Abelian Kummer Theory

M. J. Narlikar

In this article, we study abelian extensions of exponent m when the underlying field k has characteristic coprime to m and it contains all the m-th roots of unity. When the field k has characteristic $p > 0$, we shall also discuss the abelian extensions of k of exponent p.

§1. Independence of Group Characters

Let G be a group. A character ψ of G in a field K is a homomorphism $\psi : G \to K^*$, where K^* is the set of all nonzero elements of the field K. Let μ_m be the group of m^{th} roots of unity in K.

Examples (1) $f : \mathbf{R}/\mathbf{Z} \to \mathbf{C}^*$ given by $f(x) = e^{2\pi imx}$ for some fixed integer m where $\mathbf{R}$ (resp. $\mathbf{C}$) is the field of real (resp. complex) numbers and $\mathbf{Z}$ is the ring of rational integers.
(2) For a cyclic group $G =< a >$ of order n, the character $f : G \to \mu_n$ given by $f(a) = \alpha$, for some α in μ_n.

Theorem 1.1 (Artin) Let $\psi_1, \psi_2, \cdots, \psi_n$ be distinct group characters of G in K. Then they are linearly independent over K.

Proof : Suppose $\psi_1, \psi_2, \cdots, \psi_n$ are linearly dependent over K. Then there are $a_1, \cdots, a_n$ in K, not all 0, such that $a_1\psi_1 + a_2\psi_2 + \cdots + a_n\psi_n = 0$. Without loss of generality, assume that n is the smallest natural number with all a_i's non-zero.

Since ψ_1, ψ_2 are distinct characters, there is a z in G such that $\psi_1(z) \neq \psi_2(z)$. Also, $a_1\psi_1(zx) + a_2\psi_2(zx) + \cdots + a_n\psi_n(zx) = 0$, for all $x \in G$. Hence, $a_1\psi_1(x) + a_2\frac{\psi_2(z)}{\psi_1(z)}\psi_2(x) + \cdots + a_n\frac{\psi_n(z)}{\psi_1(z)}\psi_n(x) = 0$, for any x in G.

Thus, together with $a_1\psi_1(x) + a_2\psi_2(x) + \cdots + a_n\psi_n(x) = 0$, we arrive at

$$[a_2 - a_2\frac{\psi_2(z)}{\psi_1(z)}]\psi_2(x) + [a_3 - a_3\frac{\psi_3(z)}{\psi_1(z)}]\psi_3(x) + \cdots [a_n - a_n\frac{\psi_n(z)}{\psi_1(z)}]\psi_n(x) = 0,$$

for any x in G, which contradicts the minimality of n.

Theorem 1.2 (Hilbert's theorem 90) : If K/k is a cyclic extension of degree n with its Galois group $G =< \sigma >$, then for $\beta \in K$, $N(\beta) = 1 \Leftrightarrow \exists\ \alpha$ in K such that $\beta = \alpha/\sigma\alpha$. In other words, the kernel of the norm map from K^* to K^* consists of elements of the form $\alpha/\sigma\alpha, \alpha \in K$.

Proof : The implication ($\Leftarrow$) is obvious.

We shall prove the other implication. Let $N(\beta) = 1$, for $\beta \in K$. Consider the homomorphisms $\sigma, \sigma^2, \cdots, \sigma^n = \text{ id }$ of K^* into itself and apply the theorem of independence of characters (Theorem 1.1) to deduce that

$$\text{id } + \beta\sigma + \beta^{1+\sigma}\sigma^2 + \cdots + \beta^{1+\sigma+\cdots+\sigma^{n-2}}\sigma^{n-1}$$

is not identically zero. Here $\beta^\sigma = \sigma(\beta), \beta^{\sigma^2} = \sigma^2(\beta)$, etc.. Hence, there is θ in K such that

$$\alpha = \theta + \beta\theta^\sigma + \beta^{1+\sigma}\theta^{\sigma^2} + \cdots + \beta^{1+\sigma+\cdots\sigma^{n-2}}\theta^{\sigma^{n-1}} \neq 0.$$

Therefore, $\beta\alpha^\sigma = \alpha$, and hence, $\beta = \dfrac{\alpha}{\sigma(\alpha)}$.

Theorem 1.3 (Hilbert's theorem 90 in additive form). If K/k is a cyclic extension of degree n with its Galois group $G = \ < \sigma >$, then for $\beta \in K$, $\text{Tr}(\beta) = 0 \Leftrightarrow \exists\ \alpha$ in K such that $\beta = \alpha - \sigma\alpha$. In other words, the kernel of the trace map from K to K consists of elements of the form $\alpha - \sigma\alpha,\ \alpha \in K$.

