30.1.

Hilbert's "Theorem 90":

Let K/F be a cyclic Galois extension of fields.

Suppose $a \in K$ has $N_{K/F}(a) = 1$.

Then $a = \frac{\beta}{\sigma(\beta)}$ for some $\beta \in K$ with $Gal(K/F) = \langle \sigma \rangle$.

Three questions. (Increasing order of difficulty)

(1) How do we prove it?

(2) who cares?

(3) what does it mean?

Theorem. (Independence of Group Characters)

Let $\chi_1, \dots, \chi_n$ be homomorphisms $\underbrace{G}_{\text{some group}} \longrightarrow \underbrace{L}_{\text{any field}}^{\times}$

If they are distinct, they are linearly independent.

i.e. $\nexists$ $a_1, \dots, a_n$ not all zero with

$$a_1 \chi_1 + \dots + a_n \chi_n = 0 \text{ identically on } G.$$

(See DF, 14.2; Aluffi?)

Proof of Hilbert 90. (version due to D. Speyer)
(MathOverflow 21110; see also Emerton's)

Define $\tau : K \longrightarrow K$ $\quad \tau(b) = a\sigma(b)$

$$\tau^n(b) = a\sigma(a)\sigma^2(a) \cdots \sigma^{n-1}(a)\, b$$
$$= N(a) \cdot b = 1. \quad \text{So } \tau^n \text{ is the identity.}$$

(This is an F-linear rep'n of $\mathbb{Z}/n$ on L)

30.2.

Does τ have a fixed point? Suppose $\tau(\beta) = a\sigma(\beta) = \beta$

Then $a = \frac{\beta}{\sigma(\beta)}$ as desired.

If $\xi : K \to K$ is $\xi = \frac{1}{n}(1 + \tau + \tau^2 + \dots + \tau^{n-1})$

Then $\tau(\xi(x)) = \xi(x)$ clearly.

As long as ξ is not the zero operator we're done.

Previous theorem settles it!

Example. $K/F = \mathbb{Q}(i)/\mathbb{Q}$.

Iff $a = x + iy$ has norm 1, $x^2 + y^2 = 1$.

So $\{a \in \mathbb{Q}(i) : N(a) = 1\} \leftrightarrow$ rat'l pts. on circle.

By Hilbert 90, can write $x + iy = \frac{c+di}{c-di}$

$$= \frac{(c+di)^2}{c^2+d^2}$$

$$= \frac{c^2-d^2}{c^2+d^2} + \frac{2cd}{c^2+d^2} i.$$

Get the parametrization again.

Now, let G be a finite group,

and A an abelian group which is a left G-module:

$1(x) = x$.

$g(g'(x)) = (gg')x$.

$g(x + x') = gx + g'x$.

Example. G is a Galois group and A is a field.

(In fact we're interested in $A = K^\times$ with multiplication. i.e. $g(xx') = g(x)g(x')$.)

Definition. If A is a G-module we write

$$A^G = \{a \in A : g(a) = a \text{ for all } g \in G\}.$$

In Galois theory this is the fixed field.

Proposition / Exercise. ("Taking G-invariants is left exact")

Given an ES of G-modules

$$0 \to A \to B \to C \to 0.$$

(1) Prove there is an exact sequence

$$0 \to A^G \to B^G \to C^G.$$

(2) Show by example that we don't always have the final $\to 0$.

We also write this $H^0(G, A)$, the zeroth cohomology group.

Definition. Write

$$C^1(G, A) = \{\text{functions } \xi : G \to A\}. \quad \text{(1-cochains)}$$

$$Z^1(G, A) = \{\xi \in C^1(G, A) : \cancel{g(g(x)) =} \; \cancel{(gg)(x) =} \; \xi(g'g) = g'\xi(g) + \xi(g') \text{ for all } g, g'\}.$$

(1-cocycles)

$$B^1(G, A) = \{\xi \in C^1(G, A) : \xi(g) = ga - a \text{ for some fixed } a\}.$$

30.4.

The first cohomology group is

$$H^1(G, A) := Z^1(G, A) \big/ B^1(G, A).$$

Remark. (1) If A is a trivial G-module then

$$Z^1(G, A) = \{\xi : G \to A : \xi(gg') = \xi(g) + \xi(g')\}$$
$$= \mathrm{Hom}(G, A).$$

(2) You can define $H^i(G, A)$ for all $i \geq 0$.

Theorem. Given a SES of G-modules

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

there is a LES

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

Theorem. (Hilbert 90 again)

Let K/F be cyclic Galois. Then $H^1(G, K^\times) = 0$.

Proof. Given a cocycle $\xi : G \to K^\times$

Choose $x \in K^\times$ with $\displaystyle\sum_{i=0}^{n-1} \xi(\sigma^i)\sigma^i(x) = \beta \in K^\times$.
(use linear indep.!)

Then $$\sigma(\beta) = \sum_{i=0}^{n-1} \sigma\xi(\sigma^i)\sigma^{i+1}(x)$$
$$= \sum_{i=0}^{n-1} \xi(\sigma^{i+1})\xi(\sigma)^{-1}\sigma^{i+1}(x) \quad \text{(cocycle cond.)}$$
$$= \xi(\sigma^{-1})\beta.$$

So $\cancel{\xi(\sigma^{-1}) = \frac{\sigma(\beta)}{\beta}}$.

$$\xi(\sigma) = \frac{\beta}{\sigma(\beta)} = \frac{\sigma(\beta^{-1})}{\beta^{-1}}.$$

30.5

We also have

$$\xi(\sigma^2) = \sigma\xi(\sigma)\cdot\xi(\sigma)$$
$$= \sigma\left(\frac{\sigma(\beta^{-1})}{\beta^{-1}}\right)\cdot\frac{\sigma(\beta^{-1})}{\beta^{-1}} = \frac{\sigma^2(\beta^{-1})}{\sigma(\beta^{-1})}\cdot\frac{\sigma(\beta^{-1})}{\beta^{-1}} = \frac{\sigma^2(\beta^{-1})}{\beta^{-1}}$$

and so on.

