Notes on Galois Theory

Math 431 04/28/2009 Radford

We outline the foundations of Galois theory. Most proofs are well beyond the scope of the our course and are therefore omitted. The symbols $\leq$ and $\trianglelefteq$ in the context of groups denote subgroup and normal subgroup respectively.

---

1 The Galois Group, Roots of Polynomials, and Splitting Fields

For a ring E with unity $\mathrm{Aut}(E)$ denotes the group of ring automorphisms of E under function composition. Observe that $\mathrm{Aut}(E) \leq \mathrm{Sym}(E)$, the group of permutations on the set E under composition.

For the remainder of these notes E is field. $F \subseteq E$ will mean F is a field and E is a field extension of F.

Suppose $F \subseteq E$. The subset of automorphisms $\sigma \in \mathrm{Aut}(E)$ which fix F pointwise, that is satisfy $\sigma(a) = a$ for all $a \in F$, is denoted $\mathrm{Gal}(E/F)$. Observe that $\mathrm{Gal}(E/F) \leq \mathrm{Aut}(E)$. Recall that E is a vector space over F where scalar multiplication is defined by multiplication in E; that is $a{\cdot}\alpha = a\alpha$ for all $a \in F$ and $\alpha \in E$. For such a, α, and for $\sigma \in \mathrm{Gal}(E/F)$, the calculation

$$\sigma(a{\cdot}\alpha) = \sigma(a\alpha) = \sigma(a)\sigma(\alpha) = a\sigma(\alpha) = a{\cdot}\sigma(\alpha)$$

shows that σ is F-linear.

Here is our first important connection between the Galois group and roots of polynomials. The roots of $p(x) \in F[x]$ which are contained in E are permuted by all $\sigma \in \mathrm{Gal}(E/F)$.

Lemma 1 *Suppose $F \subseteq E$, $p(x) \in F[x]$, $a \in E$, and $\sigma \in \mathrm{Gal}(E/F)$. Then $\sigma(p(a)) = p(\sigma(a))$. In particular $p(a) = 0$ implies $p(\sigma(a)) = 0$. Thus σ permutes the roots of $p(x)$ in E.*

PROOF: Write $p(x) = a_0 + a_1x + \cdots + a_nx^n$, where $n \geq 0$ and $a_0, \ldots, a_n \in F$. Then $\sigma(a_i) = a_i$ for all $0 \leq i \leq n$ since $\sigma \in \mathrm{Gal}(E/F)$. The calculation

$$\begin{aligned}
\sigma(p(a)) &= \sigma(a_0 + a_1a + \cdots + a_na^n) \\
&= \sigma(a_0) + \sigma(a_1a) + \cdots + \sigma(a_na^n) \\
&= \sigma(a_0) + \sigma(a_1)\sigma(a) + \cdots + \sigma(a_n)\sigma(a^n) \\
&= a_0 + a_1\sigma(a) + \cdots + a_n\sigma(a)^n \\
&= p(\sigma(a))
\end{aligned}$$

establishes $\sigma(p(a)) = p(\sigma(a))$. The remaining details are left to the reader. □

If $\sigma, \tau \in \mathrm{Gal}(E/F)$ then $\sigma = \tau$ when σ and τ agree on generators of E as a field extension of F.

Lemma 2 *Suppose $F \subseteq E$ and $E = F(S)$, where $S \subseteq E$, and $\sigma, \tau \in \mathrm{Gal}(E/F)$ satisfy $\sigma(s) = \tau(s)$ for all $s \in S$. Then $\sigma = \tau$.*

PROOF: Since $\sigma, \tau \in \mathrm{Aut}(E)$ the set $D = \{a \in E \,|\, \sigma(a) = \tau(a)\}$ is a subfield of E. We need only show $D = E$.

By assumption $S \subseteq D$. Now $F \subseteq D$ since σ, τ fix the elements of F. Therefore $F \cup S \subseteq D$ which means the subfield $F(S)$ of E generated by $F \cup S$ is contained in D. Since $E = F(S)$, $D = E$. □

Let $H \subseteq \mathrm{Gal}(E/F)$. Then $\boxed{E_H = \{a \in E \,|\, \sigma(a) = a \;\; \forall\, \sigma \in H\}}$ is a subfield of E and $F \subseteq E_H \subseteq E$. In particular $F \subseteq E_{\mathrm{Gal}(E/F)}$. When the latter two fields are equal minimal polynomials over F split into distinct linear factors.

