• 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

$$\frac{(\mathbb{J}_k/k^\times)}{N^K_k(\mathbb{J}_K/K^\times)} \leftrightarrow K/k$$

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

$$\frac{\mathbb{J}_k/k^\times}{N^L_k(\mathbb{J}_L/L^\times)} \xrightarrow{\alpha_{L/k}} \text{Gal}(L/k)$$

$$\frac{\mathbb{J}_k/k^\times}{N^K_k(\mathbb{J}_K/K^\times)} \xrightarrow{\alpha_{K/k}} \text{Gal}(K/k)$$
Main Theorem of Local Classfield Theory: The Galois groups of finite abelian extensions $K$ of a local field $k$ are the quotients

$$k^\times / N^K_k(K^\times) \leftrightarrow K/k$$

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

$$
\begin{array}{ccc}
  k^\times / N^L_k(L^\times) & \longrightarrow & \text{Gal}(L/k) \\
  \downarrow \text{quot} & & \downarrow \text{quot} \\
  k^\times / N^K_k(K^\times) & \longrightarrow & \text{Gal}(K/k)
\end{array}
$$

**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

\[
\begin{array}{ccc}
\mathbb{F}^\times / N_k^L (L^\times) & \xrightarrow{\alpha_{L/k}} & \text{Gal}(L/k) \\
\downarrow \text{quot} & & \downarrow \text{quot} \\
\mathbb{F}^\times / N_k^K (K^\times) & \xrightarrow{\alpha_{K/k}} & \text{Gal}(K/k) \\
\end{array}
\]

for unramified $K$

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

\[(p, K/k)(x) = x^q \pmod{p \mathfrak{o}_K} \quad (x \in \mathfrak{o}_K, \text{where } q = \# \mathfrak{o}_k/p)\]
(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

$$\mathbb{Q}_p^\times / N^{K}_{\mathbb{Q}_p}(K^\times) \cong \text{Gal}(K/\mathbb{Q}_p)$$

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

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

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

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 $\ell$ of a field $k$ of characteristic not dividing $\ell$ and containing $\ell^{th}$ roots of unity are in bijection with cyclic subgroups of $k^\times /(k^\times)^\ell$, by $K = k(\sqrt[\ell]{\alpha}) \leftrightarrow \langle \alpha \rangle \mod (k^\times)^\ell$. 

*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 $\text{Gal}(K/k)$-eigenvectors, with eigenvalues roots of unity lying in $k$. That is, the $k$-linear automorphisms $\text{Gal}(K/k)$ of $K$ are simultaneously diagonalized by such a basis. In particular, $\text{Gal}(K/k)$ is abelian. 

///
Fix $2 \leq \ell \in \mathbb{Z}$, $k$ a field of characteristic not dividing $\ell$, containing a primitive $\ell^{th}$ 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 $\sigma \in \text{Gal}(K/k)$ such that $\sigma(\alpha_i)/\alpha_i \neq \sigma(\alpha_j)/\alpha_j$. Since $\sigma(\alpha_i) = \omega_i \cdot \alpha_i$ for some $\ell^{th}$ root of unity $\omega_i$ (depending on $\sigma$), 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 $\text{Gal}(K/k)$ on the lines $k \cdot \alpha_j$ are pairwise non-isomorphic.

**Proposition:** The $\alpha_j$’s are *linearly independent* over $k$. ///
Corollary: For (pairwise) relatively prime square-free integers $a_1, \ldots, a_n$, the $2^n$ algebraic numbers $\sqrt{a_{i_1} \cdots a_{i_k}}$ with $i_1 < \ldots < i_k$ and $0 \leq k \leq n$ 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 $\Theta$ of $k^\times$ containing $(k^\times)^n$ and with $\Theta/(k^\times)^n$ finite,

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

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 $\Theta$ of $k^\times$ containing $(k^\times)^n$ and with $\Theta/(k^\times)^n$ finite. Let

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

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

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

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

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

$$= \sigma(\omega_{\theta}(\tau) \cdot \sqrt[n]{\theta}) = \omega_{\theta}(\tau) \cdot \sigma(\sqrt[n]{\theta}) = \omega_{\theta}(\tau)\omega_{\theta}(\sigma) \cdot \sqrt[n]{\theta}$$
Also, $\sigma \times \theta \rightarrow \omega_\theta(\sigma)$ is a group homomorphism in $\theta$: 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 $\omega$,

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

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

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

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

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

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

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

The popular identification

$$\mathbb{Q}/\mathbb{Z} \approx \{\text{roots of unity}\} \quad \text{by} \quad t \rightarrow e^{2\pi it} \in \mathbb{C}^\times$$

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* $\gamma$ for a cyclic group of order $n$ gives an isomorphism to its dual, by

$$\gamma^s \quad \rightarrow \quad (\gamma^t \rightarrow \frac{st}{n})$$
Global cyclotomic extensions:

Let \( K = \mathbb{Q}(\zeta) \) for \( \zeta \) 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 \( \varphi(p_1^{e_1} \ldots) = (p_1 - 1)p_1^{e_1-1} \ldots \) and the Galois group is isomorphic to \((\mathbb{Z}/n)^\times\), by

\[
(\mathbb{Z}/n)^\times \ni \ell \rightarrow \sigma_\ell : \zeta \rightarrow \zeta^\ell
\]

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

\[
\sigma_p \left( \sum_i c_i \zeta^i \right) = \sum_i c_i \zeta^{ip} = \left( \sum_i c_i \zeta^i \right)^p \mod p \mathfrak{o}
\]

\((\mathbb{Z}/n)^\times\) 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 $\sigma$, 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 $\sigma \in \text{Gal}(K/k)$ and $\alpha \in K$,

$$N^K_k \left( \frac{\sigma \alpha}{\alpha} \right) = \prod_{\tau \in \text{Gal}(K/k)} \tau \left( \frac{\sigma \alpha}{\alpha} \right) = \frac{\prod_{\tau} \tau \sigma \alpha}{\prod_{\tau} \tau \alpha} = \frac{\prod_{\tau} \tau \alpha}{\prod_{\tau} \tau \alpha} = 1$$

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 $\varphi = 1_K + \beta \sigma + \beta^2 \sigma^2 + \ldots + \beta^{1+\sigma+\ldots+\sigma^2} \sigma^2$ 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 \( \zeta \), 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 $\sigma$. Then $\text{tr}_K^k(\beta) = 0$ 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 $\gamma$ with non-zero trace. With

$$\alpha = \frac{1}{\text{tr}_K^k(\gamma)} \left( \beta \gamma^\sigma + (\beta + \beta^\sigma) \gamma^\sigma^2 + \ldots + (\beta + \beta^\sigma + \ldots + \beta^{n-2}) \gamma^{\sigma^{n-1}} \right)$$

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 $\alpha$ satisfying an equation $x^p - x + a = 0$ with $a \in k$.

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