \sigma \in G\}$.
- For $a, a' \in Z^1(G, A)$, define $a \sim a'$ iff there exists $b \in A$ such that $a_\sigma = b^{-1} a'_\sigma {}^\sigma b$ for all $\sigma \in G$.
- Set $H^1(G, A) = Z^1(G, A)/\sim$ (pointed set).

One checks:

- $H^1(G, A) = \varinjlim_{U \trianglelefteq_o G} H^1(G/U, A^U)$,
- $H^i(G, A)$ is functorial in A for $i = 0, 1$,
- " coincides w/ the prev. def. if A is comm.

Prop. IV.1.2 (cf. Prop. I.4) Let $A \trianglelefteq_G B$ be G-groups. Then $G \curvearrowright B/A$ is a G-set (G-group) and

$$1 \to H^0(G,A) \to H^0(G,B) \to H^0(G, B/A) \xrightarrow{\delta^0} H^1(G,A) \xrightarrow{i^1} H^1(G,B) \xrightarrow{j^1} H^1(G, B/A)$$ is exact.

Description of δ^0: For $bA \in (B/A)^G$, set $\delta^0(bA) = [b^{-1} \cdot {}^\sigma b]$.

Exercise: (i) Check $\delta^0(bA)$ is a well-defined 1-cocycle and prove IV.1.2.

Observe that for $A \trianglelefteq_G B$, we have an action $(B/A)^G \curvearrowright H^1(G,A)$ defined as follows: For $bA \in (B/A)^G$ and $[a] \in H^1(G,A)$, set $bA . [a] = [\sigma \mapsto b^{-1} a_\sigma {}^\sigma b]$.

Prop. IV.1.3 $i^1(\alpha) = i^1(\alpha')$ iff $\alpha' \in (B/A)^G . \alpha$.

Proof. Write $\alpha = [a]$, $\alpha' = [a']$. Then there is $b \in B$ w/ $a'_\sigma = b^{-1} a_\sigma {}^\sigma b$. Then ${}^\sigma b \, a'^{-1}_\sigma = a_\sigma b = b(\underbrace{b^{-1} a_\sigma b}_{\in A})$, so $bA \in (B/A)^G$ and $bA . [a] = [a']$. The converse is clear. $\square$

Prop. IV.1.4 If $A \trianglelefteq_G B$ is central, then

$$H^1(G,B) \to H^1(G, B/A) \xrightarrow{\delta^1} H^2(G,A)$$ is exact and δ^0 is a homomorphism. $\square$

Description of δ^1: Lift $a : G \to B/A$ to $b : G \to B$ (continuity is automatic) and set $\delta^1([a]) = [(\sigma,\tau) \mapsto b_\sigma {}^\sigma b_\tau b_{\sigma\tau}^{-1}]$.

IV.2 Twisting

Let $1 \to A \xrightarrow{i} B \xrightarrow{p} C \to 1$ be a S.E.S. of G-groups and let $\beta = [b] \in H^1(G, B)$.

To describe the fiber $(p^1)^{-1}(p^1(\beta))$ of the map

$$p^1 : H^1(G, B) \longrightarrow H^1(G, C),$$

we define the twisted G-group ${}_bB$ which equals B as a group but the new G-action is given by ${}^{\sigma\prime}x := b_\sigma \cdot {}^{\sigma}x \cdot b_\sigma^{-1}$ for $x \in B$, $\sigma \in G$. This also defines ${}_bA$ because $A \trianglelefteq B$ and ${}_bC := {}_{p \circ b}C$. So we have $1 \to {}_bA \to {}_bB \to {}_bC \to 1$ and correspondingly

$$\begin{tikzcd}
H^1(G, A) \arrow[r, "i^1"] & H^1(G, B) \arrow[r, "p^1"] & H^1(G, C) \\
H^1(G, {}_bA) \arrow[r, "{}_bi^1"] & H^1(G, {}_bB) \arrow[u, "\tau_b", "\cong"'] \arrow[r, "{}_bp^1"] & H^1(G, {}_bC) \arrow[u, "\tau_{p \circ b}", "\cong"']
\end{tikzcd}$$

where τ_b, defined by $\tau_b([x]) = [x \cdot b]$, and $\tau_{p \circ b}$ are bijections sending the trivial class to β and $p^1(\beta)$, respectively. This transforms the fiber of β into $\ker {}_bp^1$. Similarly, for a central ext.