Proposition 1 *Suppose that $F \subseteq E$ and $F = E_{\mathrm{Gal}(E/F)}$; that is if $a \in E$ and $\sigma(a) = a$ for all $\sigma \in \mathrm{Gal}(E/F)$ then $a \in F$. Suppose that $a \in E$ is algebraic over and has minimal polynomial $p(x) \in F[x]$. Then $S = \{\sigma(a) \,|\, \sigma \in \mathrm{Gal}(E/F)\}$ is finite and $p(x) = \prod_{s \in S}(x - s)$.*

PROOF: S consists of roots of $p(x)$ by Lemma 1. Now S is finite since $p(x) \neq 0$. Set $g(x) = \prod_{s \in S}(x - s)$. Then $g(x)$ divides $p(x)$ in $E[x]$ as each factor does.

Let $\tau \in \mathrm{Gal}(E/F)$. Since S is finite $\tau(S) = S$. Since $\tau \in \mathrm{Aut}(E)$ it induces a ring automorphism $\overline{\tau} : E[x] \longrightarrow E[x]$ defined by

$$\overline{\tau}(a_0 + a_1 x + \cdots + a_n x^n) = \tau(a_0) + \tau(a_1)x + \cdots + \tau(a_n)x^n$$

for all $h(x) = a_0 + a_1 x + \cdots + a_n x^n \in E[x]$. Observe that $\overline{\tau}(h(x)) = h(x)$ for all $\tau \in \mathrm{Gal}(E/F)$ if and only if $h(x) \in F[x]$ since $F = E_{\mathrm{Gal}(E/F)}$.

For all $\tau \in \mathrm{Gal}(E/F)$ the calculation

$$\overline{\tau}(g(x)) = \overline{\tau}(\prod_{s\in S}(x-s)) = \prod_{s\in S}\overline{\tau}(x-s) = \prod_{s\in S}(x-\tau(s)) = \prod_{s\in S}(x-s) = g(x)$$

shows that $g(x) \in F[x]$. Since $g(a) = 0$ it follows that $p(x)$ divides $g(x)$ in $F[x]$. Therefore the monic polynomials $p(x)$ and $g(x)$ divide each other in $E[x]$ which means that $p(x) = g(x)$. $\square$

Theorem 1 *Suppose $F \subseteq E$ and E is a finite extension of F. Then* $\mathrm{Gal}(E/F)$ *is a finite group and* $[E : F] = |\mathrm{Gal}(E/F)|[E_{\mathrm{Gal}(E/F)} : F]$. $\square$

Let E be a finite extension of F. Then E is a *Galois extension* if $[E : F] = |\mathrm{Gal}(E/F)|$ or equivalently $F = E_{\mathrm{Gal}(E/F)}$. Thus E is a Galois extension of F if for $a \in E$, $\sigma(a) = a$ for all $\sigma \in \mathrm{Gal}(E/F)$ implies $a \in F$.

As a result of Theorem 1 and Proposition 1:

Corollary 1 *Suppose $F \subseteq E$ is finite extension which is Galois. Then E is a splitting field of some polynomial $f(x) \in F[x]$ over F.* $\square$

In characteristic zero the converse is true.

Theorem 2 *Suppose that F is a field of characteristic zero, $F \subseteq E$ and $[E : F]$ is finite. If E is a splitting field of some non-zero $f(x) \in F[x]$ over F then E is a Galois extension of F.* $\square$

2 The Galois Correspondence

Suppose $F \subseteq K \subseteq E$. Then $\mathrm{Gal}(E/K) \leq \mathrm{Gal}(E/F)$. Thus there is an inclusion reversing map

$$K \mapsto \mathrm{Gal}(E/K)$$

from extensions $F \subseteq K \subseteq E$ to subgroups of $\mathrm{Gal}(E/F)$. Likewise

$$H \mapsto E_H$$

is an inclusion reversing map from subgroups of $\mathrm{Gal}(E/F)$ to extensions of F which are subfields of E. If $F \subseteq E$ is a finite Galois extension then these are inverses.

3 The Fundamental Theorem of Galois Theory

Theorem 3 *Suppose that F is a field of characteristic zero and $F \subseteq E$ is a finite Galois extension. Then:*

(a) *There is an inclusion reversing bijection*

$$\{\textit{subgroups of } \mathrm{Gal}(E/F)\} \longrightarrow \{K \mid F \subseteq K \subseteq E\}$$

described by $H \mapsto E_H$ whose inverse is given by $K \mapsto \mathrm{Gal}(E/K)$.

Suppose $F \subseteq K \subseteq E$.

(b) *E is a Galois extension of K. Thus*

$$[E : K] = \mathrm{Gal}(E/K)| \quad \textit{and} \quad [K : F] = [\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)].$$

(c) *K is a Galois extension of F if and only if $\sigma(K) = K$ for all $\sigma \in \mathrm{Gal}(E/F)$ if and only if $\mathrm{Gal}(E/K) \trianglelefteq \mathrm{Gal}(E/K)$. In this case*

$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(K/F).$$

Proof: Part (a), which we will assume, is the heart of the theorem. Let $F \subseteq K \subseteq E$.

