Chapter 1: C_i fields

Def. (Artin, Lang) K field, $i \geq 0$ integer. Then K is $\boxed{C_i}$ if $\forall n, d \geq 0$ integers s.t. $n \geq d^i$, $\forall X \subseteq \mathbb{P}^n_K$ projective surface of degree d: $X(K) \neq \emptyset$.

Rmk. $i = 0$: $n \geq 1$, $\forall X \subseteq \mathbb{P}^n_K$: $X(K) \neq \emptyset$. Hence $C_0 \iff K$ is algebraically closed.

§1 Finite fields

Thm. (Chevalley – Warning) Finite fields are C_1.

Pf: Let $f \in \mathbb{F}_q[x_0, \dots, x_n]$ be a homogeneous polynomial of $\deg = d$, $d \leq n$.

Want to find $z \in \mathbb{F}_q^{n+1} \setminus \{0\}$ s.t. $f(z) \neq 0$.

$F := 1 - f^{q-1}$. Then $\forall \underline{x} \in \mathbb{F}_q^{n+1}$: $F(\underline{x}) = \begin{cases} 1 & f(\underline{x}) = 0 \\ 0 & f(\underline{x}) \neq 0 \end{cases}$

$\Rightarrow N := \# \{ \underline{x} \in \mathbb{F}_n^{q+1} \mid f(\underline{x}) = 0 \} \underset{\text{in } \mathbb{F}_q}{=} \sum_{\underline{x} \in \mathbb{F}_q^{n+1}} F(\underline{x})$

$F(\underline{x}) = \sum_{\underline{i} \in \mathbb{N}^{n+1}_{\geq 0}} a_{\underline{i}} \underline{x}^{\underline{i}}$ polynomial, $N = \sum_{\underline{x} \in \mathbb{F}_q^{n+1}} \sum_{\underline{i} \in \mathbb{N}^{n+1}_{\geq 0}} a_{\underline{i}} \underline{x}^{\underline{i}}$

$$= \sum_{\underline{i}} a_{\underline{i}} \sum_{\underline{x}} \underline{x}^{\underline{i}}$$

$$= \sum_{\underline{i}} a_{\underline{i}} \underbrace{\Big(\sum_{x \in \mathbb{F}_q} x^{i_0} \Big)}_{=0 \text{ if } i_0 < q-1} \cdots \underbrace{\Big(\sum_{x \in \mathbb{F}_q} x^{i_n} \Big)}_{=0 \text{ if } i_n < q-1}$$

$\deg F = (q-1) \cdot d < (q-1) \cdot (n+1)$

$\Rightarrow$ in each term of the formula for N, at least one of the i_j's must be $< q-1$

$\Rightarrow N = 0$ in $\mathbb{F}_q$ $\Rightarrow N \equiv 0$ (mod char $\mathbb{F}_q$). But $N \geq 1 \Rightarrow N \geq 2$.

§2
Transition theorems

Def. K field. $\varphi \in K[x_0, \dots, x_n]$ homogeneous polynomial is a **normic form** if

- $\deg \varphi =: d = n+1$
- $\forall \underline{x} \in K^{n+1}: \ \varphi(\underline{x}) = 0 \iff \underline{x} = 0$

Lemma. K non-alg closed field. Then there are normic forms over K of arbitrarily large degree.

Pf: Let L/K be a fin extn of $(L:K) = e > 1$.

Consider $\varphi_0 : L \longrightarrow K$
$x \longmapsto N_{L/K}(x)$

By writing $x \in L$ in some basis of L/K, we see that φ_0 is homogeneous of degree e in e variables. $\Rightarrow \varphi_0$ is a normic form of $\deg = e$.

Let $\varphi_1 := \varphi_0(\varphi_0 | \cdots | \varphi_0) = \varphi_0(\varphi_0(x_0), \dots, \varphi_0(x_{e-1}))$

$\varphi_2 := \varphi_1(\varphi_0 | \cdots | \varphi_0)$ etc.

Each φ_i is a normic form of $\deg = e^{i+1}$

Thm. (Lang – Nagata) K C_i-field, $X \subseteq \mathbb{P}^n_K$ closed subvariety which is an intersection of r hypersurfaces of degree d with $r \cdot d^i \leq n$.
Then $X(K) \neq \emptyset$.

Generalisation (open question): r hypersurfaces of degrees $d_1, \dots, d_r$ s.t. $d_1 + \dots + d_r \leq n$.
$\overset{?}{\Rightarrow} X(K) \neq \emptyset$.

Pf: 1) $K = \overline{K}$ $\Rightarrow$ $\dim X \geq n - r \geq 0$ $\Rightarrow$ has a rational point.

2) $K \neq \overline{K}$ Find φ normic form, $\deg \varphi = e \geq r$ (Lemma)

Let $f_1, \dots, f_r$ be the polynomials defining X, $d = \deg f_1 = \dots = \deg f_r$

$\varphi_1 := \varphi(f_1, \dots, f_r \,|\, f_1, \dots, f_r \,|\, \dots \,|\, f_1, \dots, f_r \,|\, \underbrace{0, \dots, 0}_{< r \text{ zeros}})$

$|$ means change in variables
$,$ variable stays the same

Do this with φ_1 in place of φ $\Rightarrow \varphi_2$, and repeat.

$D_m := \deg \varphi_m$, $N_m :=$ number of variables of φ_m

$D_{m+1} = D_m \cdot d \Rightarrow D_m = d^m \cdot e$

$N_{m+1} = \left\lfloor \frac{N_m}{r} \right\rfloor \cdot (n+1)$

Exercise: $\frac{N_m}{D_m} \longrightarrow 0$ as $m \longrightarrow \infty$

For $m \gg 0$: $N_m > D_m^i$

C_i-property $\Rightarrow$ $\varphi_m = 0$ has a nontrivial solution

Induction $\Rightarrow$ all the f_i's have a nontrivial common zero.

Thm. (Tsen) K'/K extension of trdeg $= \delta$, K is C_i $\Rightarrow$ K' is $C_{i+\delta}$.
In particular, the C_i-property is preserved under finite extension.

Pf: We only have to deal with 2 cases:

1) K'/K is finite $(\delta = 0)$

2) $K' = K(T)$. $(\delta = 1)$

Everything else can be built up from these two.

1) Consider $f \in K'[x_0, \dots, x_n]$ homogeneous, $\deg f = d$, $d^i \leq n$

Write $f = 0$ in a K-basis of K'. Then $f = 0$ is equivalent to a system of $[K':K]$ equations in $(n+1)[K':K]$ variables, each of degree d.

Lang–Nagata $\Rightarrow$ this system has a nontrivial solution.

2) $K' = K(T)$, $f \in K'[x_0, \dots, x_n]$ homogeneous, $\deg f = d$. $d^i \leq n$.

Wma $f \in K[T][x_0, \dots, x_n]$

$d_0 :=$ the largest degree of a coefficient of f

Look for a solution of the form

$$\left.\begin{array}{l} X_0(T) = x_{00} + x_{10} T + \dots + x_{D0} T^D \\ \vdots \\ X_n(T) = x_{0n} + x_{1n} T + \dots + x_{Dn} T^D \end{array}\right\}$$

for some $D > 0$.

Then $f = 0$ is equivalent to a system of equations over K in variables x_{ij}. There are $(D+1)(n+1)$ variables, $D \cdot d + d_0$ equations, each of which has degree d.

Since $d^i \leq n$, for $D \gg 0$: $(D+1)(n+1) > (Dd + d_0)\, d^i$

Lang–Nagata $\Rightarrow$ the system has a nontrivial solution.

§3 Discrete valuation fields

Thm. (Greenberg's approximation thm.) R complete discrete DVR, $\pi \in R$ uniformiser, $K = R/(\pi)$ fraction field. Let $f_1, \dots, f_r$ be homogeneous polynomials over R. Assume that $\forall \nu \geq 0$ the system of congruences

$$\left.\begin{array}{l} f_1(\underline{x}) \equiv 0 \mod \pi^\nu \\ \vdots \\ f_r(\underline{x}) \equiv 0 \mod \pi^\nu \end{array}\right\}$$

has a solution in $R^{n+1} \setminus \pi R^n$. Then the system $f_1 = 0, \dots, f_r = 0$ has a nonzero solution.

PO, the main difficulty is with non-smooth points.

Cor. Let K be a C_i-field. Then $K((T))$ is C_{i+1}.

Pf: Use Greenberg to reduce to Tsen.

Consider $f \in K((T))[x_0, \dots, x_n]$, $\deg f = n$, $d^{i+1} \leq n$.

Wma $f \in K[[T]][x_0, \dots, x_n]$.

For every $\nu \geq 0$ we can consider $f_\nu \in K[T][x_0, \dots, x_n]$ s.t. $f_\nu \equiv f \mod T^\nu$ and f_ν is still homog in $n+1$ variables of deg d.

Tsen $\Rightarrow$ $f_\nu = 0$ has a solution in $K[T]$, wma it is not a multiple of T.

Hence $f \equiv 0 \mod T^\nu$ has a solution not divisible by T.

Note that here the local situation (Laurent series) is more complicated than the global one.

p-adic fields

Thm. (Terjanian, 1966) $\mathbb{Q}_2$ is not C_2.

Pf: $g(X, Y, Z) := X^2YZ + Y^2ZX + Z^2XY + X^2Y^2 + Y^2Z^2 + Z^2X^2 - X^4 - Y^4 - Z^4$

$h(X_1, \dots, X_9) := g(X_1, X_2, X_3) + g(X_4, X_5, X_6) + g(X_7, X_8, X_9)$

$f(X_1, \dots, X_{18}) := h(X_1, \dots, X_9) + 4\, h(X_{10}, \dots, X_{18})$

One can check: $\forall (x, y, z) \in \mathbb{Z}_2^3$: $g(x, y, z) \equiv 0$ or $3 \mod 4$,

and $g(x, y, z) \equiv 0 \mod 4 \Rightarrow 2 \mid x, y, z$.

