Lecture 20 : Cyclic Extensions and Solvable Groups

Objectives

(1) Cyclic extensions of degree p over fields with characteristics p.

(2) Solvable groups.

(3) Simplicity of S_n and A_n.

Keywords and phrases : Cyclic extensions, solvable groups, commutator, simple groups.

Structure of cyclic Galois extensions over fields of characteristic p

Let F be a field of positive characteristic p. We discuss the structure of Galois extensions of F of degree p. Consider the map $\delta : F \to F$ defined by $\delta(a) = a^p - a$. Then δ is a homomorphism of the additive group F. Moreover $\mathbb{F}_p =$ Ker δ. Note that $\delta^{-1}(a) = \{a + i \mid i = 0, 1, \ldots, p-1\}$.

Theorem 20.1 (**Artin-Schreier**). (1) *Let E/F be a cyclic Galois extension of degree p where char $F = p$, a prime number. Then $E = F(a)$ where a is a root of $x^p - x - b$ for some $b \in F$.*

(2) *Suppose that $a \notin F^p - F$. Then $f(x) = x^p - x - a$ is irreducible over F and a splitting field of $f(x)$ over F is cyclic of degree p.*

Proof. (1) Let $G = G(E/F) = (\sigma)$ and let $T : E \to E$ be the linear map of the F-vector space E defined by $T(a) = \sigma(a) - a$. Then

$$\text{Ker } T = \{a \in E \mid \sigma(a) = a\} = F.$$

Since $T^p = (\sigma - id)^p = \sigma^p - id = 0$, we have Im $(T^{p-1}) \subset$ Ker $T = F$. If $T^{p-1} = 0$ then there is a nontrivial F-linear relation among $\sigma^{p-1}, \sigma^{p-2}, \ldots, \sigma, id$. This contradicts Dedekind's theorem. Hence Im $T^{p-1} =$ Ker $T = F$. Let $b \in E$ so that $T^{p-1}(b) = 1$. Set $\alpha = T^{p-2}(b)$. Then $T(\alpha) = \sigma(\alpha) - \alpha = 1$. Hence $\sigma(\alpha) = \alpha + 1$. Thus $\sigma^i(\alpha) = \alpha + i$ for all $i = 1, 2, \ldots, p-1$. Therefore $E = F(\alpha)$.

Since $\sigma(\alpha^p - \alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$, The element $a = \alpha^p - \alpha \in E^G = F$. Hence α is a root of $x^p - x - a$.

(2) Conversely, suppose that $a \notin F^p - F$. Then we show that $f(x) = x^p - x - a$ is irreducible over F. If α is a root of $f(x)$ then $\alpha + i$ is a root of $f(x)$ for all $i = 1, 2, \ldots, p-1$. Hence $E = F(\alpha)$ is a splitting field of $f(x)$. If we assume that $f(x)$ is irreducible over F then $[E : F] = p$ and the Galois group is generated by the automorphims $\sigma(\alpha) = \alpha + 1$.

Suppose that $f(x) = g_1(x)g_2(x)\ldots g_n(x)$ where each g_i is irreducible over F. If β is a root of g_i then $E = F(\beta)$ as shown above. Hence each $g_i(x)$ has same degree r and so $\deg f(x) = p = rn$. Thus $r = p$ and $n = 1$. Hence $f(x)$ is irreducible over F.

□

Solvable groups

Definition 20.2. *Let G be a group. A sequence of subgroups*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{s+1} = 1 \tag{1}$$

is called a **normal series** *for G if G_i is a normal subgroup of G_{i-1} for $i = 1, 2, \ldots, s$. The normal series* (1) *is called* **abelian** (**resp. cyclic**) *if the quotients G_i/G_{i+1} are abelian* (*resp. cyclic*) *for $i = 0, 1, \ldots s$. A group having an abelian series is called a* **solvable group**.