$$1 \to A \xrightarrow{i} B \xrightarrow{p} C \to 1$$

of G-groups and $\gamma = [c] \in H^1(G, C)$, we get

$$\begin{tikzcd}
H^1(G, B) \arrow[r] & H^1(G, C) \arrow[r, "\delta^1"] & H^2(G, A) \\
H^1(G, {}_cB) \arrow[r] & H^1(G, {}_cC) \arrow[u, "\tau_c", "\cong"'] \arrow[r, "{}_c\delta^1"] & H^2(G, A)
\end{tikzcd}
\qquad 1 \mapsto \gamma$$

w/ $\delta^1(\tau_c(\gamma')) = {}_c\delta^1(\gamma') + \delta^1(\gamma)$, so $(\delta^1)^{-1}(\delta^1(\gamma)) \cong \ker {}_c\delta^1$.

IV.3 Noncommutative Galois cohomology and forms

From now on, let K be perfect. Recall from Chap. I:

Meta-thm. IV.3.1

If L/K is Galois and X is a "K-object", then
$$\underbrace{\{Y \text{ } K\text{-object} \mid X \cong_L Y\}}_{\text{"}L/K\text{-forms of } X\text{"}} / \cong_K \quad \overset{1:1}{\longleftrightarrow} \quad H^1(L/K, \mathrm{Aut}_L X).$$

Meta-proof. Let Y be a K-object and $f: X \xrightarrow{\cong_L} Y$.

Set $a: \mathrm{Gal}(L/K) \longrightarrow \mathrm{Aut}_L X$, $\sigma \mapsto a_\sigma = f^{-1} \circ {}^\sigma f$.

Then
$$a_{\sigma\tau} = f^{-1} \circ {}^{\sigma\tau} f = f^{-1} \circ {}^\sigma(f \circ (f^{-1} \circ {}^\tau f)) =$$
$$= (f^{-1} \circ {}^\sigma f) \circ {}^\sigma(f^{-1} \circ {}^\tau f) = a_\sigma \circ {}^\sigma a_\tau,$$
so we may assign $Y \mapsto [a] \in H^1(L/K, \mathrm{Aut}_L X)$.

Since two $f, f': X \xrightarrow{\cong_L} Y$ satisfy $f' = f \circ \underbrace{(f^{-1} \circ f')}_{=: b \in \mathrm{Aut}_L X}$,

we have $a'_\sigma := f'^{-1} \circ {}^\sigma f' = b^{-1} \circ (f^{-1} \circ {}^\sigma f) \circ {}^\sigma b$, so $[a] = [a']$ is well-defined.

Injectivity: Suppose Y_1 and Y_2 define $[f_1^{-1} \circ {}^\sigma f_1] = [f_2^{-1} \circ {}^\sigma f_2]$. Then there exists $b \in \mathrm{Aut}_L X$ s.t.
$$f_2^{-1} \circ {}^\sigma f_2 = b^{-1} \circ f_1^{-1} \circ {}^\sigma f_1 \circ {}^\sigma b = (f_1 \circ b)^{-1} \circ {}^\sigma (f_1 \circ b).$$
Hence
$${}^\sigma(f_2 \circ b^{-1} \circ f_1^{-1}) = {}^\sigma f_2 \circ {}^\sigma(f_1 \circ b)^{-1} = {}^\sigma f_2 \circ {}^\sigma f_2^{-1} \circ f_2 \circ b^{-1} \circ f_1^{-1}$$
$$= f_2 \circ b^{-1} \circ f_1^{-1},$$

so the iso. $f_2 \circ b^{-1} \circ f_1^{-1}$ is def. over K, hence $Y_1 \cong_K Y_2$.