Take $(x_1, \dots, x_{18}) \in \mathbb{Z}_2^{18}$ s.t. $f(x_1, \dots, x_{18}) = 0$

$\Rightarrow h(x_1, \dots, x_9) \equiv 0 \mod 4 \Rightarrow g(x_1, x_2, x_3) \equiv g(x_4, x_5, x_6) \equiv g(x_7, x_8, x_9) \equiv 0 \mod 4$

$\Rightarrow 2 \mid x_1, \dots, x_9 \Rightarrow h(x_{10}, \dots, x_{18}) = -\frac{1}{4} h(x_1, \dots, x_9) \equiv 0 \mod 4$

$\Rightarrow 2 \mid x_{10}, \dots, x_{18}$. $\Rightarrow$ We can do an infinite descent $\Rightarrow x_1, \dots, x_{18} = 0$.

18 variables, degree 4 $\Rightarrow$ not C_2.

Thm. (Arkhipov, Karatsuba 1982, Alemu 1985)

A p-adic local field is not C_i for any $i \geq 0$.

Exc. This implies that number fields are not C_i for any i.

Thm. (Lang) K complete discrete valuation field with algebraically closed residue field $\Rightarrow$ K is C_1.

§4 Open questions.

Conjectures:

1) Artin: $\mathbb{Q}^{ab} = \mathbb{Q}(\zeta_n \mid n \geq 1)$ is C_1?

2) Lang: $X/\mathbb{R}$ smooth projective variety, $\dim X = n$, $X(\mathbb{R}) = \emptyset$. Is $\mathbb{R}(X)$ C_1?

3) $\mathbb{C}((X,Y))$ is C_2?

Known: works for diagonal equations: $a_0 x_0^d + \ldots + a_n x_n^d = 0$. (exercise)

Chapter 2. Galois cohomology and cohomological dimension

§1 Group cohomology

Def. G profinite group: $\varprojlim$ finite groups as a topological group.

Def. G-module M: abelian group, $G \times M \to M$ continuous action s.t. $\forall g \in G$: $m \mapsto gm$ is a group homomorphism.

Rmk. $M = \bigcup_{\substack{U \leq G \\ \text{open}}} M^U$

$K^0(G,M) := M$, $K^i(G,M) := C(G^i, M)$ for $i > 0$

$K^0(G,M) \xrightarrow{d^0} K^1(G,M) \xrightarrow{d^1} K^2(G,M) \xrightarrow{d^2} \ldots$ complex

$$(d^i f)(g_1, \ldots, g_{i+1}) = g_1 \cdot f(g_2, \ldots, g_{i+1}) + \sum_{j=1}^{i+1} (-1)^j f(g_1, \ldots, g_j g_{j+1}, g_{j+2}, \ldots, g_{i+1}) + (-1)^{i+1} f(g_1, \ldots, g_i)$$

Def. Cohomology of G with coeffs in M: $H^0(G,M) := M^G$, $H^i(G,M) := \operatorname{Ker} d^i / \operatorname{Im} d^{i-1}$

Ex. $$H^1(G,M) = \frac{\{f : G \to M \text{ cont.} \mid \forall s,t: f(st) = f(s) + s f(t)\}}{\{G \to M \mid s \mapsto sm - m \text{ for some } m \in M\}}$$

If $G \curvearrowright M$ trivially then $H^1(G,M) = \operatorname{Hom}_c(G,M)$

Rmk. $\mathcal{A}$, $\mathcal{B}$ abelian cats, $\mathcal{A}$ has enough injectives, $F: \mathcal{A} \to \mathcal{B}$ functor, F left exact. Given an injective resolution $0 \to A \to I^0 \to \dots$ where $\forall I_i$ is injective, we get a complex $0 \to FA \to FI^0 \to \dots$

The derived functors of F are given by the cohomologies of this complex.

For a profinite group G, the group cohomology of G is given by the derived functors of $F: G\text{-Mod} \to Ab$
$$M \mapsto M^G$$

Thm. A short exact sequence $0 \to M \to N \to P \to 0$ in G-Mod induces a long exact sequence $0 \to H^0(G,M) \to H^0(G,N) \to H^0(G,P) \to$
$$\to H^1(G,M) \to H^1(G,N) \to H^1(G,P) \to \dots$$

Pf: Follows from abstract nonsense.

Or use the dfn from lec. 1: we get $0 \to K^\cdot(G,M) \to K^\cdot(G,N) \to K^\cdot(G,P) \to 0$, which induces a long exact sequence $0 \to \underbrace{H^0(K^\cdot(G,M))}_{=H^0(G,M)} \to \underbrace{H^0(K^\cdot(G,N))}_{=H^0(G,N)} \to \dots$ by the snake lemma.

Prop. G profinite gp, M a G-module. Then $H^i(G,M) \cong \varinjlim_{\substack{U \trianglelefteq G \\ \text{open}}} H^i(G/U, M^U)$

Note that by profiniteness of G, the quotients G/U are all finite.

Shapiro's Lemma. $H \leq G$ closed, G profinite, M an H-module.

Consider $\boxed{I_G^H(M)} := \{ f: G \to M \text{ cont.} \mid \forall h \in H\ \forall g \in G: f(hg) = hf(g) \}$.

Endow $I_G^H(M)$ with the following G-action: for $g \in G$, $f \in I_G^H(M)$,

$g \cdot f: g' \mapsto f(g'g)$.

Then we have a natural iso $H^i(G, I_G^H(M)) \cong H^i(H,M)$ induced by
$$I_G^H(M) \longrightarrow M$$
$$f \longmapsto f(1)$$

Pf: We have, for A a G-module and B an H-module an isomorphism
$$\mathrm{Hom}_G(A, I_G^H(B)) \cong \mathrm{Hom}_H(A,B),$$
$$f \mapsto (a \mapsto f(a)(1))$$
i.e. I_H^G is the right adjoint of the forgetful functor.

Right adjoint functors preserve injective objects.

Moreover, one can check that I_G^H is exact (easy).

Now consider any injective resolution $0 \to M \to I^0 \to I^1 \to \dots$

Then by applying I_G^H, we get another injective resolution $0 \to I_G^H(M) \to \dots$

The cohomology of $I_G^H(M)$ is the cohomology of the complex

$$\begin{array}{ccccc} 0 \to & I_G^H(I^0)^G & \to & I_G^H(I^1)^G & \to \dots \\ & \wr\!\wr & & \wr\!\wr & \\ 0 \to & (I^0)^H & \to & (I^1)^H & \to \dots \end{array}$$

The cohomology of the bottom row is $H^\bullet(H, M)$.

Thm. (Inflation – Restriction) $H \trianglelefteq G$ closed, G profinite, M G-module.

Res: $H^i(G, M) \to H^i(H, M)$ induced by $H \hookrightarrow G$

Inf: $H^i(G/H, M) \to H^i(G, M)$ induced by $G \twoheadrightarrow G/H$ and $M^H \hookrightarrow M$.

We have an exact sequence

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M) \to 0$$

Pf: Exercise.

We may generalise this theorem using spectral sequences.

Thm. In the setting as above, we have a spectral sequence

$$H^p(G/H, H^q(H, M)) \Rightarrow H^{p+q}(G, M)$$

Cor. 1) The group $H^n(G, M)$ has a filtration

$$F_0 = H^n(G, M) \supseteq F_1 \supseteq F_2 \supseteq \dots \supseteq F_n = 0$$

s.t. F_p/F_{p+1} is a subquotient of $H^p(G/H, H^{n-p}(H, M))$.

2) If $H^i(H, M) = 0$ for $1 \le i \le n-1$ then we have an exact sequence

$$0 \to H^n(G/H, M^H) \xrightarrow{\text{Inf}} H^n(G, M) \to H^n(H, M) \to 0.$$

(This generalises the Inf-Res sequence.)

Prop. (Restriction – Corestriction) $H \le G$ open, G profinite. Consider the morphism

Cores: $H^n(H, M) \to H^n(G, M)$ induced by $I_G^H(M) \to M$

$$f \mapsto \sum_{g \in G/H} g \cdot f(g')$$

(Note that the sum is finite since H is open.)

Then $\text{Cores} \circ \text{Res}$ is multiplication by $[G:H]$.

Pf: On the level of G-modules:

$$M \xrightarrow{\text{Res}} I_G^H(M) \xrightarrow{\text{Cores}} M$$

$$m \longmapsto \underbrace{(g \mapsto gm)}_{f} \longmapsto \sum_{g \in G/H} g \cdot f(g^{-1}) = \sum_{g\in G/H} g \cdot g^{-1} m = [G:H]\, m$$

In particular: if $\#G < \infty$ then $\#G \cdot H^n(G,M) = 0$.

In general, for any profinite group G, $H^n(G,M)$ is torsion $\forall n \geq 1$.

Exc. Prove that if M is uniquely divisible then $H^n(G,M) = 0$ $\forall n \geq 1$.

§2 Cohomology of cyclic groups

Thm. G cyclic group, $\langle \sigma \rangle = G$. Then for any G-module M we have natural isomorphisms

$$H^{2r-1}(G,M) \cong \frac{\operatorname{Ker}(1+\sigma+\dots+\sigma^{n-1})}{\operatorname{Im}(1-\sigma)}$$

$$H^{2r}(G,M) \cong \frac{\operatorname{Ker}(1-\sigma)}{\operatorname{Im}(1+\sigma+\dots+\sigma^{n-1})} \quad \text{where } n = \#G.$$

Pf: Consider $D := 1-\sigma$, $N := 1+\sigma+\dots+\sigma^{n-1}$ and the complex

$$K'(G,M) := (0 \to M \xrightarrow{D} M \xrightarrow{N} M \xrightarrow{D} M \xrightarrow{N} \dots)$$

Observe that if $0 \to M \to N \to P \to 0$ is short exact in G-Mod then we have an exact sequence $0 \to K'(G,M) \to K'(G,N) \to K'(G,P) \to 0$, and hence a long exact sequence $0 \to H^0(K'(G,M)) \to \dots$

We prove the theorem by induction on the degree of the cohomology.

Step 1. Computing $H^1(G,M)$. Let $f: G \to M$ s.t. $f(st) = f(s) + s f(t)$ $\forall s,t \in G$.

Then $f(\sigma^2) = f(\sigma) + \sigma f(\sigma) = (1+\sigma) f(\sigma)$.