Proof : The implication ($\Leftarrow$) is obvious.

For the other implication, we take $\beta \in K$ with $\text{Tr}(\beta) = 0$. By applying the theorem of independence of characters, we have θ in K such that $\text{Tr}(\theta) \neq 0$. Let

$$\alpha = \frac{1}{\text{Tr}(\theta)}\left\{\beta\theta^\sigma + (\beta + \beta^\sigma)\theta^{\sigma^2} + \cdots + (\beta + \beta^\sigma + \cdots + \beta^{\sigma^{n-2}})\theta^{\sigma^{n-1}}\right\}.$$

Then $\beta = \alpha - \sigma\alpha$.

§2. Cyclic Extensions

Theorem 2.1 Let k be a field and n an integer > 0, prime to the characteristic of k and assume that the n^{th} roots of unity are in k.
(i) Let K/k be a cyclic extension of degree n. Then there is α in K such that $K = k(\alpha)$ and α is a root of $X^n - a = 0$, for some a in k.
(ii) Conversely if $a \in k$ and α is a root of $X^n - a$, then $k(\alpha)$ is a cyclic extension of k of degree d where $d \mid n$ and α^d is in k.

Proof : (i) Let ζ be a primitive n^{th} root of unity in k and K/k be cyclic of order n. We know that $N(\zeta^{-1}) = \zeta^{-n} = 1$. Hence by Hilbert's theorem 90, there is α in K such that $\sigma\alpha = \zeta\alpha$. Then $\sigma^2\alpha = \zeta^2\alpha$ and so on. Also $\alpha, \sigma\alpha, \cdots, \sigma^{n-1}\alpha$ are all distinct. Hence, $[k(\alpha) : k] \geq n$. Since $\alpha \in K$, we get $k(\alpha) = K$. Also, $\sigma(\alpha^n) = \zeta^n\alpha^n = \alpha^n$. Thus, $\alpha^n \in k$ and we take $a = \alpha^n$.

(ii) If $a \in k$ and α is a root of $X^n - a$, then $\alpha\zeta^j$ is a root for each j and all the roots of $X^n - a$ are in $k(\alpha)$. Hence, $k(\alpha) = K$ is a cyclic extension of degree d which divides n.

If σ is an automorphism of K, then $\sigma\alpha = \omega_\sigma\alpha$, where ω_σ is an n^{th} root of unity. If ω_σ is not a primitive n^{th} root of unity, then $\omega : G \to \mu_n$ is injective, not surjective and G is isomorphic to a subgroup (cyclic) of μ_n.

Theorem 2.2 Let k be a field of characteristic p.
(i) Let K/k be a cyclic extension of degree p. Then there is α in K such that $K = k(\alpha)$ and α is a root of $X^p - X - a = 0$, for some a in k.
(ii) Conversely, for $a \in k$, if the polynomial $f(X) = X^p - X - a$ has a root in k then all the roots are in k; or else it is irreducible. In the latter case, $k(\alpha)$ is cyclic of degree p over k.

Proof : (i) Let K/k be cyclic of degree p. We know that $\mathrm{Tr}_k^K(-1) = 0$. Hence, by Hilbert's theorem 90, there is α in K such that $-1 = \alpha - \sigma\alpha$, that is, $\sigma\alpha = \alpha + 1$. Hence, $\sigma^j\alpha = \alpha + j$ and all $\sigma\alpha, \sigma^2\alpha, \cdots, \sigma^n\alpha$ are distinct. Thus $K = k(\alpha)$. Now, $\sigma(\alpha^p - \alpha) = (\sigma\alpha)^p - (\sigma\alpha) = (\alpha+1)^p - (\alpha+1) = \alpha^p - \alpha$. Hence, $\alpha^p - \alpha \in k$.

(ii) If α is a root of f, then $\alpha + j$ is a root for $1 \leq j \leq p$. Hence, the first part of (ii). Assume that there is no root in k. Then f is irreducible. Otherwise, $f(X) = g(X)h(X)$ where g and h have degrees strictly less than p. Since $f(X) = \prod_{j=1}^{p}(X - \alpha - j)$ for any root α, $g(X)$ is a product of some $(X - \alpha - j)$. Let $d = \deg g$. The coefficient of X^{d-1} is the sum of terms $-(\alpha + j)$ over d of the integers. Hence it is $-d\alpha + m$ for some integer m. Hence $d\alpha \in k$, and as $d \neq 0, \alpha \in k$. Contradiction.

