• **Classfield Theory...**

• More modern statement of part of *global* classfield theory
• Recall facts about extensions of *finite* fields
• Recall: unramified extensions of *local* fields
• Recall: special case, unramified local classfield theory
• Recall: special case: quadratic local classfield theory over $\mathbb{Q}_p$
• Recall: general Kummer theory

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

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

The maps $\alpha_{*/k}$ are **Artin maps** or **reciprocity law maps**

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

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

The maps $\alpha_{*/k}$ are **local Artin** or **local reciprocity law** maps.

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

Note that the adelic rewrite of global classfield theory shows the connection to *norms*.

In *cyclic* extensions, the connection between global and local norms is clear:

Cyclic local-global principle for norms: In a *cyclic* extension K/k of number fields, an element of k is a *global norm* if and only if it is a *local norm everywhere*. That is, for $\alpha \in k$,

$$\alpha \in N_k^K(K^\times) \iff \alpha \in N_{k_v}^{K_w}(K_w^\times) \text{ for all } v, w$$

Proof by analytic properties of *zeta functions of simple algebras*.

Norm index inequalities play a central role in proofs of classfield theory.

Unramified extensions of local fields: Inside a fixed algebraic closure of a local field k, for each positive integer n there is a unique *unramified* extension K of k of degree n. It is generated by a primitive $q^n - 1$ root of unity, where $\#\mathfrak{o}_k/\mathfrak{p} = q$. ///

Artin/Frobenius elements in Galois groups over local fields An unramified extension K/k of a local field k has cyclic Galois group with canonical generator the Artin/Frobenius $(\mathfrak{p}, K/k)$, where $\mathfrak{p}$ is the prime in $\mathfrak{o}_k$, characterized by

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

Claim: The Galois norm $N : K \to k$ of local fields gives a *surjection* on local units $\mathfrak{o}_K^\times \to \mathfrak{o}_k^\times$. ///

[Proof was by surjectivity of norms on *finite* fields, as well as surjectivity of *traces*, and completeness of k.]

Two very special sub-cases:

(Mock) Theorem: *Unramified local classfield theory:* Galois groups of unramified extensions K of a local field k are in bijection with finite-index subgroups of $k^\times$ containing $\mathfrak{o}_k^\times$, by

$$k^\times / N_k^K(K^\times) \;\approx\; \mathrm{Gal}(K/k) \qquad\qquad \text{(reciprocity law map)}$$

(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

$$\mathbb{Q}_p^\times / N_{\mathbb{Q}_p}^K(K^\times) \;\approx\; \mathrm{Gal}(K/\mathbb{Q}_p) \qquad\qquad \text{(reciprocity law map)}$$

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

For *unramified extensions* $L \supset K \supset k$ of a local field k, we do have the commutative compatibility diagram

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

Remark: Again, the maps $\alpha_{K/k}$ are *Artin maps* or *reciprocity law maps.* It is typically not obvious how to recover classical reciprocity laws.

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

Proof: On one hand, certainly $k(\sqrt[n]{\alpha}) = k(\sqrt[n]{\alpha\beta^n})$.

In one direction, in $K = k(\sqrt[n]{a})$, any $g \in \mathrm{Gal}(K/k)$ sends $\alpha = \sqrt[n]{a}$ to another n^{th} root of a, which is $\omega_g \cdot \alpha$ for some n^{th} root of unity ω_g. The map $g \to \omega_g$ is a group homomorphism, and is injective because the effect of g is determined by its effect on α, so G is cyclic of order dividing n.

On another hand, let G be the Galois group of cyclic K over k, with order dividing n. Since k contains n^{th} roots of unity, the commuting k-linear endomorphisms of K given by G are *simultaneously diagonalizable.* Since this assertion is central to this proof of the theorem of Kummer theory, we give details.

To get an idea how to proceed, observe that the minimal polynomial $P(x) = \prod_\zeta (x - \zeta)$ of a generator g of G has roots n^{th} roots of unity. For each root ζ, with $Q_\zeta(x) = P(x)/(x - \zeta)$, $Q_\zeta(g)$ is not the 0 endomorphism of K, so there is $\alpha \in K$ such that $Q_\zeta(g)(\alpha) \neq 0$. Nevertheless, $(g - \zeta)Q_\zeta(g)(\alpha) = P(g)(\alpha) = 0$. Thus, $Q_\zeta(g)(\alpha)$ is a (non-zero) ζ-eigenvector for g.