We show part (b). By Corollary 1 E is a splitting field of some $f(x) \in F[x]$ over F. Thus $f(x) \in K[x]$ and E is a splitting field of $f(x)$ over K. This means E is a Galois extension of K by Theorem 2 and therefore $[E : K] = |\mathrm{Gal}(E/K)|$. The second equation of part (b) follows from the first and the equation $|\mathrm{Gal}(E/F)| = [E : F] = [E : K][K : F]$.

To show part (c), assume that K is a Galois extension of F. Then K is a splitting field of some $g(x) \in F[x]$ over F. Let $\sigma \in \mathrm{Gal}(E/F)$. Then σ fixes $a \in F$ and by Lemma 1 permutes the roots of $g(x)$. Therefore $\sigma(K) \subseteq K$. Now σ is injective and a F-linear map. Since K is a finite-dimensional vector space over F it follows that $\sigma(K) = K$.

Assume that $\sigma(K) = K$ for all $\sigma \in \mathrm{Gal}(E/F)$. Then the restriction map $\pi : \mathrm{Gal}(E/F) \longrightarrow \mathrm{Gal}(K/F)$ given by $\pi(\sigma) = \sigma|_K$ is well-defined and a group homomorphism. Note $\mathrm{Ker}\,\pi = \mathrm{Gal}(E/K)$. Since π induces an injection $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \hookrightarrow \mathrm{Gal}(K/F)$, by part (b) and Theorem 1 it follows that $[K : F] = |\mathrm{Gal}(K/F)|$. Therefore K is a Galois extension of F. To complete the proof of part (c) we use part (a) and note that $\sigma(E_H) = E_{\sigma H \sigma^{-1}}$ for all $\sigma \in \mathrm{Gal}(E/F)$ and $H \leq \mathrm{Gal}(E/F)$. $\square$

4 Solvability of Polynomials by Radicals

The goal of this section is to prove:

Proposition 2 *Let F be a field of characteristic zero, $F \subseteq E \subseteq F(a_1, \ldots, a_r)$, where E is a finite Galois extension of F, $r \geq 1$, and there are $n_1, \ldots, n_r > 0$ such that $a_1^{n_1} \in F$ and $a_i^{n_i} \in F(a_1, \ldots, a_{i-1})$ for all $1 < i \leq r$. Then $\mathrm{Gal}(E/F)$ is solvable.*

First commentary on splitting fields of $x^n - 1$ and $x^n - a$ over F, where $a \in F$.

Let E' be a splitting field of $f(x) = x^n - 1$ over F. We may assume $n > 1$. Now $f(x)$ has no multiple zeros since $f'(a) = na^{n-1} \neq 0$ for all non-zero $a \in E$. Therefore the set of roots G of $f(x)$ in E' has n-elements. Since G is a finite subgroup of the group of units of E' it follows that G is cyclic. Thus $G = (\omega)$, ω is a primitive n^{th} root of unity since it generates G, and $E' = F(\omega)$.

A splitting field of $x^n - a$ over F has the form $F(\omega, a^{1/n})$, where $(a^{1/n})^n = a$. Note that $x^n - a$ has n distinct roots $a^{1/n}, \omega a^{1/n}, \ldots, \omega^{n-1} a^{1/n}$. Thus

$$x^n - a = \prod_{i=0}^{n-1} (x - \omega^i a^{1/n}).$$

Lemma 3 *Let $n \geq 1$. Then $\mathrm{Gal}(F(\omega)/F)$ is abelian, hence solvable, where ω is a primitive n^{th} root of unity.*

PROOF: Let $\sigma \in \mathrm{Gal}(F(\omega)/F)$. Then $\sigma(G) = G$ by Lemma 1. Thus the restriction map $\pi : \mathrm{Gal}(F(\omega)/F) \longrightarrow \mathrm{Aut}(G)$ given by $\pi(\sigma) = \sigma|_G$ is a group homomorphism. Since ω generates $F(\omega)$ as a field extension of F necessarily π is injective by Lemma 2. Since G is a finite-cyclic group $\mathrm{Aut}(G)$ is abelian. Therefore $\mathrm{Gal}(F(\omega)/F)$ is abelian. □

Lemma 4 *Let $n \geq 1$. Suppose F contains a primitive n^{th} root of unity and $0 \neq a \in F$. Then $\mathrm{Gal}(F(a^{1/n})/F)$ is abelian, hence solvable, where $a^{1/n}$ is a root of $x^n - a$.*