$f(\sigma^3) = f(\sigma^2) + \sigma^2 f(\sigma) = (1+\sigma) f(\sigma) + \sigma^2 f(\sigma) = (1+\sigma+\sigma^2) f(\sigma)$

$$\dots \Rightarrow \underbrace{f(\sigma^n)}_{0 = f(1)} = \underbrace{(1+\sigma+\dots+\sigma^{n-1})}_{N} f(\sigma) \Rightarrow f(\sigma) \in \operatorname{Ker} N$$

One can easily check that there is an iso

$$H^1(G,M) \xrightarrow{\sim} \operatorname{Ker} N / \operatorname{Im} D$$

$$f \longmapsto f(\sigma)$$

$$(\sigma \mapsto (1+\sigma+\dots+\sigma^{n-1})a) \longleftarrow a$$

Inductive step: From $H^{r}(G,M)$ to $H^{r+1}(G,M)$. Use shifting.

Consider the exact sequence $0 \to M \to I_G(M) \to N \to 0$

$$m \mapsto (g \mapsto gm)$$

where $\boxed{I_G} := I_G^{\{1\}}$. This induces exact sequences

$$\begin{array}{ccccccc}
\underset{\substack{= \\ 0 \\ \text{Shapiro}}}{H^{r}(G, I_G(M))} & \to & H^{r}(G,N) & \to & H^{r+1}(G,M) & \to & \underbrace{H^{r+1}(G, I_G(M))}_{=0 \ \text{Shapiro}} \\
 & & \wr\!\wr \ \text{induction} & & & & \\
H^{r}(K'(G, I_G(M))) & \to & H^{r}(K'(G,N)) & \to & H^{r+1}(K'(G,M)) & \to & H^{r+1}(K'(G, I_G(M)))
\end{array}$$

We have an iso $I_G(M) \cong M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \cong \bigoplus_{i=0}^{n-1} M e_{\sigma^i}$

σ acts by permuting the e_{σ^i}

$$N: \bigoplus_i M e_{\sigma^i} \longrightarrow \bigoplus M e_{\sigma^i}$$

$$\sum_i a_i e_{\sigma^i} \longmapsto \Big(\sum_i a_i\Big)(e_1 + e_\sigma + \dots + e_{\sigma^{n-1}})$$

$$D: \bigoplus M e_{\sigma^i} \longrightarrow \bigoplus M e_{\sigma^i}$$

$$\sum_i a_i e_{\sigma^i} \longmapsto \sum_i (a_i - a_{i-1}) e_{\sigma^i}$$

By this explicit description, $\operatorname{Ker} N = \left\{ \sum a_i e_{\sigma^i} \,\middle|\, \sum a_i = 0 \right\} = \operatorname{Im} D$

$\operatorname{Ker} D = \left\{ \sum a_i e_{\sigma^i} \,\middle|\, a_0 = \dots = a_{n-1} \right\} = \operatorname{Im} N$

$H^t(K'(G, I_G(M))) = 0 \quad \forall t \geq 1.$

$\Rightarrow H^{r+1}(G,M) \longrightarrow H^{r+1}(K'(G,M))$.

§3 Galois cohomology

Def. K field.

1) A $\boxed{\text{Galois module}}$ is a module over $\mathrm{Gal}(\overline{K}/K)$.

2) The $\boxed{\text{Galois cohomology}}$ of M over K is $\boxed{H^r(K,M)} := H^r(\mathrm{Gal}(\overline{K}/K), M)$.

3) For a Galois extn L/K, M $\mathrm{Gal}(L/K)$-module: $\boxed{H^r(L/K, M)} := H^r(\mathrm{Gal}(L/K), M)$.

Thm. 1) L/K fin Galois, $r \geq 1 \Rightarrow H^r(L/K, L) = 0$

2) (Hilbert 90) L/K fin Galois $\Rightarrow H^1(L/K, L^\times) = 0$.

Cor. 1) $H^r(K, \overline{K}) = 0$.

2) $H^1(K, \overline{K}^\times) = 0$.

PF OF THM:

1) Normal basis theorem: L has a K-basis that is permuted by $\mathrm{Gal}(L/K)$.

$\Rightarrow L \cong I_{\mathrm{Gal}(L/K)}(K)$ as $\mathrm{Gal}(L/K)$-modules.

Shapiro $\Rightarrow H^r(L/K, L) \cong H^r(\{1\}, K) = 0$.

2) Consider $f: \mathrm{Gal}(L/K) \longrightarrow L^\times$ s.t. $f(st) = f(s) + s\,f(t)$ $\quad \forall s,t \in \mathrm{Gal}(L/K)$.

By linear independence of the elements of $\mathrm{Gal}(L/K)$ over K we can find $\underset{L^\times}{\underset{\cap}{b}}$ s.t. $\underbrace{\sum_{g \in \mathrm{Gal}(L/K)} f(s)\, s(b)}_{=:c} \neq 0$.

$$\Rightarrow s(c) = \sum_{t \in \mathrm{Gal}(L/K)} s f(t)\, st(b) = \sum_t f(st)\, f(s)^{-1}\, st(b) \qquad \forall s \in \mathrm{Gal}(L/K).$$

$$= f(s)^{-1} \sum_t f(st)\, st(b)$$

$$= f(s)^{-1} \sum_{t'} f(t')\, t'(b) = f(s)^{-1} c$$

$\Rightarrow f(s) = c\, s(c)^{-1}$ $\Rightarrow$ the class of f in $H^1(L/K, L^\times)$ is trivial.

<u>Cor.</u> $n \geq 1$ prime to $\mathrm{char}(K)$, $\boxed{\mu_n} := \{x \in \overline{K} \mid x^n = 1\}$. Then

$H^0(K, \mu_n) = \{x \in K \mid x^n = 1\}$

$H^1(K, \mu_n) = K^\times / K^{\times n}$

$H^2(K, \mu_n) \cong H^2(K, \overline{K}^\times)[n]$.

PF: $1 \to \mu_n \to \overline{K}^\times \xrightarrow{x \mapsto x^n} \overline{K}^\times \to 1$ induces a long exact sequence

$$0 \to H^0(K, \mu_n) \to H^0(K, \overline{K}^\times) \to H^0(K, \overline{K}^\times) = K^\times$$

$$\to H^1(\mu_n) \to H^1(\overline{K}^\times) \to H^1(\overline{K}^\times) = 0 \text{ by Hilbert 90}$$

$$\to H^2(\mu_n) \to H^2(\overline{K}^\times) \xrightarrow{x \mapsto nx} H^2(\overline{K}^\times)$$

Def. $\boxed{Br(K)} := H^2(K, \overline{K}^\times)$ is the $\boxed{\text{Brauer group}}$ of K.

For a finite extension L/K, $\boxed{Br(L/K)} := Ker\left(Br\, K \xrightarrow{Res} Br\, L\right)$

For L/K Galois, the inf-res sequence in degree 2 gives $Br(L/K) \simeq H^2(L/K, L^\times)$

§4 Cohomological dimension

Def. K a field. The $\boxed{\text{cohomological dimension}}$ of K is
$\boxed{cd(K)} := \min\left\{ n \geq 0 \mid \forall M \text{ finite Galois module over } K, \forall r \geq n+1 : H^r(K, M) = 0 \right\}$

Thm. Assume char $K = 0$. Then (III) $\Rightarrow$ (II) $\Rightarrow$ (I) where
(I) $cd(K) \leq 1$
(II) $\forall L/K$ finite Galois extn: $Br\, L = 0$
(III) $\forall M/L/K$ tower of finite extensions: $N_{M/L} : M^\times \longrightarrow L^\times$ is surjective.

Pf: (III) $\longrightarrow$ (II). We only need to prove $Br\, L[p] = 0$ $\forall p$ prime.
In fact, we only need $Ker\left(Br\, L[p] \longrightarrow Br\, M[p]\right) = 0$ $\forall M/L$ fin Galois.
Let $G_p \leq Gal(M/L)$ be the p-Sylow subgroup with fixed field L_0.
$Gal(M/L)$ is a p-group $\Rightarrow$ solvable $\Rightarrow \exists L_1, \ldots, L_r$ extensions of M s.t.
$L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = M$, L_i/L_{i-1} is cyclic of degree p.
Consider $Br\, L[p] \longrightarrow Br\, L_0[p] \longrightarrow Br\, L_1[p] \longrightarrow \ldots \longrightarrow Br\, M[p]$; this composite is the map whose injectivity we need to show.

- $Br\, L[p] \longrightarrow Br\, L_0[p]$: $Cores \circ Res : Br\, L_0[p] \longrightarrow Br\, L_0[p]$ is multiplication by $[L_0 : L]$ which is prime to p. $\Rightarrow Cores \circ Res$ is injective $\Rightarrow$ so is Res.
- $Ker\left(Br\, L_i[p] \longrightarrow Br\, L_{i+1}[p]\right) = Br\, (L_{i+1}/L_i)[p]$

$$= H^2(L_{i+1}/L_i, L_{i+1}^\times)[p]$$
$$= \left(L_i^\times / N_{L_{i+1}/L_i}(L_{i+1}^\times) \right)[p] = 0 \qquad \forall i \geq 0$$

$\Rightarrow Br\, L[p] \longrightarrow Br\, M[p]$ is injective $\Rightarrow Br\, L = 0$.

(II) $\longrightarrow$ (I): We are going to prove $H^r(K, M) = 0$ $\forall M$. $\forall r \geq 2$
We may assume M to be a simple Galois module, in particular, we assume M to be p-torsion for some prime p.

Consider a finite Galois extension L/K containing p^{th} roots of 1 and s.t. $Gal(L/K) \curvearrowright M$ is trivial.

We can find $K \subseteq L_0 \subseteq L$ s.t. $p \nmid [L_0 : K]$ and $Gal(L/L_0)$ is a p-group.

By $\mathrm{Cores} \circ \mathrm{Res}$ as before: $H^2(K, M) \hookrightarrow H^2(L_0, M)$, thus it suffices to prove $H^2(L_0, M) = 0$ instead.

$Gal(\overline{L_0}/L_0) \curvearrowright M$ through the p-group $Gal(L/L_0)$ where M is viewed as an $\mathbb{F}_p$-vector space.