Since $f(X)$ has no multiple roots, $k(\alpha)$ is Galois and moreover cyclic with $\sigma : \alpha \to \alpha + 1$ as a generator of the Galois group.

§3. The Duality Theorem

Let A be an abelian group of exponent m (i.e. $a^m = 1$ for any $a \in A$). For the cyclic group $\mathbf{Z}_m$ of order m, let $\hat{A} = \mathrm{Hom}(A, \mathbf{Z}_m)$. Then $\hat{A}$ is called the dual of A. If $f : A \to B$ is a homomorphism between two groups of exponent m, then we have a natural homomorphism $\hat{f} : \hat{B} \to \hat{A}$ such that $\widehat{(f \circ g)} = \hat{g} \circ \hat{f}$.

Theorem 3.1 If A is a finite abelian group and it is a direct product $A = B \times C$, then $\hat{A} \cong \hat{B} \times \hat{C}$. Any finite abelian group is isomorphic to its own dual.

Proof : We have

$$B \xleftarrow{f} B \times C \xrightarrow{g} C$$

where f (leftarrow) and g (rightarrow) are the projections onto the first and the second components. Then $\psi_1 \in \hat{B}$ and $\psi_2 \in \hat{C}$ generate (ψ_1, ψ_2) in $\widehat{(B \times C)}$ by

$$(\psi_1, \psi_2)(x, y) = \psi_1(x) + \psi_2(y).$$

Thus

$$\widehat{(f, g)} : \hat{B} \times \hat{C} \to \widehat{(B \times C)}$$

is a map which has inverse $\phi \to (\phi_1, \phi_2)$ as

$$\phi(x, y) = \phi_1(x, e) + \phi_2(e, y),$$

where e is the identity element.

We know that any finite abelian group is a direct product of cyclic groups. Hence it is enough to show that a cyclic group is isomorphic to its own dual.

Let $A = \ < a >$ be of order n. Then any $f \in \hat{A}$ is determined by $f(a)$ and $f(a)$ can take precisely n different values. Let $t \in \mathbf{Z}_n$ be a primitive element in $\mathbf{Z}_n$. Then ψ defined by $\psi(a) = t$ is seen to generate $\hat{A} =< \psi >$. Thus, the result follows.

If C, A and A' are abelian groups, then a map $F : A \times A' \to C$ is called bilinear if $F(a, a')$ is linear in each component, i.e., $F(a_1 a_2, a') = F(a_1, a') + F(a_2, a')$ (the group operation on C is written additively) and $F(a, a'_1 a'_2) = F(a, a'_1) + F(a, a'_2)$. The kernel of F on the right is $\{x' \in A' \mid F(a, x') = 0 \ \forall \ a \in A\}$ and the kernel of F on the left is $\{x \in A \mid F(x, a') = 0, \ \forall \ a' \in A\}$.

There are natural injections

$$0 \to A'/B' \to \mathrm{Hom}(A/B, C) \quad \cdots \quad I$$

and

$$0 \to A/B \to \mathrm{Hom}(A'/B', C) \quad \cdots \quad II,$$

where B' is the kernel on the right and B is the kernel on the left. If C is cyclic of order m, then A'/B' and A/B have exponent m.

Theorem 3.2 Let $F : A \times A' \to C$, be a bilinear map of two abelian groups A and A' into a cyclic group C. With the same notation as above, A'/B' is finite if and only if A/B is finite and in that case, $A'/B' \cong \widehat{(A/B)}$.

Proof : The sequences I and II give the result immediately. We have to note that A/B is finite implies that Hom $(A/B, C)$ and hence A'/B' are finite. The last part follows from the Theorem 3.1 above.

§4. Abelian Extensions

Theorem 4.1 Let k be a field and $m > 0$ an integer coprime to the characteristic of k and assume that all the m^{th} roots of unity are in k. Let B be a subgroup of k^* such that $k^{*m} \subset B$ and let $K_B = k(B^{1/m})$. Then K_B is Galois and abelian of exponent m. Let $G = \mathrm{Gal}(K_B/k)$.

Then we have a bilinear map $< \ , \ >: G \times B \to \mu_m$ as described below: $\sigma \in G, \ a \in B$ and $\alpha^m = a \Rightarrow \ < \sigma, a > \ = \sigma\alpha/\alpha$. The kernel on the left is 1 and the kernel on the right is k^{*m}.

The extension K_B/k is finite if and only if $[B : k^{*m}]$ is finite. In that case,

$$B/k^{*m} \cong \hat{G} = \mathrm{Hom}(G, \mu_m).$$

In particular, $[K_B : k] = [B : k^{*m}]$.

