- **Classfield Theory...**

- More modern statement of part of classfield theory
- Recall: special case, unramified local classfield theory
- Recall: special case: quadratic local classfield theory over $\mathbb{Q}_p$
- Recall: general Kummer theory, linear independence of roots
- Cyclotomic extensions
- Recollection of Hilbert's Theorem 90

Part of Global Classfield Theory: The Galois groups of finite abelian extensions K of a number field k are the finite quotients of the idele class group $\mathbb{J}_k/k^\times$, namely

$$(\mathbb{J}_k/k^\times)/N_k^K(\mathbb{J}_K/K^\times) \quad \longleftrightarrow \quad K/k$$

The maps of quotients of idele class groups to Galois groups are *natural*, in the sense that, for finite abelian extensions $L \supset K \supset k$ there is a commutative diagram, with horizontal maps the **Artin** or **reciprocity law** maps

$$\begin{tikzcd} \mathbb{J}_k/k^\times)/N_k^L(\mathbb{J}_L/L^\times) \arrow[r, "\alpha_{L/k}"] \arrow[d, "\text{quot}"'] & \mathrm{Gal}(L/k) \arrow[d, "\text{quot}"] \\ \mathbb{J}_k/k^\times)/N_k^K(\mathbb{J}_K/K^\times) \arrow[r, "\alpha_{K/k}"'] & \mathrm{Gal}(K/k) \end{tikzcd}$$

Main Theorem of Local Classfield Theory: The Galois groups of finite abelian extensions K of a local field k are the quotients

$$k^\times / N_k^K(K^\times) \quad \longleftrightarrow \quad K/k$$

The maps to Galois groups are *natural*, in the sense that, for finite abelian extensions $L \supset K \supset k$ there is a commutative diagram, with horizontal maps the **Artin** or **reciprocity law** maps

$$\begin{tikzcd} k^\times / N_k^L(L^\times) \arrow[r, "\alpha_{L/k}"] \arrow[d, "\text{quot}"'] & \mathrm{Gal}(L/k) \arrow[d, "\text{quot}"] \\ k^\times / N_k^K(K^\times) \arrow[r, "\alpha_{K/k}"'] & \mathrm{Gal}(K/k) \end{tikzcd}$$

Remark: We'd want a precise connection between local and global, too.

(Mock) Theorem: *Unramified local classfield theory:* For *unramified extensions* $L \supset K \supset k$ of a local field k, we have the commutative compatibility diagram

$$\begin{tikzcd} k^\times/N_k^L(L^\times) \arrow[r, "\alpha_{L/k}"] \arrow[d, "\text{quot}"'] & \mathrm{Gal}(L/k) \arrow[d, "\text{quot}"] \\ k^\times/N_k^K(K^\times) \arrow[r, "\alpha_{K/k}"'] & \mathrm{Gal}(K/k) \end{tikzcd} \qquad \text{for unramified} \qquad \begin{tikzcd} L \arrow[d, dash] \\ K \arrow[d, dash] \\ k \end{tikzcd}$$

Remark: The maps $\alpha_{K/k}$ are called *Artin maps* or *reciprocity law maps*, are here given by Frobenius, characterized by

$$(\mathfrak{p}, K/k)(x) \;=\; x^q \bmod \mathfrak{p}\mathfrak{o}_K \qquad\qquad (x \in \mathfrak{o}_K, \text{ where } q = \#\mathfrak{o}_k/\mathfrak{p})$$

(Mock) Theorem: Let $p > 2$. The quadratic extensions K of $\mathbb{Q}_p$ are in bijection with the subgroups H of index 2 in $\mathbb{Q}_p^\times$, by

$$\mathbb{Q}_p^\times / N_{\mathbb{Q}_p}^K(K^\times) \quad \approx \quad \mathrm{Gal}(K/\mathbb{Q}_p)$$

The extension $K/\mathbb{Q}_p$ is unramified if and only if $N_{\mathbb{Q}_p}^K(K^\times) \supset \mathbb{Z}_p^\times$.

