School of Mathematics and Statistics

MT5836 Galois Theory

Handout VI: Galois groups; the Fundamental Theorem of Galois Theory

6 Galois Groups and the Fundamental Theorem of Galois Theory

Galois groups

Definition 6.1 Let K be an extension of the field F. The *Galois group* $\mathrm{Gal}(K/F)$ of K over F is the set of all F-automorphisms of K with binary operation being composition of automorphisms.

The sets $\mathscr{F}$ and $\mathscr{G}$

Definition 6.3 Let K be an extension of the field F and let $G = \mathrm{Gal}(K/F)$ be the Galois group of K over F.

(i) Define $\mathscr{G}$ to be the set of subgroups of G.

(ii) Define $\mathscr{F}$ to be the set of *intermediate fields*; that is,

$$\mathscr{F} = \{\, L \mid L \text{ is a field with } F \subseteq L \subseteq K \,\}.$$

(iii) If $H \in \mathscr{G}$, define

$$H^* = \{\, x \in K \mid x\phi = x \text{ for all } \phi \in H \,\},$$

the set of points in K fixed by all F-automorphisms in H.

(iv) If $L \in \mathscr{F}$, define

$$L^* = \{\, \phi \in G \mid x\phi = x \text{ for all } x \in L \,\},$$

the set of all F-automorphisms that fix all points in L.

We shall show that (iii) and (iv) in this definition provide us with maps ${}^*\colon \mathscr{G} \to \mathscr{F}$ and ${}^*\colon \mathscr{F} \to \mathscr{G}$ and then investigate properties of these maps.

Lemma 6.4 *Let K be an extension of the field F and $G = \mathrm{Gal}(K/F)$.*

(i) *If $H \in \mathscr{G}$, then $H^* \in \mathscr{F}$;*

(ii) *If $L \in \mathscr{F}$, then $L^* \in \mathscr{G}$;*

(iii) *If $H_1, H_2 \in \mathscr{G}$ with $H_1 \leqslant H_2$, then $H_1^* \supseteq H_2^*$;*

(iv) *If $L_1, L_2 \in \mathscr{F}$ with $L_1 \subseteq L_2$, then $L_1^* \geqslant L_2^*$.*

Thus our definitions of * provide us with maps $\mathscr{G} \to \mathscr{F}$ and $\mathscr{F} \to \mathscr{G}$ that *reverse inclusions.*

The Fundamental Theorem of Galois Theory

Definition 6.5 A finite extension of fields is called a *Galois extension* if it is normal and separable.

Lemma 6.6 *Let K be a finite Galois extension of a field F and L be an intermediate field ($F \subseteq L \subseteq K$). Then K is a Galois extension of L.*

Theorem 6.7 (Fundamental Theorem of Galois Theory) *Let K be a finite Galois extension of a field F and $G = \mathrm{Gal}(K/F)$. Then:*

(i) $|G| = |K : F|$.

(ii) *The maps $H \mapsto H^*$ and $L \mapsto L^*$ are mutual inverses and give a one-one inclusion-reversing correspondence between $\mathscr{G}$ and $\mathscr{F}$.*

(iii) *If L is an intermediate field, then*

$$|K : L| = |L^*| \qquad \text{and} \qquad |L : F| = |G|/|L^*|.$$

(iv) *An intermediate field L is a normal extension of F if and only if L^* is a normal subgroup of G. Moreover, in this situation,*

$$\mathrm{Gal}(L/F) \cong G/L^*.$$

Tools used in the proof of the Fundamental Theorem

Lemma 6.8 *Let K be a finite Galois extension of a field F and $G = \mathrm{Gal}(K/F)$. The fixed field of G,*

$$G^* = \mathrm{Fix}_K(G) = \{\, x \in K \mid x\phi = x \text{ for all } \phi \in G \,\},$$

is precisely the base field of F.

Lemma 6.9 *Let K be a finite separable extension of a field F and let H be a finite group of F-automorphisms of K (that is, H is some subgroup of $\mathrm{Gal}(K/F)$). Then*

$$|K : H^*| = |H|$$

(where $H^* = \mathrm{Fix}_K(H)$).

Lemma 6.10 *Let K be a finite Galois extension of a field F and $G = \mathrm{Gal}(K/F)$. The following conditions on an intermediate field L are equivalent:*

(i) *L^* is a normal subgroup of G;*

(ii) *$L\phi \subseteq L$ for all $\phi \in G$;*

(iii) *L is a normal extension of F.*

Definition 6.11 When K is a finite Galois extension of the field F, the maps $H \mapsto H^*$ and $L \mapsto L^*$ are called the *Galois correspondence* between the set $\mathscr{G}$ of subgroups of the Galois group and the set $\mathscr{F}$ of intermediate fields.

Final observations for examples of Galois groups

Definition 6.12 Let $f(X)$ be a polynomial over a field F. The *Galois group* $\mathrm{Gal}(f(X))$ of $f(X)$ is the Galois group $\mathrm{Gal}(K/F)$ of the splitting field K of $f(X)$ over F.

Lemma 6.14 *Let $f(X)$ be a polynomial over the field F, let K be the splitting field of $f(X)$ over F and let Ω be the set of roots of $f(X)$ in K. Then $\mathrm{Gal}(K/F)$ is isomorphic to the group of permutations that it induces on Ω.*

Since a polynomial of degree n has at most n roots in a splitting field, the above lemma has the following consequence as an immediate corollary.

Corollary 6.15 *Let $f(X)$ be a polynomial of degree n over a field F. The Galois group of $f(X)$ over F is isomorphic to a subgroup of the symmetric group S_n of degree n.*

Galois groups of finite fields

Definition 6.17 The *Frobenius automorphism* γ of the finite field $\mathbb{F}_{p^n}$ of order p^n is the map $\gamma \colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by

$$\gamma \colon a \mapsto a^p$$

for all $a \in \mathbb{F}_{p^n}$.

Lemma 6.18 *The Frobenius automorphism γ of $\mathbb{F}_{p^n}$, given by $a\gamma = a^p$ for all $a \in \mathbb{F}_{p^n}$, is an $\mathbb{F}_p$-automorphism of $\mathbb{F}_{p^n}$ (that is, an element of the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$).*

Theorem 6.19 *Let p be a prime number and n a positive integer. Then the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ of the Galois field of order p^n over its prime subfield is cyclic of order n generated by the Frobenius automorphism γ.*