$\Rightarrow$ We have exact sequences of $Gal(\overline{L_0}/L_0)$-modules

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow M \longrightarrow M_0 \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow M_0 \longrightarrow M_1 \longrightarrow 0$$

$$\vdots$$

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow M_s \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

(self-defining up to this one)

But $H^2(L_0, \mathbb{Z}/p\mathbb{Z}) \underset{\substack{\uparrow \\ \mu_p(\overline{L_0}) \subseteq L_0}}{\simeq} H^2(L_0, \mu_p) = Br\, L_0[p] = 0$, hence $H^2(L_0, M) = 0$,
$H^2(K, M) = 0$.

For $r \geq 3$, consider $0 \longrightarrow M \longrightarrow I^{\{1\}}_{Gal(\overline{K}/K)}(M) \longrightarrow N \longrightarrow 0$

LES $\Rightarrow$ $0 = H^{r-1}(K, N) \simeq H^r(K, M)$ □

Rmk. Here N is torsion. $H^{r-1}(K, N')$ is finite if N' is finite, and since N is the inductive limit of finite submodules N', $H^{r-1}(K, N) = 0$.

Cor. char $K = 0$, K is C_1 $\Rightarrow$ $cd\, K \leq 1$.

Pf: We want to prove that for any tower of finite extensions $M/L/K$ the norm map $N_{M/L} : M^\times \to L^\times$ is surjective.

$e := [M : L]$

Let $\mathbb{P}^e_K$ be the hypersurface given by $N_{M/K}(\underline{x}) = a t^e$, $a \in K^\times$

This is a degree e hypersurface, and since K is C_1, it has a rational point. $\Rightarrow$ $a \in \mathrm{Im}\, N_{M/K}$.

Since L is also C_1, we obtain surjectivity of $N_{M/L}$ in the same way. □

Prop. 1) $\operatorname{trdeg}(L/K) = \delta$, $\operatorname{cd}(K) = i$ $\Rightarrow$ $\operatorname{cd}(L) \leq i + \delta$.

2) K complete DVF w/ residue field k. $\Rightarrow$ $\operatorname{cd}(K) \leq \operatorname{cd}(k) + 1$.

Pf: 1) We reduce to the following two cases:

(a) L/K is finite, (b) $L = K(x)$.

(a) $\forall r \geq i+1$ $\forall M$ fin Gal module:

$$H^r(L, M) \simeq H^r\left(K, I^{\mathrm{Gal}(\bar{K}/L)}_{\mathrm{Gal}(\bar{K}/K)}(M)\right) = 0 \quad ✓$$

(b) By the spectral sequence (p. 7), $H^r(L, M)$ has a filtration

$$H^r(L, M) = F_0 \supseteq F_1 \supseteq \dots \supseteq F_r = 0$$

s.t. F_p / F_{p+1} is a subquotient of $\underbrace{H^p\Big(\underbrace{\bar{K}(x)/K(x)}_{\bar{K}/K},\ H^{r-p}(\bar{K}(X), M)\Big)}_{=0 \text{ if } p \geq i+1 \text{ or } r-p \geq 2}$

$\Rightarrow$ for $r \geq i+2$, this is trivial, thus so is the filtration, and $H^r(L, M) = 0$, so $\operatorname{cd}(L) = \operatorname{cd}(K(x)) \leq i+1$. ✓

2) $H^r(K, M)$ has a filtration $F_0 \supseteq \dots \supseteq F_r = 0$ s.t. F_p / F_{p+1} is a subquotient of $\underbrace{H^p\left(K^{ur}/K,\ H^{r-p}(K^{ur}, M)\right)}_{=0 \text{ if } p \geq i+1 \text{ or } r-p \geq 2}$ K^{ur} is C_1 by Lang $\Rightarrow$ $\operatorname{cd} = 1$

Ex. • $\mathbb{F}_q$ is C_1 with $\operatorname{cd} = 1$

• $\mathbb{C}(X)$ is C_n with $\operatorname{cd} \leq n$ where X is an n-dim vty $/\mathbb{C}$

• $\mathbb{C}((t))$ is C_1 with $\operatorname{cd} = 1$

Question. $\operatorname{cd} K \leq i \overset{?}{\Longleftrightarrow} K$ C_i

No: $\mathbb{Q}_p$ is not C_2 but $\operatorname{cd}(\mathbb{Q}_2) = 2$.

Question. (Serre) K $C_i \overset{?}{\Rightarrow} \operatorname{cd} K \leq i$

Still open for $i = 1, 2$.

Def. K a field, p rational prime. The $\boxed{\text{p-cohomological dimension}}$ of K is

$$\boxed{cd_p(K)} := \min\left\{ n \geq 0 \;\middle|\; \forall r \geq n+1 \;\; \forall M \text{ Galois module killed by a power of } p : \; H^r(K, M) = 0 \right\}$$

$$\Rightarrow \; cd(K) = \sup_p cd_p(K)$$

Thm. (Krashen, 1914) Fix $i \geq 0$ and a prime p. $\Rightarrow \exists \, c_{p,i}$ explicit constant s.t. $\forall K$ C_i-field: $cd_p(K) \leq c_{p,i} \cdot i$

Idea. (Kato–Kuzumaki) Replace rational points by the following properties:

1) Ask for the existence of a 0-cycle of degree 1:

find finite extensions $L_0, \ldots, L_r / K$ s.t. $X(L_i) \neq \emptyset$ $\forall i$ and $\left([L_0 : K], \ldots, [L_r : K]\right) = 1$.

2) $$\left\langle N_{L/K}(L^\times) \;\middle|\; L/K \text{ finite s.t. } X(L) \neq \emptyset \right\rangle = K^\times$$

$$\rotatebox{90}{$\subseteq$}$$

$$N_{L_i/K}(L_i^\times) \supseteq (K^\times)^{[L_i : K]}$$

3) "Higher" 0-cycles of deg 1 by using K-theory.

Questions (Kato–Kuzumaki)

- K is $\boxed{C_i^0}$ if $\forall X \subseteq \mathbb{P}^n_K$ of degree d with $d^i \leq n$, X has a cycle of deg 1.

  $cd\, K \leq i \overset{?}{\iff} K$ is C_i^0

- K is $\boxed{C_i^1}$ if $\forall X \subseteq \mathbb{P}^n_K$ of degree d with $d^i \leq n$, $\left\langle N_{L/K}(L^\times) \;\middle|\; X(L) \neq \emptyset \right\rangle = K^\times$

  $cd\, K \leq i+1 \overset{?}{\iff} K$ is C_i^1

Answer to both: no.

Thm. (Wittenberg, 1915) p-adic fields and totally imaginary number fields are C_1^1.

It is open whether these fields are C_2^0.

Chapter 3: The Brauer group

Recall: $Br(K) = H^2(K, \bar{K}^\times)$

§1 Central simple algebras

Def. K a field. A $\boxed{\text{central simple algebra}}$ over K is a finite dimensional K-algebra A s.t. any two-sided ideal in A is either 0 or A itself, and the centre of A is K.

Ex. 1) $M_n(K)$

2) $\boxed{\text{Quaternion algebras}}$: for $a, b \in K^\times$ consider the 4-dimensional algebra $\boxed{(a,b)}$ with basis $1, i, j, ij$ s.t. $i^2 = a$, $j^2 = b$, $ji = -ij$

3) $\boxed{\text{Cyclic algebras}}$: Let L/K be a degree n cyclic extension, $\sigma \in Gal(L/K)$ a generator, $b \in K^\times$.

$$\boxed{(\sigma, b)} := \bigoplus_{i=0}^{n-1} L y^i \Big/ \left\langle y^n = b,\ \sigma(\alpha) y = y\alpha \;\middle|\; \alpha \in L \right\rangle \quad \text{is a CSA.}$$

4) If D is a central division K-algebra then $M_n(D)$ is a CSA.

Thm. (Wedderburn) K field, A CSA over K. $\Rightarrow \exists n \geq 0\ \exists D$ CDA: $A \cong M_n(D)$
Moreover, D is uniquely defined up to isomorphism.

Lemma. A fin dim K-algebra, $I \subseteq A$ nonzero left ideal.

1) Schur's Lemma: if I is simple then $End_A(I)$ is a division algebra.

2) Rieffel's Lemma: if A is simple and $E := End_A(I)$ then we have an isomorphism of K-algebras
$$\lambda_A : A \longrightarrow End_E(I)$$
$$a \longmapsto (x \mapsto ax)$$

Pf: 1) Let $f \in End_A(I) \setminus \{0\}$. $\Rightarrow$ $\ker f$ is a left A-submodule of I $\Rightarrow \ker f = 0$.
$\operatorname{Im} f$ is also a left A-submodule of I and $\{0\} \neq \operatorname{Im} f$ since $0 \neq f$ $\Rightarrow \operatorname{Im} f = I$
$\Rightarrow f$ is an iso.

2) $\ker \lambda_A$ is a two-sided ideal in $End_E(I)$. $\Rightarrow \ker \lambda_A = 0$, λ_A is injective.
For surjectivity, we first prove that $\lambda_A(I)$ is a left ideal in $End_E(I)$.
$\forall \varphi \in End_E(I)\ \forall \alpha \in I$: $\quad \varphi \cdot \lambda_A(\alpha) : x \in I \longmapsto \varphi(\alpha x)$

For $x \in I$, $y \mapsto yx$ is in $E = End_A(I)$. $\Rightarrow \forall x \in I: \varphi(\alpha x) = \varphi(\alpha) \cdot x$
$\Rightarrow \varphi \lambda_A(\alpha) \in \lambda_A(I) \Rightarrow$ left ideal.

Observe that IA is a two-sided ideal in A, hence $IA = A$,

and $1 = \sum_j i_j a_j$ with $i_j \in I$, $a_j \in A$.

For $\varphi \in \mathrm{End}_E(I)$:

$$\varphi = \varphi \circ \lambda_A\left(\sum_j i_j a_j\right) = \sum_j \overbrace{\varphi\, \lambda_A(i_j)}^{\in \lambda_A(I)}\, \lambda_A(a_j) \in \lambda_A(A)$$

because $\lambda_A(I)$ is a left ideal in $\mathrm{End}_E(I)$. □

Pf of Thm: 29.04.2019

A fin dim $\Rightarrow$ has a minimal nonzero left ideal I.