PROOF: Note that $F(a^{1/n})$ is a splitting field of $x^n - a$ over Fv since F contains a primitive n^{th} root of unity ω. Let $\sigma \in \mathrm{Gal}(F(a^{1/n}/F)$. Then $\sigma(a^{1/n})$ is a root of $x^n - a$. Therefore $\sigma(a^{1/n}) = \omega^i a^{1/n}$ for a unique $0 \leq i < n$. Define $\pi : \mathrm{Gal}(F(a^{1/n}/F) \longrightarrow \mathbf{Z}_n$ by $\pi(\sigma) = i$. Then π is a homomorphism to the additive group $\mathbf{Z}_n$ which is injective since $a^{1/n}$ generates $F(a^{1/n})$ as a field extension of F. Thus $\mathrm{Gal}(F(a^{1/n}/F)$ is cyclic. □

Suppose that $F \subseteq K \subseteq L$, where K and L are finite Galois extensions of F. Then $\mathrm{Gal}(L/K) \trianglelefteq \mathrm{Gal}(L/F)$ and $\mathrm{Gal}(L/F)/\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(K/F)$ by part (c) of Theorem 3. Therefore

Lemma 5 *Suppose that $F \subseteq K \subseteq L$, where K and L are finite Galois extensions of F. Then $\mathrm{Gal}(L/F)$ is solvable if and only if $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(K/F)$ are solvable.* □

We will establish Proposition 2 by a series of reductions to Lemmas 3 and 4. Let n be the least common multiple of $n_1, \ldots, n_r$. Since E is a finite Galois extension of F it is a splitting field over F by Proposition 1. Let $f(x) \in F[x]$ be a polynomial such that E is a splitting field of $f(x)$ in $F(a_1, \ldots, a_r)$.

Lemma 6 *If Proposition 2 holds whenever F contains a primitive n^{th} root of unity then it holds in general.*

PROOF: Let L be a splitting field of $x^n - 1$ over $F(a_1, \ldots, a_r)$. Then L contains a primitive n^{th} root of unity ω. Regard $F(\omega)$ as the base field and consider the extensions $F(\omega) \subseteq E(\omega) \subseteq F(\omega)(a_1, \ldots, a_r) \subseteq L$. Since E is a splitting field of $f(x)$ over F and $f(x) \in F(\omega)[x]$, it follows that $E(\omega)$ is a splitting field of $f(x)$ over $F(\omega)$ in $F(\omega)(a_1, \ldots, a_r)$.

Observe that $F(\omega) \subseteq E(\omega) \subseteq F(\omega)(a_1, \ldots, a_r)$ satisfies the hypothesis of Proposition 2 and $F(\omega)$ contains a primitive n^{th} root of unity. Assume that $\mathrm{Gal}(E(\omega)/F(\omega))$ is solvable. The sequence $F \subseteq F(\omega) \subseteq E(\omega)$ satisfies the hypothesis of Lemma 5 since $F(\omega)$ and $E(\omega)$ are splitting fields of $x^n - 1, f(x)(x^n - 1) \in F[x]$ respectively over F. Since $\mathrm{Gal}(F(\omega)/F)$ is solvable by Lemma 3, $\mathrm{Gal}(E(\omega)/F)$ is solvable by Lemma 5. Applying the same to $F \subseteq E \subseteq E(\omega)$ we conclude that $\mathrm{Gal}(E/F)$ is solvable. $\Box$

Lemma 7 *Suppose F contains a primitive n^{th} root of unity ω. Then Proposition 2 holds then it holds when $r = 1$.*

PROOF: The sequence of Proposition 2 is $F \subseteq E \subseteq F(a_1)$. Since ω^{n/n_1} is a primitive n_1^{th} root of unity $F(a_1)$ is a splitting field of $x^{n_1} - a_1^{n_1}$ over F. Thus $\mathrm{Gal}(F(a_1)/F)$ is solvable by Lemma 4 and hence $\mathrm{Gal}(E/F)$ is solvable by Lemma 5. $\Box$

We now complete the proof of Proposition 2. By virtue of Lemmas 6 and 7 we may assume F contains a primitive n^{th} root of unity and $r > 1$. Consider the sequence $F(a_1) \subseteq E(a_1) \subseteq F(a_1)(a_2, \ldots, a_r)$. Note that $E(a_1)$ is a Galois extension of $F(a_1)$ since it is a splitting field of $f(x)(x^{n_1} - a_1^{n_1})$ over F, hence over $F(a_1)$. The hypothesis of Proposition 2 applies to this sequence with base field $F(a_1)$. Thus by induction in r we conclude that $\mathrm{Gal}(E(a_1)/F(a_1))$ is solvable. Now $F(a_1)$ is a splitting field of $x^{n_1} - a_1^{n_1}$ over F. We can apply Lemma 5 to $F \subseteq F(a_1) \subseteq E(a_1)$ and $F \subseteq E \subseteq E(a_1)$ to conclude that $\mathrm{Gal}(E/F)$ is solvable. $\Box$