Claim. This implies the old Hilbert 90.

Why? Suppose $x \in K^\times$ and define a cocycle ξ by

$$\xi(\sigma) = x.$$

Then
$$\xi(\sigma^2) = \sigma\xi(\sigma)\cdot\xi(\sigma) = \sigma(x)\cdot x$$
$$\xi(\sigma^3) = \sigma\xi(\sigma^2)\cdot\xi(\sigma) = \sigma(\sigma(x)\cdot x)\cdot x$$
$$= \sigma^2(x)\cdot\sigma(x)\cdot x$$

$\vdots$

$$\xi(1) = \sigma^{n-1}(x)\,\sigma^{n-2}(x)\cdots\cdot x = N(x).$$

We get a cocycle iff $N(x)=1$.

But $\xi(\sigma) = \dfrac{\beta}{\sigma(\beta)}$ for some β. DONE.

31.1

Proposition. (Basic Kummer Theory)

Given any $\begin{cases} \text{integer } m \geq 2 \\ \text{number field with } \mu_m \subseteq K \\ \text{cyclic extension } L/K \text{ of degree } m \end{cases}$

Then $L = K(\sqrt[m]{\alpha})$ for some $\alpha \in K$.

Proof. Let $\mathrm{Gal}(L/K) = \langle \sigma \rangle$. Since $N(\zeta_m) = N(\zeta_m^{-1}) = 1$,

$\exists\ \alpha \in L$ with $\sigma(\alpha) = \zeta_m \cdot \alpha$.

Then $\alpha \notin K$, and $\zeta_m^i \cdot \alpha$ are distinct conjugates of α, all in L, so $[K(\sqrt[m]{\alpha}) : K] \geq m$

so equality with $L = K(\sqrt[m]{\alpha})$.

Proposition. (More serious Kummer theory)

Same m and K.

An abelian extension L/K is of exponent m if $\sigma^m = 1$ for all $\sigma \in \mathrm{Gal}(L/K)$.

There is a bijection

$$K^\times / (K^\times)^m \longleftrightarrow \text{abelian extensions of exponent } m$$

$$B \longrightarrow K(\sqrt[m]{B}).$$

31.2.

The basic idea: If $L = K(\sqrt[m]{B})$, $G = \mathrm{Gal}(L/K)$, the map

$$G \times B \longrightarrow \mu_m$$
$$(\sigma, x) \longrightarrow \frac{\sigma(x)}{x} =: \langle \sigma, x \rangle$$

is: bilinear: $\langle \sigma\sigma', x \rangle = \langle \sigma, x \rangle \langle \sigma', x \rangle$

$\langle \sigma, x x' \rangle = \langle \sigma, x \rangle \langle \sigma, x' \rangle$

and perfect: $\operatorname{Ker} \langle \sigma, - \rangle = 1$

$\operatorname{Ker} \langle -, B \rangle = 1.$

Via cohomology:

Start with the SES

$$1 \longrightarrow \mu_m \longrightarrow \bar{K}^\times \xrightarrow{x \to x^m} \bar{K}^\times \longrightarrow 1.$$

Take $G_{\bar{K}/K}$ - cohomology:

$$1 \to \mu_m^{G_{\bar{K}/K}} \to (\bar{K})^{\times\, G_{\bar{K}/K}} \xrightarrow{x \to x^m} (\bar{K}^\times)^{G_{\bar{K}/K}}$$
$$\longrightarrow H^1(G_{\bar{K}/K}, \mu_m) \longrightarrow H^1(G_{\bar{K}/K}, \bar{K}^\times) \longrightarrow \cdots$$

This is

$$1 \to \mu_m \longrightarrow K^\times \longrightarrow K^\times \longrightarrow H^1(G_{\bar{K}/K}, \mu_m) \longrightarrow \underset{\text{Hilbert 90!}}{0} \longrightarrow \cdots$$

Since $\mu_m \subseteq K$, $G_{\bar{K}/K}$ acts trivially on μ_m.

Therefore $H^1(G_{\bar{K}/K}, \mu_m) = \mathrm{Hom}(G_{\bar{K}/K}, \mu_m)$

and so $K^\times/(K^\times)^m \xrightarrow{\sim} \mathrm{Hom}(G_{\bar{K}/K}, \mu_m)$.

This is what we can get from a perfect bilinear pairing

$$\cancel{G_{K}}\ G_{\bar{K}/K} \times K^\times/(K^\times)^m \longrightarrow \mu_m$$

The map above is $x \longrightarrow \langle -, x \rangle$.

Really this says $\mathrm{Hom}(A \times B, C) = \mathrm{Hom}(A, \mathrm{Hom}(B, C))$.

The elliptic curve version.

Start with

$$0 \longrightarrow E[m] \longrightarrow E(\bar{K}) \xrightarrow{\times m} E(\bar{K}) \longrightarrow 0$$

Take $G_{\bar{K}/K}$ - cohomology:

$$0 \to E(K)[m] \to E(K) \longrightarrow E(K) \longrightarrow \underbrace{H^1(G_{\bar{K}/K}, E[m])}$$

This is $\mathrm{Hom}(G_{\bar{K}/K}, E[m])$ if $\mu_m \subseteq K$ (assume $m=2$ is easy!!)

And so (if $\mu_m \subseteq K$) $E(K)/mE(K) \hookrightarrow \mathrm{Hom}(G_{\bar{K}/K}, E[m])$.

we'll pick this up.