Remark: In the unique unramified quadratic extension, the map to the Galois group takes the prime p to the Frobenius element

$$(p, K/\mathbb{Q}_p)(x) \quad = \quad x^p \mod p\mathfrak{o}_K \qquad\qquad (x \in \mathfrak{o}_K)$$

But this cannot describe the isomorphisms for the ramified extensions, since the residue class field extensions are *trivial* in these cases.

General Kummer theory: Cyclic extensions K of degree dividing ℓ of a field k of characteristic not dividing ℓ and containing ℓ^{th} roots of unity are in bijection with cyclic subgroups of $k^\times/(k^\times)^\ell$, by $K = k(\sqrt[\ell]{\alpha}) \longleftrightarrow \langle\alpha\rangle \bmod (k^\times)^\ell$. ///

Just to be clear: Any finite extension K of k obtained by adjoining n^{th} roots, where k contains n^{th} roots of unity and characteristic does not divide n, is *abelian*:

Proof: K has a k-basis of elements $\sqrt[n]{a}$ for $a \in k$, and these are $\mathrm{Gal}(K/k)$-eigenvectors, with eigenvalues roots of unity lying in k. That is, the k-linear automorphisms $\mathrm{Gal}(K/k)$ of K are simultaneously diagonalized by such a basis. In particular, $\mathrm{Gal}(K/k)$ is abelian. ///

Fix $2 \leq \ell \in \mathbb{Z}$, k a field of characteristic not dividing ℓ, containing a primitive ℓ^{th} root of unity. Let $a_1, \ldots, a_n \in k^\times$, and $\alpha_j = \sqrt[\ell]{a_j}$ in a fixed finite Galois extension K of k.

Suppose that, for any pair of indices $i \neq j$, there is $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(\alpha_i)/\alpha_i \neq \sigma(\alpha_j)/\alpha_j$. Since $\sigma(\alpha_i) = \omega_i \cdot \alpha_i$ for some ℓ^{th} root of unity ω_i (depending on σ), the hypothesis is equivalent to a_i/a_j *not* being an n^{th} power in k.

The hypothesis is that the one-dimensional representations of $\mathrm{Gal}(K/k)$ on the lines $k \cdot \alpha_j$ are pairwise non-isomorphic.

Proposition: The α_j's are *linearly independent* over k. ///

Corollary: For *(pairwise) relatively prime* square-free integers $a_1, \ldots, a_n$, the 2^n algebraic numbers $\sqrt{a_{i_1} \ldots a_{i_k}}$ with $i_1 < \ldots < i_k$ and $0 \le k \le n$ are linearly independent over $\mathbb{Q}$, so are a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$. In particular, the degree of that field over $\mathbb{Q}$ is the maximum possible, 2^n. ///

Corollary: Let k be a field containing n^{th} roots of unity, with characteristic not dividing n. For a subgroup Θ of $k^\times$ containing $(k^\times)^n$ and with $\Theta/(k^\times)^n$ *finite*,

$$[k\Big(n^{th} \text{ roots of } a \in \Theta\Big) : k] \quad = \quad \# \, \Theta/(k^\times)^n$$

Remark: Reformulate to resemble classfield theory...

As above, let k be a field containing n^{th} roots of unity, with characteristic not dividing n.

Fix a subgroup Θ of $k^\times$ containing $(k^\times)^n$ and with $\Theta/(k^\times)^n$ *finite*. Let

$$K \;=\; k\Big(n^{th} \text{ roots of } \theta \in \Theta/(k^\times)^n\Big)$$

For $\sigma \in \mathrm{Gal}(K/k)$ and $\theta \in \Theta$, for an n^{th} root $\sqrt[n]{\theta}$,

$$\sigma(\sqrt[n]{\theta}\,) \;=\; \omega_\theta(\sigma) \cdot \sqrt[n]{\theta} \qquad\qquad (\text{with } \omega_\theta(\sigma)^n = 1)$$