Surjectivity: Use $[a] \in H^1(L/K, \mathrm{Aut}_L X)$ to "twist"

the action $\mathrm{Gal}(L/K) \curvearrowright X_L$ and let ${}_aX = X_L/_{\mathrm{Gal}(L/K)}$.
Then ${}_aX \mapsto [a]$. $\square$

<u>Remark:</u> · To ensure $X_L/_{\mathrm{Gal}(L/K)}$ defines a K-object, one typically has to impose conditions. For example, if X is a K-variety V, it should be quasiprojective (e.g. an algebraic group).

· Similarly, $\mathrm{Aut}\, V$ is not always representable and even if, the representing object might not be of finite type, so some care is necessary when applying the Meta-thm.

· We see that K-objects w/ L-isomorphic automorphism groups have bijectively corresponding K-forms, e.g.

K-objects:	quat. alg.	$\overset{1:1}{\longleftrightarrow}$	Severi-Brauer curves	$\overset{1:1}{\longleftrightarrow}$	rk-3 quadr. forms w/ discr 1
Aut_L :	PGL_2	$=$	PGL_2	$\cong$	SO_3

<u>IV.4 Affine algebraic group schemes</u>

From now on, let $\mathrm{char}(K) = 0$.

<u>Def. IV.4.1</u> An (affine) (algebraic) K-group (scheme) is a functor $G: \underline{K\text{-Alg}} \longrightarrow \underline{\mathrm{Set}}$, representable by a f.g. K-alg. $\mathcal{O}(G)$, together w/ a nat. trafo.

$m : G \times G \longrightarrow G$ s.t. for all $A \in \underline{K\text{-Alg}}$,
$m_A : G(A) \times G(A) \longrightarrow G(A)$ defines a group structure on $G(A)$. Morphisms are nat. trafo.s preserving the gp. structure.

<u>Examples:</u> • μ_n, $\mathcal{O}(\mu_n) = K[X]/(X^n - 1)$.

• A finite group M defines a constant group scheme M w/ $\mathcal{O}(M) = K^M \cong \prod_{g \in M} K$ so that $M(K) = \mathrm{Hom}_{K\text{-alg}}(K^M, K) \cong M$ (standard basis (e_g) of K^M consists of idempotents and $1 = \phi(1) = \sum_{g \in M} \underbrace{\phi(e_g)}_{\in \{0,1\}}$.)

• SL_n, $\mathcal{O}(SL_n) = K[X_{11}, \dots, X_{nn}]/(\det(X_{ij}) - 1)$.

• Let G be a K-group and L/K, then precomp. w/ $\underline{L\text{-Alg}} \to \underline{K\text{-Alg}}$ defines the L-group G_L w/ $\mathcal{O}(G_L) = L \otimes_K \mathcal{O}(G)$ called base extension of G from K to L.

<u>Prop. IV.4.2</u> Let G be an algebraic K-group and L/K Galois. Then $G(L)$ is a $\mathrm{Gal}(L/K)$-group by the functorial action.

<u>Proof.</u> Let $a \in G(L) = \mathrm{Hom}_{K\text{-alg}}(K[X_1, \dots, X_n]/(\dots), L)$ be determined by $\ell_1, \dots, \ell_n \in L$ and set $L_0 = K(\ell_1, \dots, \ell_n)$. Then $\mathrm{Gal}(L/K)_a \supseteq \mathrm{Gal}(L/L_0) \leq_o \mathrm{Gal}(L/K)$.
For $a, b \in G(L)$ and $\sigma \in \mathrm{Gal}(L/K)$, we have
$${}^\sigma(ab) = G(\sigma)(m_L(a,b)) \overset{\text{nat.}}{=} m_L(G(\sigma)(a), G(\sigma)(b)) = {}^\sigma a\, {}^\sigma b. \quad \square$$

- A (normal) algebraic subgroup $\mathbb{H} \leq \mathbb{G}$ is a subfunctor such that $\mathbb{H}(A) \leq \mathbb{G}(A)$ is a (normal) subgroup for all $A \in K\text{-Alg}$ and $\mathbb{H}$ is represented by a quotient of $\mathcal{O}(\mathbb{G})$.
- We have $\{\mathbb{H} \leq \mathbb{G}\} \overset{1:1}{\longleftrightarrow} \{H \leq_c \mathbb{G}(\overline{K}) \mid \mathrm{Gal}(K)(H) \subseteq H\}$.
- Morphisms $\mathbb{G}_1 \to \mathbb{G}_2$ have kernels and for $\mathbb{H} \trianglelefteq \mathbb{G}$, the factor group $\mathbb{G}/\mathbb{H}$ is defined (subtle...).

