23. Cyclic extensions

Problem. *Given a field F, describe all finite Galois extensions K/F with $\mathrm{Gal}(K/F)$ cyclic.*

In this lecture we shall obtain a partial solution to this problem.

23.1. **Linear independence of characters.**

Definition. Let G be a group and L a field. A character of G with values in L is a group homomorphism $\chi : G \to L^*$

Lemma 23.1. *Let G be a group and L a field. Let $\chi_1, \ldots, \chi_n : G \to L^*$ be distinct characters of G with values in L. Then $\chi_1, \ldots, \chi_n$ are linearly independent over L (as functions), that is, if we are given $a_1, \ldots, a_n \in L$ s.t.*

$$\sum_{i=1}^{n} a_i \chi_i(g) = 0 \text{ for all } g \in G,$$

then each $a_i = 0$.

Proof. Suppose not, and let $l_1\chi_1 + \ldots + l_m\chi_m = 0$ be a linear dependence, with m minimal possible. Clearly, $m \geq 2$ and WOLOG $l_1 \neq 0$.

Fix $g \in G$ s.t. $\chi_m(g) \neq \chi_1(g)$. We have

$$l_1\chi_1(x) + \ldots + l_m\chi_m(x) = 0 \text{ for all } x \in G$$

$$l_1\chi_1(gx) + \ldots + l_m\chi_m(gx) = 0 \text{ for all } x \in G$$

Since each χ_i is multiplicative, the second equation can be rewritten as

$$l_1\chi_1(g)\chi_1(x) + \ldots + l_m\chi_m(g)\chi_m(x) = 0 \text{ for all } x \in G \qquad (***)$$

Multiplying the first equation by $\chi_m(g)$ on the left and subtracting from (***), we get

$$\sum_{i=1}^{m-1} l_i(\chi_i(g) - \chi_m(g))\chi_i(x) = 0 \text{ for all } x \in G.$$

Since $l_1(\chi_1(g)-\chi_m(g)) \neq 0$, we get a linear dependence between $\chi_1, \ldots, \chi_{m-1}$, which contradicts minimality of m. □

Corollary 23.2. *Let K and L be fields, and let $\sigma_1, \ldots, \sigma_n$ be distinct embeddings of K into L. Then $\sigma_1, \ldots, \sigma_n$ are linearly independent.*

Proof. Apply Lemma 23.1 with $G = K^*$. □

23.2. **Basic facts about norms in field extensions.** We recall from Homework#9 the definition of the norm of a field extension.

Definition. Let K/F be a finite separable extension. The norm function $N = N_{K/F} : K \to F$ is defined by

$$N_{K/F}(\alpha) = \prod_{\sigma \in Emb(K,\overline{F})} \sigma(\alpha).$$

The fact that the values of N lie in F is not obvious and was proved in the homework. Clearly, N is mulitplicative, that is,

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Remark: Suppose that K/F is Galois. Then

(1) $N(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$
(2) For any $\tau \in \mathrm{Gal}(K/F)$ we have $N(\tau\alpha) = N(\alpha)$. Indeed,

$$N(\tau\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma\tau(\alpha) = N(\alpha)$$

since if σ runs over all elements of $\mathrm{Gal}(K/F)$, then so does $\sigma\tau$.

Corollary 23.3. *If K/F is a finite Galois extension, then for each $\sigma \in \mathrm{Gal}(K/F)$ and $\alpha \in K^*$ we have $N(\frac{\sigma\alpha}{\alpha}) = 1$.*

Theorem 23.4 (Hilbert's Theorem 90)**.** *Let K/F be a finite Galois extension with $\mathrm{Gal}(K/F)$ cyclic and let σ be a generator of $\mathrm{Gal}(K/F)$. Then for any $\beta \in K$ with $N(\beta) = 1$ there exists $\alpha \in K$ s.t. $\beta = \frac{\sigma\alpha}{\alpha}$.*

Proof. Let $n = [K : F] = |\mathrm{Gal}(K/F)| = ord(\sigma)$. Define the function $\varphi : K \to K$ by

$$\varphi(x) = \frac{x}{\beta} + \frac{\sigma(x)}{\beta\sigma(\beta)} + \ldots + \frac{\sigma^{n-1}(x)}{\beta\sigma(\beta)\ldots\sigma^{n-1}(\beta)}.$$

Since $ord(\sigma) = n$, we know that $id, \sigma, \ldots, \sigma^{n-1}$ are distinct automorphisms of K, and thus also distinct embeddings from K to K. By Corollary 23.1 $\varphi \neq 0$ as a function. Choose $\theta \in K$ s.t. $\varphi(\theta) \neq 0$, and let $\alpha = \varphi(\theta)$. We claim that $\beta = \frac{\sigma(\alpha)}{\alpha}$, which is equivalent to showing that $\sigma(\alpha) = \beta\alpha$. Indeed,

$$\alpha = \frac{\theta}{\beta} + \frac{\sigma(\theta)}{\beta\sigma(\beta)} + \frac{\sigma^2(\theta)}{\beta\sigma(\beta)\sigma^2(\beta)} + \ldots + \frac{\sigma^{n-1}(\theta)}{\beta\sigma(\beta)\ldots\sigma^{n-1}(\beta)} \text{ and} \tag{23.1}$$

$$\sigma(\alpha) = \frac{\sigma(\theta)}{\sigma(\beta)} + \frac{\sigma^2(\theta)}{\sigma(\beta)\sigma^2(\beta)} + \ldots + \frac{\sigma^n(\theta)}{\sigma(\beta)\sigma^2(\beta)\ldots\sigma^n(\beta)} \tag{23.2}$$