$\Rightarrow$ I is simple

Schur $\Rightarrow E = \mathrm{End}_A(I)$ is a division algebra.

Rieffel $\Rightarrow A \simeq \mathrm{End}_E(I)$

By choosing an E-basis of I, we get $A \simeq M_n(E^{opp})$ where $n = \dim_E I$ and E^{opp} is the opposite algebra of E (this actually matters since we are working over a division algebra).

Uniqueness: Assume $A \simeq M_n(D) \simeq M_m(D')$ with D, D' div algebras

The minimal left ideals in $A \simeq M_n(D)$ are $\left\{ \begin{pmatrix} 0 & \begin{smallmatrix} * \\ \vdots \\ * \end{smallmatrix} & 0 \end{pmatrix} \in M_n(D) \right\}$

$\Rightarrow D^n \simeq (D')^m$ as A-modules

$\Rightarrow D \simeq \mathrm{End}_A(D^n) \simeq \mathrm{End}_A(D'^m) \simeq D'$. Looking at dimensions, we thus get $n = m$. □

Goal: Br classifies central simple algebras.

Lemma. A algebra over a field K. Consider an alg extn L/K. Then A is a CSA over K $\Leftrightarrow$ $A \otimes_K L$ is a CSA over L.

Pf: $\Leftarrow$: If $Z(A) \supsetneq K$ then $Z(A \otimes_K L) \supseteq Z(A) \otimes_K L \supsetneq L$.

If I is a nonzero 2-sided ideal in A, $I \neq A$ then $I \otimes_K L$ is a 2-sided ideal in $A \otimes_K L$ and $I \otimes_K L \neq A \otimes_K L$.

$\Rightarrow$: Wma L/K is finite and (by Wedderburn's Thm) that A is a div alg.

if $L/M/K$ then $Z(A \otimes L) \subseteq Z(A \otimes M) \otimes L \Rightarrow Z(A \otimes L) \subseteq L$

Choose a K-basis $\omega_1, \dots, \omega_n$ of L. We get an A-basis of $A \otimes_K L$ $1 \otimes \omega_1, \dots, 1 \otimes \omega_n$.

Centrality: $x := \sum_{i=1}^n \alpha_i (1 \otimes \omega_i) \in Z(A \otimes_K L)$

$\forall a \in A$: $a x a^{-1} = \sum_{i=1}^n a \alpha_i a^{-1} (1 \otimes \omega_i) \Rightarrow \forall i: \alpha_i \in Z(A) = K$, and $x \in L$.

Simplicity: Let $I \subseteq A \otimes_K L$ be a 2-sided nonzero ideal.

Let $z_1, \dots, z_r$ be an A-basis of I.

By adjoining some of the $(1 \otimes w_i)$'s, say $1 \otimes w_{r+1}, \dots, 1 \otimes w_n$, we get an A-basis of $A \otimes_K L$.

For $i \leq r$ write $1 \otimes w_i = \sum_{j=r+1}^{n} \alpha_{ij} (1 \otimes w_j) + y_i$ where $y_i \in I$.

Since $1 \otimes w_1, \dots, 1 \otimes w_n$ form an A-basis of $A \otimes_K L$, the y_i's have to be A-linearly independent. $\Rightarrow$ $y_1, \dots, y_r$ form an A-basis of I.

Since I is a 2-sided ideal, $a \in A^\times \Rightarrow a y_i a^{-1} \in I$, and we can write

$$a y_i a^{-1} = \sum_{l=1}^{r} b_{il} y_l.$$

$$\Rightarrow 1 \otimes w_i = \sum_{j=r+1}^{n} \alpha_{ij} (1 \otimes w_j) + a^{-1} \left(\sum_{l=1}^{r} b_{il} y_l \right) a$$

$$= \sum_{j=r+1}^{n} a \alpha_{ij} a^{-1} (1 \otimes w_j) + \sum_{l=1}^{r} b_{il} y_l$$

$$= \sum_{j=r+1}^{n} a \alpha_{ij} a^{-1} (1 \otimes w_j) + \sum_{l=1}^{r} b_{il} \left(1 \otimes w_l - \sum_{j=r+1}^{n} \alpha_{lj} (1 \otimes w_j) \right) \qquad (*)$$

We identify coefficients:

- $i \leq r$: $b_{ii} = 1$ (coeff of $1 \otimes w_i$ in $(*)$)
- $i \neq l \leq r$: $b_{il} = 0$ (coeff of $1 \otimes w_l$ in $(*)$)
- $j \geq r+1$: $a \alpha_{ij} a^{-1} = \alpha_{ij}$ (coeff of $1 \otimes w_j$ in $(*)$)

$\Rightarrow a y_i a^{-1} = y_i$, $y_i \in Z(A \otimes_K L) = L$

$\Rightarrow I \supseteq L \Rightarrow I \supseteq A \otimes_K L$.

Thm. Let A be an algebra over a field K. Then A is CS over K $\Leftrightarrow$ $\Leftrightarrow$ $\exists L/K$ finite extn s.t. $A \otimes_K L \simeq M_n(L)$ for some $n \geq 1$.

Pf.: $\Leftarrow$: This is the Lemma.

$\Rightarrow$: By the Lemma: $A \otimes_K \overline{K}$ is CS over $\overline{K}$.

Wedderburn's Thm: $A \otimes_K \overline{K} \simeq M_n(D)$ for some $n \geq 1$ and D CDA over $\overline{K}$.

Take $x \in D$, and observe that $\bar{K}(x)/\bar{K}$ is a finite extn $\Rightarrow \bar{K}(x) = \bar{K}$, $x \in \bar{K}$.

$\Rightarrow D = \bar{K}$, and $A \otimes_K \bar{K} \simeq M_n(\bar{K})$.

Since A is fin dim, this iso descends to an iso $A \otimes_K L \simeq M_n(L)$ for some L/K finite. □

§3 The group $B(K)$

Lemma. L/K fin extn of fields

1) If A, B are CSAs over K s.t. $A \otimes_K L$, $B \otimes_K L$ are matrix algebras (A and B are $\boxed{\text{split}}$ by L) then $A \otimes_K B$ is also a CSA split by L.

2) If A is CSA over K then $i : A \otimes_K A^{op} \longrightarrow \mathrm{End}_K(A)$ is an iso.

$$a \otimes a' \longmapsto (x \mapsto a x a')$$

Pf: 1) $(A \otimes B) \otimes L \simeq (A \otimes L) \otimes (B \otimes L)$

$$\simeq M_n(L) \otimes M_m(L) \quad \text{for some } n, m$$

$$\simeq M_{nm}(L)$$

2) Since $i \neq 0$ and $A \otimes A^{op}$ is simple, i is necessarily injective.

$\dim_K (A \otimes A^{op}) = \dim_K (\mathrm{End}_K(A)) \Rightarrow i$ is an iso. □

Rmk. We have <u>not</u> used finiteness of L/K, the Lemma holds for arbitrary algebraic extensions.

Def. 1) We say that the CSAs A, B are $\boxed{\text{Brauer equivalent}}$ if $\exists m, n$:

$A \otimes M_n(K) \simeq B \otimes M_m(K)$.

2) Brauer equivalence is an equivalence relation on

$\boxed{C(L/K)} := \{\text{CSAs over } K \text{ split by } L\}$.

Let $\boxed{B(L/K)} := C(L/K) / \text{Brauer equivalence}$, $\boxed{B(K)} := \bigcup_{L/K \text{ fin}} B(L/K)$.

The Lemma shows that $B(K)$ is an abelian group under $\otimes$; same for $B(L/K)$.

We wish to identify $B(K)$ with the Brauer group.

§4 Galois descent

a) GD for vector spaces: Speiser's lemma

Lemma. (Speiser) L/K finite Galois extn, V L-vs endowed with a $\boxed{\text{semi-linear action}}$ of $G := \mathrm{Gal}(L/K)$, i.e. $\forall \sigma \in G\ \forall \lambda \in L\ \forall v \in V:\ \sigma(\lambda v) = \sigma(\lambda)\sigma(v)$.

Then the natural map $\mathrm{ev}: V^G \otimes_K L \longrightarrow V$ is an iso.

Pf: $G = \{\sigma_1, \dots, \sigma_n\}$, $e_1, \dots, e_n$ K-basis of L, $M := \big(\sigma_i(e_j)\big)_{i,j}$

Lin. independence of the Galois group (Dedekind) $\Rightarrow$ M is invertible.

(This lemma generalises H90, the proof of which uses Dedekind's lemma in a crucial way, so using it here is hardly surprising.)

Injectivity: $x := \sum_{i=1}^n v_i \otimes e_i \in \mathrm{Ker}\ \mathrm{ev} \Rightarrow \sum_{i=1}^n e_i v_i = 0,\quad v_i \in V^G$

$$\forall j:\quad \sigma_j\Big(\sum_{i=1}^n e_i v_i\Big) = 0 = \sum_{i=1}^n \sigma_j(e_i)\, v_i$$

$$M \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = 0 \Rightarrow \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = 0 \text{ by invertibility of } M.$$

Surjectivity: Take $v \in V$.

$$\underset{\text{transpose}}{{}^tM} \begin{pmatrix} \sigma_1(v) \\ \vdots \\ \sigma_n(v) \end{pmatrix} = \begin{pmatrix} \sum_i \sigma_i(e_1 v) \\ \vdots \\ \sum_i \sigma_i(e_n v) \end{pmatrix} \Rightarrow \begin{pmatrix} \sigma_1(v) \\ \vdots \\ \sigma_n(v) \end{pmatrix} = ({}^tM)^{-1} \underbrace{\begin{pmatrix} \sum_i \sigma_i(e_1 v) \\ \vdots \\ \sum_i \sigma_i(e_n v) \end{pmatrix}}_{\in V^G}$$

$\Rightarrow \sigma_1(v), \dots, \sigma_n(v) \in$ ~~ex~~ $\mathrm{Im}\ \mathrm{ev} \Rightarrow v \in \mathrm{Im}\ \mathrm{ev}$.

b) GD for Galois extensions

Let L/K be a Galois extn, finite.