IV.5 Classification of simple groups over alg. closed fields

We agree that undefined properties of $\mathbb{G}$ (e.g. "abelian" or "connected") refer to $\mathbb{G}(\overline{K})$.

Def. IV.5.1 An alg. K-group $\mathbb{G}$ is called simple if it is connected, non-commutative and every proper normal subgroup of $\mathbb{G}$ is finite. We say $\mathbb{G}$ is absolutely simple if moreover $\mathbb{G}_{\overline{K}}$ is simple.

Def IV.5.2 A simple K-group $\mathbb{G}$ is called simply connected if every surjective morphism $\overline{\mathbb{G}} \to \mathbb{G}$ w/ finite kernel and $\overline{\mathbb{G}}$ connected has trivial kernel.

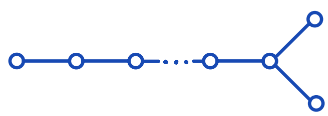
Thm IV.5.3 Suppose K is alg. closed. Then every simply connected simple alg. K-group $\mathbb{G}$ is isomorphic to precisely one of SL_n $(n \geq 1)$, Spin_n $(n \geq 4)$, Sp_n $(n \geq 2)$ or five exceptional groups.

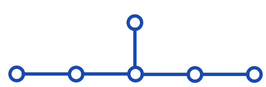
"Proof": Pick a max. torus $(\mathbb{G}_m)^n \cong \mathbb{T} \leq G$.
Then $(G, \mathbb{H})$ defines a pair $(\mathfrak{g}, \mathfrak{h})$ of a simple Lie algebra w/ a Cartan subalgebra which gives rise to an irreducible root system $\Phi(\mathfrak{g}, \mathfrak{h}) \subseteq \mathfrak{h}^*$.
These are classified by Dynkin diagrams $\Delta = \Delta(\mathfrak{g}, \mathfrak{h})$

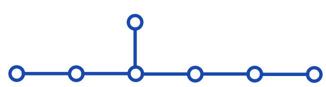
A_n $(n \geq 1)$:  $\mathfrak{sl}_{n+1}$

B_n $(n \geq 2)$:  $\mathfrak{so}_{2n+1}$

C_n $(n \geq 3)$:  $\mathfrak{sp}_n$

D_n $(n \geq 4)$:  $\mathfrak{so}_{2n}$

E_6:  $\mathfrak{e}_6$

E_7:  $\mathfrak{e}_7$

E_8:  $\mathfrak{e}_8$

F_4:  $\mathfrak{f}_4$

G_2:  $\mathfrak{g}_2$

$\left.\begin{matrix} \mathfrak{e}_6, \mathfrak{e}_7, \mathfrak{e}_8, \mathfrak{f}_4, \mathfrak{g}_2 \end{matrix}\right\}$ exceptional types

and form a complete invariant.
[https://www.math.uni-duesseldorf.de/~kammeyer/lie-algebren.pdf]
$\square$

The A_n–G_2-classification stays intact for general K w/ char $K = 0$ under the assumption that G is K-split, meaning there is a maximal torus $(GL_1)^n \cong T \leq G$ such that $T_{\bar{K}} \leq G_{\bar{K}}$ is still maximal:

<u>Thm. IV.5.4</u> The K-groups SL_{n+1} $(n \geq 1)$, $Spin(n, n+1)$ $(n \geq 2)$, Sp_n $(n \geq 3)$, $Spin(n,n)$ $(n \geq 4)$ and the K-split groups of type $E_6, E_7, E_8, F_4,$ and G_2 form a complete set of representatives for the iso. classes of K-split simply connected abs. simple K-groups.