Example 20.3. (1) Any abelian group is solvable.
(2) The group S_3 is solvable since $S_3 \supset A_3 \supset 1$ is an abelian series.
(4) The group S_4 is solvable since

$$S_4 \supset A_4 \supset V_4 \supset 1$$

is an abelian series where $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$.

Proposition 20.4. *Any group G of order p^n where p is a prime number is solvable.*

Proof. Apply induction on n. If $n = 1$ then G is cyclic and hence solvable. Let $n \geq 2$. Let C be the center of G. We know that $o(C) > 1$. Hence $o(G/C) < o(G)$. By induction, we have an abelian series

$$G/C \supset G_1/C \supset G_2/C \supset \cdots \supset G_s/C = 1$$

Since $(G_i/C)/(G_{i+1}/C) \simeq G_i/G_{i+1}$ for all i, we have an abelian series:

$$G \supset G_1 \supset G_2 \supset \cdots \supset G_s \supset C \supset 1.$$

Thus G is solvable.

□

Definition 20.5. *Let G be a group. The* **commutator** *$[g,h]$ of $g,h \in G$ is defined as $[g,h] = g^{-1}h^{-1}gh$. The* **derived subgroup** *of G denoted by G' is the subgroup generated by all the commutators in G. The k^{th}* **derived subgroup** *of G is defined inductively as $G^{(k)} = (G^{(k-1)})'$.*

Proposition 20.6. *Let $f : G \to H$ be a homomorphism of groups.*
(1) *$f(G') \subseteq H'$. If f is onto then $f(G') = H'$.*
(2) *If $K \lhd G$ then $K' \lhd G$. In particular $G' \lhd G$.*
(3) *If $K \lhd G$ then G/K is abelian if and only if $G' \subseteq K$.*

Proof. (1). Let $g,h \in G$. Then $f([g,h]) = f(g)^{-1}f(h)^{-1}f(g)f(h) = [f(g), f(h)]$. Hence $f(G') \subseteq H'$. It is clear that equality holds true if f is onto.
(2) Let $a \in G$. The inner automorphism $i_a : G \to G$ restricts to an automorphism of K as $K \lhd G$. Hence $i_a(K') = K'$. Therefore $K' \lhd G$. Since $G \lhd G$, we have $G' \lhd G$.
(3) Let $K \lhd G$. Then G/K is abelian $\Leftrightarrow$ for all $g,h \in G$, $ghK = hgK \Leftrightarrow$ $h^{-1}g^{-1}hg \in K$ for all $g,h \in G \Leftrightarrow G' \subseteq K$. □

Proposition 20.7. *A group G is solvable if and only if $G^{(s)} = 1$ for some $s \in \mathbb{N}$.*

Proof. Let G be solvable. Then there is an abelian series for G

$$1 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_s = G.$$

We show by induction on s that $G^{(s)} = 1$. If $s = 1$, then G is abelian. Hence $[g,h] = 1$ for all $g,h \in G$. Hence $G' = 1$. Now let $s > 1$. Then

$$1 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{s-1}$$

is an abelian series for G_{s-1}. Hence $G_{s-1}^{(s-1)} = 1$. Since G/G_{s-1} is abelian, $G' \subseteq G_{s-1}$. Hence

$$G^{(s)} = (G')^{(s-1)} \subseteq G_{s-1}^{(s-1)} = 1.$$

Conversely suppose that $G^{(s)} = 1$ for some s. Then

$$G \rhd G^{(1)} \rhd G^{(2)} \rhd \cdots \rhd G^{(s)} = 1$$

is an abelian series for G. Thus G is solvable. □

Proposition 20.8. *Let G be a group and H be a subgroup.*
(1) *If G is solvable then so is H.*
(2) *If $f : G \to H$ is a surjective group homomorphism and G is solvable then H is so.*
(3) *If $K \lhd G$ and G/K are solvable then G is solvable.*

Proof. (1) If G is solvable then $G^{(s)} = 1$ for some s. Since $H^{(s)} \subset G^{(s)} = 1$, we have $H^{(s)} = 1$. Thus H is solvable.
(2) Let $G^{(s)} = 1$. Since f is surjective, $f(G^{(s)}) = H^{(s)} = 1$. Hence H is solvable.
(3) Let $K \lhd G$ and K and G/K be solvable. Then there exist s and t such that $K^{(s)} = 1$ and $(G/K)^{(t)} = 1$. Hence $G^{(t)} \subset K$. Thus $G^{(t+s)} \subset K^{(s)} = 1$. Hence G is solvable.