A_0 a (fixed) K-algebra

Goal. Classify K-algebras A s.t. $A \otimes_K L \simeq A_0 \otimes_K L$, that is, the $\boxed{\text{twisted forms}}$ of A_0.

Let A be a twisted form of A_0, and fix an iso

$$\varphi: A_0 \otimes_K L \xrightarrow{\sim} A \otimes_K L$$

Let $H := \mathrm{Aut}_L(A_0 \otimes_K L)$. Since $G = \mathrm{Gal}(L/K) \curvearrowright A_0 \otimes L$, we get $G \curvearrowright H$ by conjugation.

Similarly there is an action $G \curvearrowright \mathrm{Isom}(A_0 \otimes_K L, A \otimes_K L)$ by conjugation.

Consider the map $f: G \longrightarrow H$, $\sigma \longmapsto \varphi^{-1} \circ \sigma(\varphi)$ (We are now in the process of constructing a cohomology class explicitly.)

$\forall \sigma, \tau \in G$:
$$\begin{aligned} f(\sigma\tau) &= \varphi^{-1} \circ \sigma\tau(\varphi) \\ &= \varphi^{-1} \circ \sigma(\varphi) \circ \sigma(\varphi^{-1}) \circ \sigma\tau(\varphi) \\ &= f(\sigma) \circ \sigma(f(\tau)) \end{aligned}$$

If $\varphi': A_0 \otimes_K L \to A \otimes_K L$ is another iso, $f': G \to H$, $\sigma \mapsto (\varphi')^{-1} \circ \sigma(\varphi')$

then $\forall \sigma \in G$: $f'(\sigma) = (\varphi^{-1}\varphi')^{-1} \circ f(\sigma) \circ \sigma(\varphi^{-1}\varphi')$.

Thus we associate to A a class $[A] \in \boxed{H^1(G, H)} := \{ f: G \to H \mid f(\sigma\tau) = f(\sigma) \circ \sigma(f(\tau)) \} / \sim$

where $f \sim f'$ if $\exists c \in H$ $\forall \sigma \in G$ $f'(\sigma) = c^{-1} \circ f(\sigma) \circ \sigma(c)$

We get a map $\boxed{\vartheta}: \{\text{twisted forms of } A_0 \text{ for } L \text{ fixed}\}/_{\text{iso}} \longrightarrow H^1(G, H)$.

Thm. ϑ is a bijection.

Rmk. $H^1(G, H)$ is a pointed set and not a group, with the distinguished elt being the constant 1 function. $\vartheta(A_0) = (\text{const. } 1.)$.

PF OF THM.: Consider $f: G \to H$ s.t. $f(\sigma\tau) = f(\sigma) \circ \sigma f(\tau)$ $\forall \sigma, \tau \in G$ 06.04.2019

$B := A \otimes_K L$ with $G \curvearrowright B$ by $G \curvearrowright L$

Twisted action of G on B: $\sigma_f\, b := f(\sigma)(\sigma \cdot b)$

This is indeed an action:
$$\begin{aligned} (\sigma\tau)_f\, b &= f(\sigma\tau)(\sigma\tau \cdot b) \\ &= f(\sigma) \circ \sigma \circ f(\tau) \circ \sigma^{-1} \circ \sigma\tau \cdot b \\ &= \sigma_f (\tau_f\, b) \end{aligned}$$

This action is semilinear:
$$\begin{aligned} \sigma_f(\lambda b) &= f(\sigma)\, \sigma(\lambda b) \\ &= f(\sigma)\, \sigma(\lambda)\, \sigma b \\ &= \sigma(\lambda)\, f(\sigma)(\sigma b) \\ &= \sigma(\lambda)(\sigma_f\, b) \end{aligned}$$

Speiser $\Rightarrow$ $\left({}_f B\right)^G \otimes L \xrightarrow[\sim]{L\text{-alg}} {}_f B \simeq B$ where ${}_f B$ is B with the twisted G-action

$\Rightarrow \left({}_f B\right)^G$ is a twisted form of A_0

One can check: $\psi : H^1(G, H) \longrightarrow \{\text{twisted forms of } A_0\}/\sim$
$$[f] \longmapsto \left[\left({}_f B\right)^G\right]$$
is a well-defined inverse for θ.

Rmk. When H is a gp with a compatible G-action, one can define
$\boxed{H^0(G, H)} := H^G$ and $H^1(G, H)$.

Then $H^0(G,H)$ is a group but $H^1(G,H)$ is only a pointed set.
These $H^0(G,H)$ and $H^1(G,H)$ satisfy properties similar to those of Galois cohomology.

If H is a gp with a compat & continuous action of $\mathrm{Gal}(\bar{K}/K)$ then let
$\boxed{H^0(K, H)} := H^{\mathrm{Gal}(\bar{K}/K)}$ and $\boxed{H^1(K,H)} := \varprojlim_{\substack{L/K \\ \text{fin Gal}}} H^1(L/K, H^{\mathrm{Gal}(L/K)})$

$$\Rightarrow \left\{A \ K\text{-algebra},\ A \otimes_K \bar{K} \simeq A_0 \otimes_K \bar{K}\right\} \simeq H^1\left(K, \mathrm{Aut}_{\bar{K}}\left(A_0 \otimes_K \bar{K}\right)\right)$$

Rmk. In general, if one wishes to classify objects Y/K s.t. $Y \otimes_K L \simeq X \otimes_K L$ for some X/K fixed then one may do the same and consider
$$H^1\left(\mathrm{Gal}(L/K), \mathrm{Aut}_L(X \otimes_K L)\right)$$

Examples. 1) The aut gp of the L-vector space L^n is $GL_n(L)$.
Hence $H^1(\mathrm{Gal}(L/K), GL_n(L))$ classifies n-dimensional K-vector spaces.
$\Rightarrow$ $\underline{H^1(\mathrm{Gal}(L/K), GL_n(L)) = \{*\}}$ (This is also called Hilbert 90.)

2) (V, q) n-dim quadratic space over K.
$\Rightarrow$ $\underline{H^1(K, \mathrm{Aut}_{\bar{K}}((V,q)\otimes \bar{K})) = H^1(K, O_n(\bar{K}))}$ classifies n-dim quad spaces $/K$.

c) The case of central simple algebras

Let L/K be a finite Galois extension. Then

$$\mathrm{Aut}_L(M_n(L)) \simeq PGL_n(L)$$
$$(M \mapsto CMC^{-1}) \leftarrow C$$

$\Rightarrow \left\{\begin{matrix} n\text{-dim central simple } K\text{-algebras} \\ \text{split over } L \end{matrix}\right\} \simeq H^1(L/K, PGL_n(L))$

For $m,n \geq 1$ consider the embedding

$$PGL_n(L) \hookrightarrow PGL_{mn}(L)$$
$$M \longmapsto \begin{pmatrix} \boxed{M} & & & 0 \\ & \boxed{M} & & \\ & & \ddots & \\ 0 & & & \boxed{M} \end{pmatrix}$$

This induces a map $\iota_{mn} : H^1(L/K, PGL_n(L)) \longrightarrow H^1(L/K, PGL_{mn}(L))$
$$[A] \longmapsto [M_m(A)]$$

Lemma. ι_{mn} is injective.

Pf.: Take A, B CSAs $/K$ s.t. $M_m(A) \simeq M_m(B)$ and A, B are n^2-dimensional.
Wedderburn $\Rightarrow$ the underlying division algebras are isomorphic,
moreover $\dim_K A = \dim_K B \Rightarrow A \simeq B$. □

We obtain $B(L/K) = \bigcup_{n \geq 1} H^1(L/K, PGL_n(L))$

Thm. $\delta_\infty : B(L/K) \xrightarrow{\sim} Br(L/K)$ is an iso of abelian groups.

Pf: Consider the exact sequence

$$1 \to L^\times \to GL_n(L) \to PGL_n(L) \to 1$$

and take cohomology to obtain

$$\underbrace{H^1(L/K, GL_n(L))}_{\{*\}\text{ by Hilbert 90}} \longrightarrow H^1(L/K, PGL_n(L)) \xrightarrow{\delta_n} \underbrace{H^2(L/K, L^\times)}_{Br(L/K)}$$

One gets $\delta_\infty : B(L/K) \to Br(L/K)$ by gluing all the δ_n's (this is purely formal).
Quitted: δ_∞ is a morphism of abelian groups.
Injectivity: δ_∞ is a group hom with trivial kernel $\Rightarrow$ injective.

<u>Surjectivity</u>: $e := [L:K]$. We are going to prove surjectivity of

$$\delta_e : H^1(L/K, PGL_n(L)) \longrightarrow H^2(L/K, L^\times).$$

Consider the diagram

$$\begin{tikzcd}
1 \arrow[r] & L^\times \arrow[r, "x \mapsto 1\otimes x"] \arrow[d, equal] \arrow[dr, phantom, "\circlearrowright"] & (L\otimes_K L)^\times \arrow[r] \arrow[d, "g"] & (L\otimes_K L)^\times / L^\times \arrow[r] \arrow[d, "\text{induced}"] & 1 \\
1 \arrow[r] & L^\times \arrow[r] & GL_n(L) \arrow[r] & PGL_n(L) \arrow[r] & 1
\end{tikzcd}$$

where
$$g : (L\otimes_K L)^\times \longrightarrow GL_n(L)$$
$$y \longmapsto \left(m_y : \begin{array}{ccc} L\otimes L & \longrightarrow & L\otimes L \\ x & \longmapsto & \end{array} \right)$$

Here $L \otimes_K L = K^\times \otimes_K L = L^\times$

Comm diag w/ exact rows $\Rightarrow$ if we make $Gal(L/K)$ act on $L\otimes_K L$ through the second factor, the action $Gal(L/K) \curvearrowright L\otimes_K L$ is $Gal(L/K)$-equivariant.