Proof : We have K_B Galois as $X^m - a$ splits completely in K_B for each $a \in B$. It can be checked that $< \sigma, a >= \sigma\alpha/\alpha$ is independent of the m-th root α of a, and the properties mentioned above are easily verified. Now, in the case of the kernel on the right, if $< \sigma, a > \ = 1$ for all σ in G, consider the field $k(a^{1/m})$. If $a^{1/m}$ is not in k, then there is an automorphism τ of $k(a^{1/m})$ over k which is not identity and it has an extension to K_B. Call the extension $\bar{\tau}$. Check that $< \bar{\tau}, a > \neq 1$.

In the duality theorem, let $A = G, \ A' = B$. Then we get, the injections

$$0 \to G \to \mathrm{Hom}(B/k^{*m}, \mu_m) \text{ and } \ 0 \to B/k^{*m} \to \mathrm{Hom}(G, \mu_m).$$

Thus the result follows.

Theorem 4.2 In the notation of Theorem 4.1, the map $B \to K_B$ gives a bijection of the subgroups of k^* containing k^{*m} and the abelian extensions of k of exponent m.

Proof : Let B_1, B_2 be subgroups of k^* as above and $B_1 \subset B_2$. Then $B_1^{1/m} \subset B_2^{1/m}$ so that $K_{B_1} \subset K_{B_2}$. Conversely, if $K_{B_1} \subset K_{B_2}$, then let $b \in B_1$, we shall prove that $b \in B_2$. Since $k(b^{1/m}) \subset k(B_2^{1/m})$ and $b^{1/m}$ is in some finitely generated subextension of K_{B_2}, we may assume that B_2/k^{*m} is finitely generated. Let $B_3 = \ < B_2, b >$. Then $k(B_2^{1/m}) = k(B_3^{1/m})$ and from Theorem 4.1 above, $[K_{B_2} : k] = [B_2 : k^{*m}] = [K_{B_3} : k] = [B_3 : k^{*m}]$. Hence, $B_2 = B_3$.

Now, if K is an abelian extension of k of exponent m, we have $\sigma^m = 1$ for any σ in G. Any finite subextenstion is a compositum of cyclic extensions. By Theorem 2.1, each cyclic extension of exponent m is obtained by adjoining an m-th root. Hence, K is obtained by adjoining a family of m^{th} roots of

$\{b_j\}_{j\in J}, b_j \in k^*$. If B is the subgroup of k^* generated by $\{b_j\}$ and k^{*m}, then $k(B^{1/m}) = K_B = K$. If $b' = ba^m$, for $a, b \in k$, then $k(b'^{1/m}) = k(b^{1/m})$.

If k has characteristic p and the operator P on k is defined as $P(x) = x^p - x$, then P is an additive homomorphism of k into itself. $P(k)$ now plays the role of k^{*m} in the last theorem. A root of the polynomial $x^p - x - a$ for $a \in k$ will be denoted by $P^{-1}(a)$. If B is an additive subgroup of k which contains $P(k)$, let $K_B = k(P^{-1}(B))$ be the field obtained by adjoining $P^{-1}(a)$ to k for all a in B.

Theorem 4.3 Let k be a field of characteristic p. The map $B \to k(P^{-1}(B))$ is a bijection between subgroups of k containing $P(k)$ and abelian extensions of k of exponent p. Let $K = K_B = k(P^{-1}(B))$ and G be its Galois group. For $\sigma \in G$ and $b \in B$, let $< \sigma, a > \; = \sigma\alpha - \alpha$ with $P(\alpha) = a$. Then, there is a bilinear map $C \times B \to \mathbf{Z}/p\mathbf{Z}$ given by $< \sigma, a > \; = \sigma\alpha - \alpha$, and its kernel on the left is 1 and the kernel on the right is $P(k)$. The extension K_B/k is finite if and only if $[B : P(k)]$ is finite and in that case $[K_B : k] = [B : P(k)]$.

Proof : Very similar to that of Theorem 4.2 above. We need to use Theorem 2.2 above and note $< \sigma, a >$ is a rational integer. Also, $\sigma\alpha - \alpha = 0$, for all α with $\alpha^p - \alpha = a$, implies $\alpha \in k$ and $a \in P(k)$.

REFERENCE

1. Serge Lang, *Algebra*, (Ch. VI), 3rd Ed. (Addison-Wesley), 1994.

M. J. Narlikar
1, Akashganga, IUCAA Housing
Ganeshkhind, Pune - 411007, India