School of Mathematics and Statistics

MT5836 Galois Theory

Handout VII: Solution of Equations by Radicals

7 Solution of Equations by Radicals

Radical extensions

Definition 7.1 (i) An extension K of a field F is said to be a *simple radical extension* if $K = F(\alpha)$ for some element $\alpha \in K$ satisfying $\alpha^p \in F$ for some prime number p.

(ii) An extension K of a field F is called a *radical extension* if there is a sequence of intermediate fields
$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$$
such that K_i is a simple radical extension of K_{i-1} for $i = 1, 2, \dots, n$.

Lemma 7.2 *Suppose $K = F(\alpha)$ where $\alpha^m \in F$ for some positive integer $m > 1$. Then K is a radical extension of F.*

Lemma 7.3 *Any radical extension is a finite extension.*

Definition 7.4 Let $f(X)$ be a polynomial over a field F of characteristic zero. We say that $f(X)$ is *soluble by radicals* if there exists a radical extension of F over which $f(X)$ splits.

Thus, $f(X)$ is soluble by radicals when the splitting field K of $f(X)$ over F is contained in some radical extension L of F. Then every root is some element of L and so can be expressed as a formula involving repeated use of field operations and pth roots (for a variety of prime numbers p).

Lemma 7.5 *Let K be a radical extension of a field F of characteristic zero. Then there exists an extension L of K such that L is a normal radical extension of F.*

Soluble groups and other group theory

Definition 7.6 A group G is called *soluble* (*solvable* in the U.S.) if there are subgroups

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \ldots \geqslant G_d = \mathbf{1} \tag{1}$$

such that, for each $i = 1, 2, \ldots, d$, the subgroup G_i is normal in G_{i-1} and the quotient group G_{i-1}/G_i is abelian.

Basic Observations:

- An abelian group is soluble.
- A non-abelian simple group is not soluble.

Proposition 7.7 (i) *If G is soluble, then every subgroup of G is soluble.*

(ii) *If G is soluble, then every quotient group of G is soluble.*

(iii) *If N is a normal subgroup of G such that G/N and N are both soluble, then G is soluble.*

Proposition 7.8 *Let G be a finite soluble group. Then G has a chain of subgroups*

$$G = H_0 > H_1 > H_2 > \cdots > H_n = \mathbf{1}$$

such that, for $i = 1, 2, \ldots, n$, H_i is a normal subgroup of H_{i-1} and H_{i-1}/H_i is cyclic of prime order.

Theorem 7.9 (Cauchy's Theorem) *Let G be a finite group and p be a prime number that divides the order of G. Then G contains an element of order p.*

Examples of polynomials with abelian Galois groups

Lemma 7.10 *Let F be a field of characteristic zero and let K be the splitting field of $X^p - 1$ over F, where p is a prime number. Then the Galois group $\mathrm{Gal}(K/F)$ is abelian.*

Lemma 7.11 *Let F be a field of characteristic zero in which $X^n - 1$ splits. Let $\lambda \in F$ and let K be the splitting field for $X^n - \lambda$ over F. Then the Galois group $\mathrm{Gal}(K/F)$ is abelian.*

Galois groups of normal radical extensions

Theorem 7.12 *Let F be a field of characteristic zero and K be a normal radical extension of F. Then the Galois group $\mathrm{Gal}(K/F)$ is soluble.*

Corollary 7.13 (Galois) *Let $f(X)$ be a polynomial over a field F of characteristic zero. If $f(X)$ is soluble by radicals then the Galois group of $f(X)$ over F is soluble.*

A polynomial which is insoluble by radicals

Lemma 7.14 *Let p be a prime and $f(X)$ be an irreducible polynomial of degree p over $\mathbb{Q}$. Suppose that $f(X)$ has precisely two non-real roots in $\mathbb{C}$. Then the Galois group of $f(X)$ over $\mathbb{Q}$ is isomorphic to the symmetric group S_p.*

Example 7.15 The quintic polynomial $f(X) = X^5 - 9X + 3$ over $\mathbb{Q}$ is not soluble by radicals.

Galois's Great Theorem

Lemma 7.16 *Let K be a finite normal extension of a field F of characteristic zero and suppose that $X^p - 1$ splits in F (for some prime p). If $\mathrm{Gal}(K/F)$ is cyclic of order p then $K = F(\alpha)$ for some α satisfying $\alpha^p \in F$.*

Theorem 7.17 (Galois's Great Theorem) *Let $f(X)$ be a polynomial over a field F of characteristic zero. Then $f(X)$ is soluble by radicals if and only if the Galois group of $f(X)$ over F is soluble.*