Apply cohomology:

$$\begin{tikzcd}
H^1(L/K, (L\otimes L)^\times/L^\times) \arrow[r] \arrow[d] & H^2(L/K, L^\times) \arrow[r] \arrow[d, equal] & \underbrace{H^2(L/K, (L\otimes L)^\times)}_{0} \\
H^1(L/K, PGL_e(L)) \arrow[r, "\delta_e"] & H^2(L/K, L^\times) &
\end{tikzcd}$$

As $Gal(L/K)$-modules, $L\otimes_K L \simeq L \otimes_{\mathbb{Z}} \mathbb{Z}[Gal(L/K)]$ by Normal Basis Theorem.
(i.e. $L\otimes L$ is an induced module)

$\Rightarrow (L\otimes_K L)^\times \simeq L^\times \otimes_{\mathbb{Z}} \mathbb{Z}[Gal(L/K)]$

Shapiro's Lemma $\Rightarrow H^2(L/K, (L\otimes_K L)^\times) = 0.$

Hence δ_e is surjective.

Cor. $B(K) \cong Br(K)$.

(This is just passing to the limit.)

§5 Cyclic central simple algebras

Let L/K be a cyclic extn of deg n, $\mathrm{Gal}(L/K) = \langle \sigma \rangle$, $b \in K^*$

Let $A := (\sigma, b) = \bigoplus_{i=0}^{n-1} L y^i \Big/ \langle y^n = b,\ \sigma(\lambda) y = y \lambda \ \ \forall \lambda \in L \rangle$

<u>Step 1:</u> L is a splitting field for A.

Consider the map
$$\varphi : A \otimes_K L \longrightarrow M_n(L)$$
$$y \otimes 1 \longmapsto \begin{pmatrix} 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \\ b & 0 & \cdots & 0 \end{pmatrix}$$
$$\lambda \otimes 1 \longmapsto \begin{pmatrix} \lambda & & & \\ & \sigma(\lambda) & & \\ & & \ddots & \\ & & & \sigma^{n-1}(\lambda) \end{pmatrix} \qquad \forall \lambda \in L$$

Observe that $\varphi(L \otimes_K L) = \begin{pmatrix} L & & & 0 \\ & L & & \\ & & \ddots & \\ 0 & & & L \end{pmatrix}$ because $L \otimes_K L \xrightarrow{\sim} L^n$, $\lambda \otimes \mu \longmapsto (\sigma(\lambda)\mu)$

$$\varphi(Ly \otimes_K L) = \varphi(L \otimes L) \cdot \varphi(y) = \begin{pmatrix} & L & & \\ & & \ddots & \\ & & & L \\ L & & & \end{pmatrix}$$

$$\varphi(L y^2 \otimes L) = \begin{pmatrix} & & L & & 0 \\ & & & \ddots & \\ & & & & L \\ L & 0 & 0 & & \\ 0 & L & & & \end{pmatrix}$$ etc.. These span $M_n(L) \Rightarrow \varphi$ is surjective.

$\dim_L M_n(L) = n^2 = \dim_L (A \otimes_K L) \Rightarrow \varphi$ is an iso and L splits A.

<u>Step 2.</u>

Consider
$$f_A : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Aut}_L(M_n(L))$$
$$\tau \longmapsto \varphi \circ \tau(\varphi^{-1}) = \varphi \circ \tau \circ \varphi^{-1} \circ \tau^{-1}$$

$$f_A(\sigma): \begin{pmatrix} & 1 & & \\ & & \ddots & \\ b & & & 1 \end{pmatrix} \xmapsto{\sigma^{-1}} \begin{pmatrix} & 1 & & \\ & & \ddots & \\ b & & & 1 \end{pmatrix} \xmapsto{\varphi^{-1}} y \otimes 1 \xmapsto{\tau} y \otimes 1 \xmapsto{\varphi} \begin{pmatrix} & 1 & & \\ & & \ddots & \\ b & & & 1 \end{pmatrix}$$

$$\begin{pmatrix} \lambda & & & \\ & \sigma(\lambda) & & \\ & & \ddots & \\ & & & \sigma^{n-1}(\lambda) \end{pmatrix} \xmapsto{\sigma^{-1}} \begin{pmatrix} \sigma^{n-1}(\lambda) & & & \\ & \lambda & & \\ & & \ddots & \\ & & & \sigma^{n-2}(\lambda) \end{pmatrix} \xmapsto{\varphi^{-1}} \sigma^{n-1}(\lambda) \otimes 1 \xmapsto{\sigma}$$

$$\xmapsto{\sigma} \sigma^{n-1}(\lambda) \otimes 1 \xmapsto{\varphi} \begin{pmatrix} \sigma^{n-1}(\lambda) & & \\ & \ddots & \\ & & \sigma^{n-2}(\lambda) \end{pmatrix}$$

This corresponds to $\begin{pmatrix} 0 & 1 & & 0 \\ \vdots & & \ddots & \\ b & 0 & \cdots & 1 \\ b & 0 & \cdots & 0 \end{pmatrix} \in PGL_n(L)$.

$$\Rightarrow \quad H^1(L/K, PGL_n(L)) = \{ \psi \in PGL_n(L) \mid \psi\, \sigma(\psi)\, \sigma^2(\psi) \cdots \sigma^{n-1}(\psi) = 1 \}/\sim$$

$$[f] \longmapsto f(\sigma)$$

where $\psi \sim \psi'$ if $\psi' = c^{-1} \psi\, \sigma(c)$ for some $c \in PGL_n(L)$

Hence A is split iff we can write

$f_A(\sigma) = c^{-1}\sigma(c)$ for some $c \in PGL_n(L)$,

$\mu f_A(\sigma) = \tilde{c}^{-1}\sigma(\tilde{c})$ for some $\tilde{c} \in PGL_n(L)$ and $\mu \in L^\times$.

$$\mu \tilde{c} = \sigma(\tilde{c}) \begin{pmatrix} 0 & 1 & & \\ & & \ddots & \\ & & & 1 \\ b & & & \end{pmatrix}, \quad \tilde{c} = \begin{pmatrix} \vdots & & \vdots \\ c_1 & \cdots & c_n \\ \vdots & & \vdots \end{pmatrix}$$

$$\mu c_1 = b\sigma(c_n)$$
$$\mu c_2 = \sigma(c_1)$$
$$\mu c_3 = \sigma(c_2)$$
$$\vdots$$

$\sigma(c_1) = \mu c_2$, $\sigma^2(c_1) = \mu\, \sigma(\mu)\, c_2$, $\ldots$, $\sigma^{n-1}(c_1) = \mu\, \sigma(\mu) \cdots \sigma^{n-2}(\mu)\, c_1$

$c_1 = \sigma^n(c_1) = b^{-1} N_{L/K}(\mu)\, c_1 \quad \Rightarrow \quad b = N_{L/K}(\mu)$

Conversely, if $b \in N_{L/K}(L^\times)$ then A is split.

Thm. The cyclic algebra (σ, b) is split $\Leftrightarrow$ $b \in N_{L/K}(L^\times)$ $\square$

Rmk.

$$B(L/K) \xleftarrow{\ \simeq\ } Br(L/K) \simeq \underbrace{K^\times/N_{L/K}(L^\times)}_{\text{cohom of cyclic gps.}}$$

$$(\sigma, b) \longleftarrow b$$

§6 Brauer group of local & global fields

13.05.2019

a) p-adic fields

Thm. 1) K p-adic field $\Rightarrow$ $Br\, K \simeq \mathbb{Q}/\mathbb{Z}$

2) $Br\, \mathbb{R} \simeq \mathbb{Z}/2\mathbb{Z}$, $Br\, \mathbb{C} = 0$.

SKETCH: 1) K^{ur} is C_1 $\Rightarrow$ $Br\, K^{ur} = 0$

Inf–Res $\Rightarrow$ $Br\, K \simeq Br(K^{ur}/K) = H^2(K^{ur}/K, (K^{ur})^\times)$

Understanding the module $(K^{ur})^\times$: dévissage of $(K^{ur})^\times$: $1 \to \mathcal{O}^\times_{K^{ur}} \to (K^{ur})^\times \xrightarrow{val} \mathbb{Z} \to 0$

LES: $\underbrace{H^1(K^{ur}/K, \mathbb{Z})} \to H^2(K^{ur}/K, \mathcal{O}^\times_{K^{ur}}) \to H^2(K^{ur}/K, K^{ur,\times}) \to H^2(K^{ur}/K, \mathbb{Z}) \to H^3(K, \mathcal{O}^\times_{K^{ur}})$

The Galois action is trivial $\Rightarrow$ $H^1(K^{ur}/K, \mathbb{Z}) = \mathrm{Hom}_c(Gal(K^{ur}/K), \mathbb{Z}) = 0$

($\forall G$ profinite: $\mathrm{Hom}_c(G, \mathbb{Z}) = 0$)

For $\mathcal{O}^\times_{K^{ur}}$, we have exact sequences

$$1 \to U^1_{K^{ur}} \to \mathcal{O}^\times_{K^{ur}} \to \bar{k}^\times \to 1$$

$U^1_{K^{ur}} = \{x \in \mathcal{O}_{K^{ur}} \mid x \equiv 1 \text{ in } k\}$ where k is the res field of K

$$\left.\begin{array}{l} 1 \to U^2 \to U^1 \to \bar{k} \to 0 \\ 1 \to U^3 \to U^2 \to \bar{k} \to 0 \\ \vdots \end{array}\right\}$$ apply cohomology to all these sequences, and use $H^i(K^{ur}/K, \bar{k}^\times) = H^i(k, \bar{k}^\times) = 0 \ \forall i \geq 1$ (by H90 for $i=1$, coh. dim for $i \geq 2$), and

$H^i(K^{ur}/K, \bar{k}) = H^i(k, \bar{k}) = 0 \quad \forall i \geq 1.$

LES $\Rightarrow$ $H^i(K^{ur}/K, \mathcal{O}_{K^{ur}}^\times) = H^i(K^{ur}/K, U^n_{K^{ur}}) \quad \forall n \geq 1 \quad \forall i \geq 2$

Technical limiting process $\rightsquigarrow$ $H^i(K^{ur}/K, \mathcal{O}^\times_{K^{ur}}) = 0 \ \forall i \geq 2$

Exact sequence concerning $H^2(K^{ur}/K, K^{ur,\times})$ $\Rightarrow$ $H^2(K^{ur}/K, K^{ur,\times}) \simeq H^2(K^{ur}/K, \mathbb{Z})$

$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ yields

$$\underbrace{H^1(K^{ur}/K, \mathbb{Q})}_{\substack{=0 \\ (\mathbb{Q} \text{ is divisible})}} \to H^1(K^{ur}/K, \mathbb{Q}/\mathbb{Z}) \to H^2(K^{ur}/K, \mathbb{Z}) \to \underbrace{H^2(K^{ur}/K, \mathbb{Q})}_{\substack{=0 \\ (\mathbb{Q} \text{ is divisible})}}$$

$$\mathrm{Br}\, K \simeq H^2(K^{ur}/K, \mathbb{Z}) \simeq H^1(K^{ur}/K, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}_c(\underbrace{\mathrm{Gal}(K^{ur}/K)}_{\hat{\mathbb{Z}}}, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z}$$

This proves 1).