Upshot:

- Classification over $\bar{K}$ by Cartan-Killing type A_n–G_2.
- Each type has a unique K-split K-form G_0.

Goal:

- Find all the other K-forms, or equivalently (by IV.2.1):
- For each K-split form G_0, determine $H^1(K, \mathrm{Aut}\, G_0)$.

<u>IV.6 Classification of simple groups over p-adic fields</u>

Let G_0 be a K-split simply connected absolutely simple K-group w/ Dynk. d. Δ. Then $\mathrm{Aut}\, G_0$ is a K-group and

$$1 \to \underset{\substack{\uparrow \\ \text{inner automorphisms}}}{\mathrm{Ad}\, G_0} \to \mathrm{Aut}\, G_0 \to \underset{\substack{\uparrow \\ \text{constant group scheme}}}{\mathrm{Sym}\, \Delta} \to 1$$

is a split exact sequence of $\mathrm{Gal}(K)$-groups.

From IV.1.2, we obtain

$$\begin{tikzcd} 1 \arrow[r] & H^1(K, \mathrm{Ad}\, G_0) \arrow[r] & H^1(K, \mathrm{Aut}\, G_0) \arrow[r, "\rho"] & H^1(K, \mathrm{Sym}\, \Delta) \arrow[l, bend left, dashed, "s"] \arrow[r] & 1. \end{tikzcd}$$

We have $\mathrm{Sym}\, \Delta = 1$, hence $H^1(K, \mathrm{Sym}\, \Delta) \cong 1$ if G_0 has type $A_1, B_n, C_n, E_7, E_8, F_4$, or G_2. By III.5.7, we obtain $H^1(K, \mathrm{Sym}\, \Delta) \cong K^*/(K^*)^2$ if G_0 has type A_n $(n \geq 2)$, D_n $(n \geq 5)$, or E_6 (in type D_4, we have $\mathrm{Sym}\, \Delta \cong S_3 \cong \mathbb{Z}/_3 \rtimes \mathbb{Z}/_2$ $\rightsquigarrow$ "triality").

For $\alpha = [a] \in H^1(K, \mathrm{Sym}\, \Delta)$, let $[G_1]$ correspond to $s(\alpha)$ by IV.3.1. The K-group G_1 is called the *quasi-split form w/ discriminant* α. By *twisting*, we have

$$\begin{tikzcd} 1 \arrow[r] & H^1(K, \mathrm{Ad}\, G_0) \arrow[r] & H^1(K, \mathrm{Aut}\, G_0) \arrow[r, "\rho"] & H^1(K, \mathrm{Sym}\, \Delta) \arrow[r] & 1. \\ 1 \arrow[r] & H^1(K, \mathrm{Ad}\, G_1) \arrow[r] & H^1(K, \mathrm{Aut}\, G_1) \arrow[r, "s\circ a\, \rho"] \arrow[u, "\cong", "{[G_1] \mapsfrom 1}"'] & H^1(K, {}_a(\mathrm{Sym}\, \Delta)) \arrow[r] \arrow[u, "\cong", "{\alpha \mapsfrom 1}"'] & 1. \end{tikzcd}$$

$s\circ a(\mathrm{Ad}\, G_0) \underset{\mathrm{Gal}(K)}{\cong} \mathrm{Ad}\, G_1$ $\quad$ $s\circ a(\mathrm{Aut}\, G_0) \underset{\mathrm{Gal}(K)}{\cong} \mathrm{Aut}\, G_1$ $\quad$ $= \mathrm{Sym}\, \Delta$ unless G_1 has type D_4.

so $\rho^{-1}(\alpha) \cong H^1(K, \mathrm{Ad}\, G_1)/{}_a(\mathrm{Sym}\, \Delta)(K)$ by IV.1.3.