Note that for $1 \leq i \leq n-1$ the i^{th} term on the RHS of (23.2) is equal to the $(i+1)^{\text{st}}$ term on the RHS of (23.1) multiplied by β. Finally, since $\sigma^n(\theta) = \theta$ and $\sigma(\beta)\sigma^2(\beta)\ldots\sigma^n(\beta) = N(\beta) = 1$, the last term on the RHS of (23.2) equals θ and thus equals the first term on the RHS of (23.1) multiplied by β. Thus, we showed that $\sigma(\alpha) = \beta\alpha$, as desired. $\square$

23.3. **Primitive roots of unity.**

Definition. Let F be a field and $n \in \mathbb{N}$. An element $\zeta \in F$ is called a primitive n^{th} root of unity if $\zeta^n = 1$ and $\zeta^m \neq 1$ for $0 < m < n$.

Example: (1) $\mathbb{C}$ contains primitive n^{th} root of unity for all n. The same is true for any algebraically closed field of characteristic zero.
(2) If $\operatorname{char} F = p > 0$, there is no primitive p^{th} root of unity in F since $\zeta^p = 1$ implies that $(\zeta - 1)^p = 0$, whence $\zeta = 1$.

More generally, we have the following:

Claim 23.5. *If F is a field and $n \in \mathbb{N}$, then the following are equivalent:*

(i) *Some finite extension of F contains primitive n^{th} root of unity*
(ii) $\operatorname{char} F$ *does not divide n.*

23.4. **Cyclic Galois extensions in the presence of roots of unity.**

Theorem 23.6 (Kummer)**.** *Let F be a field, $n \in \mathbb{N}$ and suppose that F contains primitive n^{th} root of unity. The following hold:*

(a) *Let K/F be a Galois extension with $\operatorname{Gal}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$. Then $K = F(\sqrt[n]{a})$ for some $a \in F$. More precisely, $K = F(\alpha)$ for some $\alpha \in K$ s.t. $\alpha^n \in F$.*
(b) *Conversely, suppose that $K = F(\sqrt[n]{a})$ for some $a \in F$. Then K/F is Galois and $\operatorname{Gal}(K/F) \cong \mathbb{Z}/d\mathbb{Z}$ for some $d \mid n$.*

Remark: If F does not contain primitive n^{th} root of unity, an extension of the form $F(\sqrt[n]{a})/F$ need not even be Galois.

Proof. (a) Let $\zeta \in F$ be primitive n^{th} root of unity, let $N : K \to F$ be the norm function and let σ be a generator of $\operatorname{Gal}(K/F)$. Since $\zeta \in F$, we have $N(\zeta) = \zeta^n = 1$, so by Hilbert's Theorem 90 there exists $\alpha \in K$ s.t. $\zeta = \frac{\sigma(\alpha)}{\alpha}$.

So, $\sigma(\alpha) = \zeta\alpha$, whence $\sigma^i(\alpha) = \zeta^i\alpha$ for $0 \leq i \leq n-1$. Hence the orbit of α under the action of $\operatorname{Gal}(K/F)$ contains n distinct elements. Therefore, $\deg_F(\alpha) \geq n = [K : F]$, and we must have $K = F(\alpha)$.

It remains to show that $\alpha^n \in F$. We have $\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n\alpha^n = \alpha^n$. Thus, α^n is fixed by σ, whence fixed by the entire Galois group $\operatorname{Gal}(K/F)$. Therefore, by Proposition 21.1 $\alpha^n \in F$.

(b) We are given that $K = F(\alpha)$ s.t. $a := \alpha^n \in F$. First note that K is a splitting field over F for $x^n - a = x^n - \alpha^n = \prod_{i=1}^n (x - \zeta^i\alpha)$ since $\zeta \in F$. Hence K/F is Galois.

Any $\sigma \in \mathrm{Gal}(K/F)$ must send α to a root of $x^n - a$, so $\sigma(\alpha) = \zeta^{I(\sigma)}\alpha$ for some integer $I(\sigma)$ which is well defined mod n. Thus, we get a map $I : \mathrm{Gal}(K/F) \to \mathbb{Z}/n\mathbb{Z}$. It is straightforward to check that I is a homomorphism, and also I is injective as σ is completely determined by where it sends α. Therefore, $\mathrm{Gal}(K/F)$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$, so $\mathrm{Gal}(K/F) \cong \mathbb{Z}/d\mathbb{Z}$ for some $d \mid n$. □