2) $\mathbb{C}$ alg closed $\Rightarrow$ $\mathrm{Br}\, \mathbb{C} = 0$.

$$\mathrm{Br}\, \mathbb{R} = H^2(\underbrace{\mathbb{C}/\mathbb{R}}_{\text{cyclic}}, \mathbb{C}^\times) \underset{\substack{\uparrow \\ \text{coh of} \\ \text{cyclic gps}}}{=} \mathbb{R}^\times/\mathbb{R}^\times_{>0} \simeq \mathbb{Z}/2\mathbb{Z}$$

$\square$

b) Global fields

Thm. (Brauer – Hasse – Noether) K number field $\Rightarrow$ there is an exact sequence

$$0 \to \mathrm{Br}\, K \to \bigoplus_{\substack{v \in \Omega_K \\ \text{(set of places)}}} \mathrm{Br}\, K_v \xrightarrow{\mathrm{inv}_K} \mathbb{Q}/\mathbb{Z} \to 0$$

where $\mathrm{inv}_K : \bigoplus \mathrm{Br}\, K_v \longrightarrow \mathbb{Q}/\mathbb{Z}$ is $\bigoplus_v \mathrm{inv}_v$ and $\mathrm{inv}_v : \mathrm{Br}\, K_v \hookrightarrow \mathbb{Q}/\mathbb{Z}$.

Here inv_v is iso if v is finite;

the unique injection if v is infinite.

The proof is complicated, would probably take a whole semester to do it properly.

For local fields, the proof consisted of understanding the Galois module K^{ur} through $1 \to O_{K^{ur}}^{\times} \to K_{ur}^{\times} \to \mathbb{Z} \to 0$.

For understanding the cohomology, a crucial tool was Hilbert 90.

For a number field K, if L/K is cyclic then one has to study the exact sequence
$$1 \to L^{\times} \to \underset{\text{idèles}}{\mathbb{I}_L} \to \underset{\text{idèle classes}}{C_L} \to 1$$

The role played by $k^{\times}$ in the local case will be played by the idèle classes; the vanishing theorem here is $H^1(L/K, C_L) = 0$ (harder than H90).

Chapter 4. The Hasse principle

Def. K number field, $\mathcal{F}$ a family of K-varieties. We say that $\mathcal{F}$ satisfies $\boxed{\text{the Hasse principle}}$ (global-local principle) if
$$\forall X \in \mathcal{F}: \prod_{v \in \Omega_K} X(K_v) \neq \emptyset \Rightarrow X(K) \neq \emptyset$$

Here $\boxed{\text{variety}}$ means a separated scheme oft.

§1 Zero-dimensional varieties

Consider the variety given by $x^m = a$, $a \in K^{\times}$, $m \geq 1$. Recall the following:

Thm. (Chebotarev) L/K finite Galois extn of number fields, C a conjugacy class in $\mathrm{Gal}(L/K)$. Then there are infinitely many places v of K at which L/K is unramified and $\mathrm{Frob}_v \in C$.

Cor. K number field, $m \geq 1$. Then the restriction map
$$H^1(K, \mathbb{Z}/m\mathbb{Z}) \longrightarrow \prod_{v \in \Omega_K} H^1(K_v, \mathbb{Z}/m\mathbb{Z}) \quad \text{is injective.}$$

Pf: The map in question is the restriction map
$$\mathrm{Hom}_c(\mathrm{Gal}(\bar{K}, K), \mathbb{Z}/m\mathbb{Z}) \longrightarrow \prod_v \mathrm{Hom}_c(\mathrm{Gal}(\bar{K}_v/K_v), \mathbb{Z}/m\mathbb{Z})$$

Let α be in the kernel. Galois Theory $\Rightarrow$ α corresponds to a cyclic extension L of K of degree $\leq m$. Moreover, all decomposition groups of α are trivial. In particular, $\forall v \in \Omega_K$ unramified in L/K, Frob_v is trivial. Chebotarev $\Rightarrow$ L/K is also trivial. $\Rightarrow \alpha = 1$.

This reformulation of Chebotarev's Thm. will be our main tool.

Lemma. p prime, $m \geq 1$, $G \leq \mathrm{Aut}(\mathbb{Z}/p^m\mathbb{Z}) \simeq (\mathbb{Z}/p^m\mathbb{Z})^\times$ subgroup. Let A be the G-module s.t. $A \simeq \mathbb{Z}/p^m\mathbb{Z}$ as abelian groups & $G \curvearrowright A$ through $\mathrm{Aut}(\mathbb{Z}/p^m\mathbb{Z})$.

Then $H^1(G, A) = 0$ unless $p=2$ & $m \geq 2$ & $-1 \in G$.

Pf: Assume $p \neq 2$.

$(\mathbb{Z}/p^m\mathbb{Z})^\times$ is cyclic of order $(p-1)p^{m-1}$

$G_p :=$ p-Sylow of $G = \mathrm{Ker}(G \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times)$. This is a cyclic group, $\# G_p = p^{m-s}$ $(s \geq 1)$

Res – Cores $\Rightarrow$ enough to check $H^1(G_p, A) = 0$.

Let $\langle \alpha \rangle = G_p$. Since α has order p^{m-s}, we may write $\alpha = 1 + p^s u$, $p \nmid u$

$$1 + \alpha + \alpha^2 + \dots + \alpha^{p^{m-s}-1} = \frac{\alpha^{p^{m-s}} - 1}{\alpha - 1} = \frac{p^m v}{p^s u} \quad \text{with } p \nmid v$$

$$= p^{m-s} w \quad \text{with } p \nmid w$$

Then $\mathrm{Im}(\alpha - 1) = p^s A = \mathrm{Ker}(1 + \alpha + \dots + \alpha^{p^{m-s}-1})$

Coh of cyclic groups $\Rightarrow$ $H^1(G_p, A) = \mathrm{Ker}(1 + \dots + \alpha^{p^{m-s}-1}) / \mathrm{Im}(\alpha - 1) = 0$

Assume $p = 2$, $m \geq 2$.

$$(\mathbb{Z}/2^m\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$$

Since $-1 \notin G$, G is cyclic, let $\langle \alpha \rangle = G$.

- Case 1.: $v_2(\alpha - 1) \geq 2$ $\longrightarrow$ do the same as for $p \neq 2$
- Case 2.: $v_2(\alpha - 1) = 1$ $\Rightarrow$ $v_2(-\alpha - 1) \geq 2$ $\longrightarrow$ do the same as for $p \neq 2$ but with $(-\alpha)$ instead of α

The Lemma follows. $\square$

Thm. K number field, $m \geq 1$, and $\sqrt{-1} \in K$ if $2 \mid m$.

Then the Hasse principle holds for the variety given by $x^m = a$. $\forall a \in K^\times$.

Pf. When $m = p^r$ (p prime, $r \geq 1$).

$L := K(\mu_m)$.

Inf - Res $\Rightarrow$ we have a commutative diagram with exact column

Trivial by prev. Lemma: $\sqrt{-1} \in K$ makes sure we avoid the exceptional case.

EXACT

$$\begin{tikzcd}
0 \arrow[d] & \\
H^1(\mathrm{Gal}(L/K), \mu_m) \arrow[d] & \\
H^1(K, \mu_m) \arrow[r] \arrow[d] \arrow[dr, phantom, "\circlearrowright"] & \prod_{v \in \Omega_K} H^1(K_v, \mu_m) \arrow[d] \\
H^1(L, \mu_m) = H^1(L, \mathbb{Z}/m\mathbb{Z}) \arrow[r, hook, "\text{injective by Chebotarev}"'] & \prod_{w \in \Omega_L} \underbrace{H^1(L_w, \mu_m)}_{= H^1(L_w, \mathbb{Z}/m\mathbb{Z})}
\end{tikzcd}$$

$$\Rightarrow \quad K^\times / K^{\times m} = H^1(K, \mu_m) \hookrightarrow \prod_{v \in \Omega_K} H^1(K_v, \mu_m) = \prod_{v \in \Omega_K} K_v^\times / K_v^{\times m}$$

<u>Prop.</u> $K := \mathbb{Q}(\sqrt{7})$. Then the restriction map $K^\times / K^{\times 8} \to \prod_{v \in \Omega_K} K_v^\times / K_v^{\times 8}$ is not injective.

(So the assumption $\sqrt{-1} \in K$ in the Thm. is really necessary.)

Pf: Observe that $16 \notin K^{\times 8}$.

Let $v \in \Omega_K$.

- If v is finite and $v \nmid 2$:

  $2, -1$ or -2 is a square in the residue field $k(v)$.

  But $16 = (\sqrt{2})^8 = (\sqrt{-2})^8 = (1+\sqrt{-1})^8 \Rightarrow 16 \in k(v)^{\times 8} \Rightarrow 16 \in K_v^{\times 8}$ by Hensel's Lemma.

- If $v \mid 2$:

  -7 is a square mod $8 \Rightarrow -7$ is a square in $\mathbb{Q}_2$ by Hensel

  $\Rightarrow \sqrt{-7}, \sqrt{7} \in K_v \Rightarrow \sqrt{-1} \in K_v \Rightarrow (1+\sqrt{-1})^8 \in K_v \Rightarrow 16 \in K_v^{\times 8}$

- If v is infinite, $16 \in K_v^{\times 8}$ obviously.

So K does not satisfy the Hasse principle.