So it remains to determine $H^1(K, \mathrm{Ad}\, G_1)/\mathrm{Sym}\, \Delta$ for all quasi-split forms G_1. By IV.1.4, the seq.

$$1 \longrightarrow Z(G_1) \longrightarrow G_1 \longrightarrow \mathrm{Ad}\, G_1 \longrightarrow 1,$$

gives the exact sequence

$$H^1(K, G_1) \longrightarrow H^1(K, \mathrm{Ad}\, G_1) \xrightarrow{\delta^1} H^2(K, Z(G_1))$$

and δ^1 is $\mathrm{Sym}\, \Delta$-equivariant (note that $\mathrm{Sym}\, \Delta(K) \curvearrowright Z(G_1)$).

<u>Thm. IV.6.1</u> (M. Kneser) Let $K/\mathbb{Q}_p$ be finite and let G be a simply connected simple K-group. Then $H^1(K, G) = \{1\}$.

<u>Proof.</u> A case by case investigation. $\square$

<u>Cor. IV.6.2</u> For $K/\mathbb{Q}_p$ fin., the map δ^1 is a bijection.

<u>Proof.</u> Injectivity: $\ker \delta^1 = \{1\}$ by the above. By twisting, $(\delta^1)^{-1}(\delta^1([a])) = \ker_a \delta^1 = \{1\}$ for all $[a] \in H^1(K, \mathrm{Ad}\, G_1)$ by the above, too. Surjectivity is a "by-product" of the proof of IV.6.1. $\square$

<u>Remark IV.6.3</u> Surjectivity also holds for number fields

Finally, for $K/\mathbb{Q}_p$ finite, local Tate duality (III.6.4) gives $H^2(K, Z(G_1)) \cong H^0(K, Z(G_1)')^*$ which can easily be computed. For example if G_1 has type A_1, B_n, C_n, or E_7, then $Z(G_1) = \mu_2$, so $H^0(K, Z(G_1)')^* \cong H^0(K, \mathbb{Z}/2)^* \cong \mathbb{Z}/2$.

The action $\mathrm{Sym}\,\Delta \circlearrowright H^2(K, Z(G_1))$ must be trivial if $H^2(K, Z(G_1))$ has order one or two. In types A_n $(n \geq 2)$, D_{2n-1} $(n \geq 3)$, and E_6, $\mathrm{Sym}\,\Delta \cong \mathbb{Z}/2$ acts by inversion. In type D_{2n} $(n \geq 3)$, $\mathrm{Sym}\,\Delta \cong \mathbb{Z}/2$ acts as one of the three order two subgroups of $\mathrm{Aut}(Z(G_1)) \cong \mathrm{Aut}(\mathbb{Z}/2 \times \mathbb{Z}/2) \cong S_3$ and for $n=2$, $\mathrm{Sym}\,\Delta \cong S_3$ acts as the full automorphism group.

The results can be summarized in the following table.

Type of G_1	${}^1A_n$	${}^2A_{2n-1}$	${}^2A_{2n}$	B_n	C_n	${}^1D_{2n-1}$	${}^2D_{2n-1}$
$H^2(K, Z(G_1))$	$\mathbb{Z}/n+1$	$\mathbb{Z}/2$	0	$\mathbb{Z}/2$	$\mathbb{Z}/2$	$\mathbb{Z}/4$	$\mathbb{Z}/2$
$\lvert p^{-1}(\alpha)\rvert$	$\lfloor \frac{n+3}{2} \rfloor$	2	1	2	2	3	2

Type of G_1	${}^1D_{2n}$	${}^2D_{2n}$	${}^3D_4$	${}^6D_4$	${}^1E_6$	${}^2E_6$	E_7	E_8	F_4	G_2
$H^2(K, Z(G_1))$	$(\mathbb{Z}/2)^2$	$\mathbb{Z}/2$	0	0	$\mathbb{Z}/3$	0	$\mathbb{Z}/2$	0	0	0
$\lvert p^{-1}(\alpha)\rvert$	3 (2 if $n=2$)	2	1	1	2	1	2	1	1	1

IV. 7 Classification of simple groups over number fields

Let G_0 be a k-split simply conn. abs. simple k-group. From the previous section, we see that determining $H^1(k, \operatorname{Aut} G_0)$ splits into determining

(i) $H^1(k, \operatorname{Sym} \Delta)$ and

(ii) $H^1(k, \operatorname{Ad} G_1)/\operatorname{Sym}\Delta$ w/ $[G_1] = s(\alpha)$ for $\alpha \in H^1(k, \operatorname{Sym}\Delta)$.