□

Lemma 20.9. *The group A_n is generated by 3-cycles. If $n \geq 5$ then all 3-cycles are conjugates in A_n.*

Proof. Let σ be an even permutation. Let $(ij)(rs)$ occur in a decomposition of σ as a product of transpositions. If (ij) and (rs) are disjoint then $(ij)(rs) = (ijr)(rsj)$. If $j = r$ then $(ir)(rs) = (irs)$. Hence every even permutation is a product of 3-cycles. Now suppose that $n \geq 5$. Let σ be any permutation and $(j_1 j_2 \dots j_p)$ be a p-cycle. Then

$$\sigma(j_1 j_2 \dots j_p)\sigma^{-1} = (\sigma(j_1)\sigma(j_2)\dots\sigma(j_p)).$$

Let (ijk) and (rst) be any two 3-cycles. Define γ by $\gamma(i) = r, \gamma(j) = s, \gamma(k) = t$ and let $\gamma(u) = u$ for any $u \neq i, j, k$. Then

$$\gamma(ijk)\gamma^{-1} = (\gamma(i)\gamma(j)\gamma(k)) = (rst).$$

If γ is odd then put $\sigma = (ij)\gamma$. Then σ is even and

$$\sigma(ijk)\sigma^{-1} = (ij)\gamma(ijk)\gamma^{-1}(ij) = (rst).$$

□

Theorem 20.10. *The groups S_n and A_n are not solvable for $n \geq 5$.*

Proof. Since S_n/A_n is abelian, $S_n' \subset A_n$. Note that since $n \geq 5$, any 3-cycle is a commutator in view of :

$$[(jkv),(ikr)] = (vkj)(rki)(jkv)(ikr) = (vkj)(jiv) = (ikj).$$

Therefore $S_n' = A_n' = A_n$. Thus $S_n^{(s)} = A_n^{(s)} = A_n$ for all s. Hence A_n and S_n are not solvable for $n \geq 5$. □

Theorem 20.11 (Galois). *The alternating group A_n is simple for $n \geq 5$.*

Proof. (S. Lang) Suppose A_n is not simple for $n \geq 5$. Let N be a proper normal subgroup of A_n for some $n \geq 5$. Let $\sigma \neq 1$ be a permutation in N that has maximum number of fixed points. We say that j is a fixed point of σ if $\sigma(j) = j$. Consider a decomposition of σ as a product of disjoint cycles of length at least two: $\sigma = \tau_1\tau_2 \dots \tau_g$. Suppose the length of each τ_j is two. Since σ is an even permutation, $g \geq 2$. Suppose that $\sigma = (ij)(rs)\tau_3 \dots \tau_g$. Let k be different from i, j, r, s and set $\tau = (rsk)$. Consider the commutator $\gamma = [\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau$. Then $1 \neq \gamma \in N$. Moreover $\gamma(i) = i$ and $\gamma(j) = j$. This is a contradiction since σ has maximum number of fixed points among the permutations in $N \setminus \{1\}$.

Now suppose that for some a, $\tau_a = (ijk...)$ has length at least 3. If $\sigma = (ijk)$ then N has a 3-cycle and hence $N = A_n$. If σ is not a 3-cycle then σ must move at least two other elements r, s besides i, j, k. Put $\tau = (rsk)$ and consider $\gamma = [\sigma, \tau]$. Then $1 \neq \gamma \in N$. Moreover $\gamma(j) = j$ and γ fixes all the elements that σ fixes. This is a contradiction. □