As for any collection of eigenvalues for a simultaneous eigenvector, $\sigma \to \omega_\theta(\sigma)$ is a *group homomorphism* for each $\sqrt[n]{\theta}$, using the fact that $\sigma, \tau \in \mathrm{Gal}(K/k)$ are k-linear and k contains n^{th} roots of unity:

$$\omega_\theta(\sigma\tau) \cdot \sqrt[n]{\theta} \;=\; (\sigma\tau)(\sqrt[n]{\theta}) \;=\; \sigma\big(\tau(\sqrt[n]{\theta})\big)$$

$$=\; \sigma\Big(\omega_\theta(\tau) \cdot \sqrt[n]{\theta}\Big) \;=\; \omega_\theta(\tau) \cdot \sigma(\sqrt[n]{\theta}) \;=\; \omega_\theta(\tau)\omega_\theta(\sigma) \cdot \sqrt[n]{\theta}$$

Also, $\sigma \times \theta \to \omega_\theta(\sigma)$ is a group homomorphism in θ: the ambiguity of choice(s) of n^{th} roots has no impact: with $\sqrt[n]{\theta\theta'} = \omega \cdot \sqrt[n]{\theta} \cdot \sqrt[n]{\theta'}$ for whatever n^{th} root of unity ω,

$$\omega_{\theta\theta'}(\sigma) \cdot \sqrt[n]{\theta\theta'} \;=\; \sigma(\sqrt[n]{\theta\theta'}) \;=\; \sigma(\omega \cdot \sqrt[n]{\theta} \cdot \sqrt[n]{\theta'})$$

$$= \; \omega \cdot \sigma(\sqrt[n]{\theta}) \cdot \sigma(\sqrt[n]{\theta'}) \;=\; \omega \cdot \omega_\theta(\sigma) \cdot \sqrt[n]{\theta} \cdot \omega_{\theta'}(\sigma) \cdot \sqrt[n]{\theta'}$$

$$= \; \omega_\theta(\sigma)\omega_{\theta'}(\sigma)\big(\omega \cdot \sqrt[n]{\theta} \cdot \sqrt[n]{\theta'}\big) \;=\; \omega_\theta(\sigma)\omega_{\theta'}(\sigma)\sqrt[n]{\theta\theta'}$$

Certainly $(k^\times)^n$ maps to 1. Thus, we have a group homomorphism

$$\mathrm{Gal}(K/k) \;\times\; \Theta/(k^\times)^n \;\longrightarrow\; (n^{th} \text{ roots of unity})$$

and both groups are abelian, torsion of exponent dividing n. This gives a *duality* rather than an *isomorphism*...

Remark: Yes, a finite abelian group A is *non-canonically* isomorphic to its dual

$$A^\vee \;=\; \mathrm{Hom}_{\mathbb{Z}}(A,\,\mathbb{Q}/\mathbb{Z})$$

The popular identification

$$\mathbb{Q}/\mathbb{Z} \approx \{\text{roots of unity}\} \qquad \text{by} \qquad t \to e^{2\pi i t} \in \mathbb{C}^\times$$

is *not* canonical, and is not relevant to consideration of abstract fields k, because it depends on complex numbers to distinguish roots of unity.

In fact, in abstract Kummer theory, it is reasonable to obtain a duality rather than an isomorphism, because in this abstraction we have no device producing a map from $k^\times$ to the Galois group.

In contrast, for example, a choice of *generator* γ for a cyclic group of order n gives an isomorphism to its dual, by

$$\gamma^s \quad\longrightarrow\quad \big(\gamma^t \longrightarrow \frac{st}{n}\big)$$

Global cyclotomic extensions:

Let $K = \mathbb{Q}(\zeta)$ for ζ a primitive n^{th} root of unity. Grant that the ring of integers $\mathfrak{o}$ is $\mathbb{Z}[\zeta]$.

We know $[K : \mathbb{Q}] = \varphi(n)$ with the Euler totient function $\varphi(p_1^{e_1} \ldots) = (p_1 - 1)p^{e_1-1} \ldots$ and the Galois group is isomorphic to $(\mathbb{Z}/n)^\times$, by

$$(\mathbb{Z}/n)^\times \ni \ell \quad \longrightarrow \quad \sigma_\ell : \zeta \to \zeta^\ell$$

For prime p, σ_p *is the* p^{th} *Frobenius/Artin element:* since p divides the inner binomial coefficients $\binom{p}{j}$ with $0 < j < p$, and since $c_i^p = c_i \bmod p$ for $c_i \in \mathbb{Z}$,

$$\sigma_p\Big(\sum_i c_i\, \zeta^i\Big) = \sum_i c_i\, \zeta^{ip} = \Big(\sum_i c_i\, \zeta^i\Big)^p \bmod p\mathfrak{o}$$

$(\mathbb{Z}/n)^\times$ *is* the generalized ideal class group with conductor n.