(i): Except when G_0 has type D_4, $\operatorname{Sym}\Delta \cong 1$ or $\mathbb{Z}/2$, so $H^1(k, \operatorname{Sym}\Delta) \cong 1$ or $k^*/(k^*)^2$ by III.5.7. As in the example of the Poitou-Tate sequence, such global square residues can be prescribed locally by

$$0 \to k^*/(k^*)^2 \to \mathbb{I}_k/\mathbb{I}_k^2 \to \left(k^*/(k^*)^2\right)^{*} \to 0 .$$

* (Pontr. dual)

(ii) We have a diagram

$$\begin{tikzcd} H^1(k, \mathrm{Ad}\, G_1) \arrow[r, two heads, "\mathrm{IV}.6.3"] \arrow[d] & H^2(k, Z(G_1)) \arrow[d] \\ \prod_{v \in V_f(k)} H^1(k_v, \mathrm{Ad}\, G_1) \arrow[r, "\cong", "\mathrm{IV}.6.2"'] & \prod_{v \in V_f(k)} H^2(k_v, Z(G_1)) \end{tikzcd}.$$

Since $Z(G_1)$ is a finite commutative $\mathrm{Gal}(k)$-module, Poitou-Tate duality shows in fact that

$$\begin{tikzcd} H^1(k, \mathrm{Ad}\, G_1) \arrow[r, two heads, "\mathrm{IV}.6.3"] \arrow[d] & H^2(k, Z(G_1)) \arrow[d] \\ \bigoplus_{v \in V_f(k)} H^1(k_v, \mathrm{Ad}\, G_1) \arrow[r, "\cong", "\mathrm{IV}.6.2"'] & \bigoplus_{v \in V_f(k)} H^2(k_v, Z(G_1)) \end{tikzcd}$$

<u>Thm IV.7.1</u> (Kneser, Harder, Chernousov) Let G be a simply connected abs. simple k-group. Then

$$H^1(k, G) \xrightarrow{\cong} \prod_{v \in V_\infty(k)} H^1(k_v, G). \qquad \square$$

So if k is totally imaginary, the exact sequence and twisting gives

$$\begin{tikzcd} H^1(k, \mathrm{Ad}\, G_1)/\mathrm{Sym}\,\Delta \arrow[r, "\cong"] \arrow[d] & H^2(k, Z(G_1))/\mathrm{Sym}\,\Delta \arrow[d, "\beta^2_{Z(G_1)}"] \\ \bigoplus_{v \in V_f(k)} H^1(k_v, \mathrm{Ad}\, G_1)/\mathrm{Sym}\,\Delta \arrow[r, "\cong"] & \bigoplus_{v \in V_f(k)} H^2(k_v, Z(G_1))/\mathrm{Sym}\,\Delta \end{tikzcd}$$

Moreover, one checks case by case that $\ker \beta^2_{Z(G_1)} = 0$. So the Poitou-Tate sequence

$$0 \to H^2(k, Z(G_1)) \xrightarrow{\beta^2} \bigoplus_v H^2(k_v, Z(G_1)) \xrightarrow{\gamma^2} H^0(k, Z(G_1)')^* \to 0$$

completes the classification.