Since $g^n = 1$, the minimal polynomial of g divides $x^n - 1$, which has no repeated roots when the characteristic does not divide n. Thus, g is *diagonalizable*, meaning that K is the direct sum of g's eigenspaces. Indeed, as ζ runs over roots of $P(x) = 0$, the quotients $Q_\zeta(x) = P(x)/(x - \zeta)$ have collective common factor 1. Thus, there are monic $R_\zeta(x) \in k[x]$ such that

$$1_{k[x]} = \sum_\zeta R_\zeta(x) \cdot Q_\zeta(x) \qquad \text{and} \qquad 1_K = \sum_\zeta R_\zeta(g) \cdot Q_\zeta(g)$$

Thus,

$$K \;=\; 1_K \cdot K \;=\; \bigoplus_\zeta \Big(R_\zeta(g) Q_\zeta(g)\Big)(K)$$

and the ζ^{th} summand is the ζ-eigenspace:

$$(g-\zeta)\cdot \big(R_\zeta(g)Q_\zeta(g)\big)(K) \;=\; R_\zeta(g)\Big((g-\zeta)Q_\zeta(g)(K)\Big) \;=\; R_\zeta(g)(0)$$

This proves the simultaneous diagonalizability of $\mathrm{Gal}(K/k)$ on K.

For g of order exactly m, with $m|n$, let ζ be a primitive m^{th} root of unity, and $v \in K$ a ζ-eigenvector. Then $g(v^m) = (gv)^m = (\zeta v)^m = v^m$, so v^m is in k, while v itself is fixed by no proper subgroup of G. By Galois theory $K = k(\sqrt[m]{v^m}) = k(\sqrt[n]{v^n})$. ///

Interaction of the various extensions of k by n^{th} roots:

Fix $2 \le \ell \in \mathbb{Z}$, 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 $\sigma(\alpha_i)/\alpha_i \neq \sigma(\alpha_j)/\alpha_j$.

Remark: 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.

That is, the hypothesis is that the one-dimensional representations of $\mathrm{Gal}(K/k)$ on the lines $k \cdot \alpha_j$ are pairwise non-isomorphic. This description of the situation correctly suggests the proof of

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

Bibliographic notes: Bibliographic pointers gleaned from [Dubuque 2011], e.g., [Bergstrom 1953]'s reference to [Hasse 1933].

[Robinson 2011] proves the quadratic case, and suggests extensions. Unsurprisingly, such questions were addressed decades ago. [Dubuque 2011] quotes reviews of sources dating to at least [Hasse 1933].

[Bergstrom 1953] H. Bergstrom, review of [Mordell 1953], Math. Reviews MR0058649.

[Besicovitch 1940] A.S. Besicovitch, *On the linear independence of fractional powers of integers*, J. Lond. Math. Soc. **15** (1940), 3-6.

[Dubuque 2011] W. Dubuque's answer to math.stackexchange.com/questions/30687, retrieved 22 Dec 2011.

[Hasse 1933] H. Hasse, *Klassenkorpertheorie*, Marburg (1933), 187-195.

[Mordell 1953] L.J. Mordell, *On the linear independence of algebraic numbers*, Pacific J. Math. **3** (1953), 625-630.

[Robinson 2011] G. Robinson's answer to math.stackexchange.com/questions/93453, retrieved 22 Dec 2011.

Proof: Let $\sum_j c_j \cdot \alpha_j = 0$ be a shortest non-trivial linear relation with $c_j \in k$. For indices $i \neq j$ appearing in this relation, take $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(\alpha_i)/\alpha_i \neq \sigma(\alpha_j)/\alpha_j$. Then

$$0 \;=\; \frac{\sigma(\alpha_i)}{\alpha_i} \cdot 0 - \sigma(0) \;=\; \frac{\sigma(\alpha_i)}{\alpha_i} \sum_t c_t \cdot \alpha_t - \sigma\Big(\sum_t c_t \cdot \alpha_t\Big)$$

$$= \sum_t c_t \cdot \alpha_t \cdot \big(\frac{\sigma(\alpha_i)}{\alpha_i} - \frac{\sigma(\alpha_t)}{\alpha_t}\big)$$

The coefficient of α_i is 0, while the coefficient of α_j is non-zero, by arrangement. This would contradict the assumption that the relation is shortest. Thus, there is no non-trivial relation. ///

Remark: The argument reproves the impossibility of mapping a sum of mutually non-isomorphic irreducibles of $\mathrm{Gal}(K/k)$ non-trivially to the trivial representation. The argument resembles the argument for *linear independence of characters*.

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 $0 \leq k \leq n$ 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.

Proof: The ratios $(a_{i_1} \ldots a_{i_k})/(a_{j_1} \ldots a_{j_\ell})$ have some prime appearing in the numerator or denominator, not both, and to first power, so is not a square, by unique factorization. ///

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*,

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

Proof: We really adjoin only n^{th} roots of *representatives* for $\Theta/(k^\times)^n$. Let K be the finite abelian extension obtained by adjoining all these roots. Given a, b in Θ but distinct mod $(k^\times)^n$, let $\alpha = \sqrt[n]{a}$ and $\beta = \sqrt[n]{b}$. Necessarily there is $g \in \mathrm{Gal}(K/k)$ such that $g\alpha/\alpha \neq g\beta/\beta$, or else α/β is fixed by $\mathrm{Gal}(K/k)$, and then $a/b = (\alpha/\beta)^n \in (k^\times)^n$, contradiction.

Thus, by the proposition, the n^{th} roots of representatives are linearly independent over k. This computes the degree of the field extension. ///

Remark: Reformulate to resemble classfield theory as closely as possible?