Recall Hilbert's Theorem 90:

Claim: In a field extension K/k of degree n with cyclic Galois group generated by σ, the elements in K of norm 1 are exactly those of the form $\sigma\alpha/\alpha$ for $\alpha \in K$.

Proof: On one hand, for *any* finite Galois extension K/k, for $\sigma \in \mathrm{Gal}(K/k)$ and $\alpha \in K$,

$$N_k^K\left(\frac{\sigma\alpha}{\alpha}\right) \;=\; \prod_{\tau\in\mathrm{Gal}(K/k)} \tau\left(\frac{\sigma\alpha}{\alpha}\right) \;=\; \frac{\prod_\tau \tau\sigma\alpha}{\prod_\tau \tau\alpha} \;=\; \frac{\prod_\tau \tau\alpha}{\prod_\tau \tau\alpha} \;=\; 1$$

by changing variables in the numerator. This is the easy direction.

The other direction uses the cyclic-ness. Let $\beta \in K$ with $N_k^K(\beta) = 1$. *Linear independence of characters* implies that the map $\varphi : K \to K$ by $\varphi = 1_K + \beta\sigma + \beta\beta^\sigma\sigma^2 + \ldots + \beta^{1+\sigma+\ldots+\sigma^{n-2}}\sigma^{n-1}$ is not identically 0.

The not-identical-vanishing assures that there is $\gamma \in K$ such that

$$0 \neq \alpha = \varphi(\gamma) = \gamma + \beta\gamma^\sigma + \beta\beta^\sigma\gamma^{\sigma^2} + \ldots + \beta^{1+\sigma+\ldots+\sigma^{n-2}}\gamma^{\sigma^{n-1}}$$

Then $\beta\alpha^\sigma = \alpha$, and $\beta = \alpha/\sigma\alpha$. ///

Hilbert' Theorem 90 gives another proof of

Corollary: A cyclic degree n extension K/k of k containing n^{th} roots of unity is obtained by adjoining an n^{th} root.

Proof: For primitive n^{th} root of unity ζ, since $N_k^K(\zeta) = \zeta^n = 1$, by Hilbert's Theorem 90 there is $\alpha \in K$ such that $\zeta = \sigma\alpha/\alpha$. That is, $\sigma\alpha = \zeta \cdot \alpha$ and $\sigma(\alpha^n) = \alpha^n$, so $\alpha^n \in k$... ///

Additive version of Theorem 90: Let K/k be cyclic of degree n with Galois group generated by σ. Then $\mathrm{tr}_k^K(\beta) = 0$ if and only if there is $\alpha \in K$ such that $\beta = \alpha - \alpha^\sigma$.

Proof: The traces of elements $\alpha - \sigma\alpha$ are easily 0, again. *Linear independence of characters* shows that trace is not identically 0, so there is γ with non-zero trace. With

$$\alpha \;=\; \frac{1}{\mathrm{tr}_k^K(\gamma)}\Big(\beta\gamma^\sigma + (\beta+\beta^\sigma)\gamma^{\sigma^2} + \ldots + (\beta+\beta^\sigma+\ldots+\beta^{\sigma^{n-2}})\gamma^{\sigma^{n-1}}\Big)$$

we have $\beta = \alpha - \alpha^\sigma$. ///

Corollary: *(Artin-Schreier extensions)* Let K/k be cyclic of order p in characteristic p. Then there is $K = k(\alpha)$ with α satisfying an equation $x^p - x + a = 0$ with $a \in k$.

Proof: Since $\mathrm{tr}_k^K(-1) = p \cdot (-1) = -p = 0$, by additive Theorem 90 there is α such that $\alpha - \alpha^\sigma = -1$, which is $\alpha^\sigma = \alpha + 1$... ///