Now allow k to have real places and consider

$$\begin{tikzcd}
H^1(k, Z(G_1)) \arrow[r] \arrow[d, two heads] & H^1(k, G_1) \arrow[r] \arrow[d, "\cong"'] & H^1(k, \mathrm{Ad}\, G_1) \arrow[r, two heads, "\delta^1"] \arrow[d, "\eta"'] & H^2(k, Z(G_1)) \arrow[d, "\beta^2_{Z(G_1)}"] \\
\bigoplus_{v \text{ real}} H^1(k_v, Z(G_1)) \arrow[r] & \bigoplus_{v \text{ real}} H^1(k_v, G_1) \arrow[r] & \bigoplus_v H^1(k_v, \mathrm{Ad}\, G_1) \arrow[r, "\oplus \delta^1_v"] & \bigoplus_v H^2(k_v, Z(G_1)) \arrow[d, "\gamma^2"] \\
& & & H^0(k, Z(G_1)')^*.
\end{tikzcd}$$

<u>Thm. IV.7.2</u> The map η is injective and $\operatorname{im} \eta = \ker(\gamma^2 \circ \bigoplus_v \delta^1_v)$.

<u>Proof.</u> By a "4-lemma" diagram chase, $\ker \eta = 1$. By twisting, η is injective. The inclusion $\operatorname{im} \eta \subseteq \ker(\gamma^2 \circ \bigoplus_v \delta^1_v)$ is clear from the exactness of the vertical P.T. seq.
Let $(\alpha_v) \in \ker(\gamma^2 \circ \bigoplus_v \delta^1_v)$. Then there exists $\beta = [b] \in H^1(k, \mathrm{Ad}\, G_1)$ such that $\beta^2(\delta^1(\beta)) = \bigoplus_v \delta^1_v((\alpha_v))$.

Twisting w/ b gives the S.E.S.

$$\begin{tikzcd}
1 \arrow[r] & Z(G_2) \arrow[r] \arrow[d, equal] & {}_b(G_2) \arrow[r] \arrow[d, "\cong"] & {}_b(\mathrm{Ad}\, G_2) \arrow[r] \arrow[d, "\cong"] & 1 \\
1 \arrow[r] & Z(G_2) \arrow[r] & \mathcal{G}_2 \arrow[r] & \mathrm{Ad}\, \mathcal{G}_2 \arrow[r] & 1
\end{tikzcd}$$

where $\mathcal{G}_2$ is the inner k-form of G_2 defined by β. In the corresponding diagram

$$\begin{tikzcd}
H^2(k, \mathcal{G}_2) \arrow[r, "p'"] \arrow[d, "\cong"'] & H^2(k, \mathrm{Ad}\, \mathcal{G}_2) \arrow[r, two heads, "\delta^2"] \arrow[d, "\eta"'] & H^2(k, Z(\mathcal{G}_2)) \arrow[d, "\beta^2"] \\
\bigoplus\limits_{v \text{ real}} H^2(k_v, \mathcal{G}_2) \arrow[r, "\oplus p'"] & \bigoplus\limits_{v} H^2(k_v, \mathrm{Ad}\, \mathcal{G}_2) \arrow[r, "\oplus \delta_v^2"] & \bigoplus\limits_{v} H^2(k_v, Z(\mathcal{G}_2))
\end{tikzcd},$$

the family $(\alpha_v) \in \bigoplus_v H^2(k_v, \mathrm{Ad}\, G_2)$ corresponds to $(\alpha_v') \in H^2(k_v, \mathrm{Ad}\, \mathcal{G}_2)$ w/ $(\alpha_v') \in \ker \bigoplus_v \delta_v^2 = \operatorname{im} \oplus p'$. Hence there exists $\alpha'' \in \operatorname{im} p'$ w/ $\eta(\alpha'') = (\alpha_v')$. Translating back, $\alpha'' \in H^2(k, \mathrm{Ad}\, \mathcal{G}_2)$ corresponds to a class $\alpha \in H^2(k, \mathrm{Ad}\, G_2)$ realizing the family (α_v) as its localizations. $\square$

Hence we may prescribe local classes $\alpha_v \in H^2(k_v, \mathrm{Ad}\, G_2)$ at will under the condition $\gamma^2\left(\bigoplus_v \delta_v((\alpha_v))\right) = 0$ and obtain a unique global class $\alpha \in H^2(k, \mathrm{Ad}\, G_2)$ realizing the local forms as completions. Inner k-forms of G_2 correspond uniquely to $\mathrm{Sym}\,\Delta$-orbits of the forms α. This completes the classification of simply connected absolutely simple k-groups.