Erin Matoza
Math434
Galois

I. Field Extensions (brief review – see handout from class (4-8))
(not explained, just displayed for quick reference)
A. (defn) F|K is a field extension where K is a subfield of F (K $\leq$ F)
B. (defn) A finite field is any field having only finitely many elements.
C. (defn) Let F be an extension field of K and b an element of F. We say b is algebraic over K if b is the root of some non-zero
polynomial with coefficients in K. WLOG assume the polynomial is monic, say $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0$.
D. (defn) With F!K, the K-dimension of F is the degree of the extension

II. Splitting Field
A. (defn) Let F|K be an extension of finite degree and p$\in$K[x]. Then F is the splitting field of p over K iff F = K (a_1, a_2, … ,a_m)
such that p = (x-a_1)(x-a_2) … (x-a_m) (Herman, 5).
B. Normality
1. (defn) a field extension F|K is called normal iff for every irreducible polynomial m(x) over K, either m(x) has no root in F or
it splits into the product of linear polynomials over F (Herman, 5).
2. Proposition: every normal extension of finite degree is the splitting field of some polynomial (Herman, 5).
Pf: Let [F:K] be finite, then F = K(a, b, c, …, z) for elements a, b, c, …, z in F. Since their minimal polynomials m_a, m_b, …, m_z
are irreducible over K, one can use the definition of a normal field extension to show that they all split into the product of
linear polynomials over F. Hence, F is the splitting field of $m_a m_b \ldots m_z$.
3. Theorem: let K F and p = $p_0+p_1x+ \ldots +p_{n-1}x^{n-1}+x$$\in$K[x]. If F is the splitting field of p over K, then F|K is a normal extension.
Pf: not displayed, too difficult
Note: splitting field ==>normal (Herman, 5).
C. Separability
1. (defn) An irreducible polynomial f over a field K is separable over K if it has no multiple zeros in a splitting field. This
means that in any splitting field, f, takes the form: k(t– a) … (t-a_n) where the a_i are all different (Stewart, 83).
2. (defn) (Logically) An irreducible polynomial over a field, K, is inseparable over K if it is not separable over K
(Stewart, 83).
D. Solvability
1. (defn) We say that a group G is solvable if G has a series of subgroups $\{e\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_k = G$ such that,
for each 0 < i < k. H is normal in H_i and $H_{i+1}|H_i$ is abelian.
Note: abelian groups are solvable as are dihedral groups and any group of order p^n, where p is a prime (Gallian, 556).
2. Theorem: A factor group of a solvable group is solvable
Pf: Suppose G has a series of subgroups $\{e\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_k = G$, where, for each 0 < i < k, H is normal in
H_{i+1} and $H_{i+1}|H_i$ is abelian. If N is any normal subgroup of G, then $\{e\} = H_oN|N \subset H_1N|N \subset H_2N|N \subset \ldots \subset H_kN|N = G|N$ is the
requisite series of subgroups that guarantees that G|N is solvable (Gallian, 557).
3. Theorem: Let F be a field of characteristic 0 and let a$\in$F. If E is the splitting field of x^n–a over F, then the Galois group
Gal(E|F) is solvable. (This makes sense intuitively and will be more logical after Galois Group is formally defined.)
Pf: not displayed, long and tedious (Gallian, 556).

III. Fundamental Theorem of Galois Theory

A. Let L:K be a field extension with Galois group G, which consists of all K-automorphisms of L. Let F be the set of intermediate fields M, and H be the set of all subgroups B of G. We have defined two maps,

$$\pi : F \to H$$
$$\theta : H \to F$$

as follows: if M∈F, then π(M) is the group of all M-automorphisms of L. If B∈H, then θ(B) is the fixed field of H (defined below).

We have observed that the maps π and θ reverse inclusions, that M≤ $\theta(\pi(M))$, and H≤ $\pi(\theta(H))$ (Stewart, 104).

(defn) Let E be an extension field of the field F. The Galois group of E over F, Gal(E|F), is the set of all automorphisms of E that take every element of F to itself (identity map). If H is a subgroup of Gal(E|F), the set E = {x∈E|π(x) = x for all π ∈H} is called the fixed field of H (Gallian, 548).

B. Fundamental Theorem: If L:K is a finite, separable, normal field extension of degree n, with Galois group G; and if F, H, π, θ, are defined as above, then:

1. The Galois group G have order n
2. The maps π and θ are mutual inverses and set up an order-reversing one-to-one correspondence between F and H
3. If M is an intermediate field, then

$$[L:M] = |\pi(M)|$$
$$[M:K] = |G| \,/\, |\pi(M)|$$

4. An intermediate field M is a normal extension of K iff (M) is a normal subgroup of G (in the usual sense of group theory)
5. and, If an intermediate field M is a normal extension of K, then the Galois group of M:K is isomorphic to the quotient group G|π(M) (Stewart, 104).

Pf (part 4.): We need a Lemma to aid us in this proof. We can use one from page 105 of I Stewart's Galois Theory. The following is Lemma 11.2:

Lemma: Suppose that L:K is a field extension, M is an intermediate field, and t is a K-automorphism of L. Then

$$\pi(t(M)) = t(\pi(M))t^{-1} .$$

Pf (lemma): Let M' = t(M), and take y∈ π(M), x_1 ∈M'. Then x_1 = t(x) for some x∈M. Then $(tyt^{-1})(x_1)$ = ty(x) = t(x) = x_1

So that $t\pi(M)t^{-1} \leq \pi(M')$. Similarly $t^{-1}\pi(M')t \leq \pi(M)$ and $t\,\pi(M)t^{-1} \geq \pi(M')$. Hence, the lemma is proved.

Pf (4.): If M:K is normal, let t∈G. Then $t|_m$ is a K-monomorphism M –> L, so is a K-automorphism of M by Theorem 10.5 (Stewart, page 99) which states that for a finite extension L:K, it is equivalent to state that L:K is normal and every extension M of K containing L, every K-monomorphism, t:L –> M, is a K-automorphism of L. Hence, t(M) = M. Using our lemma, we know $t\pi(M)t^{-1} = \pi(M)$, so that π(M) is a normal subgroup of G (Stewart, 106).

C. (defn) The set of all automorphisms of F|K is a group if multiplication of automorphisms is defined as the composition of mappings; this group is denoted by Aut(F|K). If F|K is a normal extension of finite degree, this group is called the Galois group of F|K and is denoted by Gal(F|K) (Herman, 5).

D. Proposition: Let F|K be a normal extension of finite degree, then |Gal(F|K)| = [F:K] (Herman, 6).

Pf: A corollary is needed. We will use one from a handout written by Peter Herman, 2001.

Corollary: Assume [F:K] is finite. Then there exists some c∈F such that F = K(c) (Herman, 4).

Pf (corollary): omitted, involves theories involving symmetric polynomials (Herman, 5).

Sidebar: (defn) Let K be a field and f∈K[x_1, x_2, ..., x_n] (a polynomial of n variables). Then f is called a symmetric polynomial iff for any a∈S_n, f($x_{(1)a}$,$x_{(2)a}$, ..., $x_{(n)a}$) = f(x_1, x_2, ...,$_x n$) holds (Herman, 3).

Using the corollary, there is some a$\in$F satisfying F = K(a). The minimal polynomial m_a(x) of a over K is of degree n = [F:K]

and (as F|K is normal) splits into the product of linear polynomials over F. Let $m_a(x) = (x-a_1)(x-a_2) \ldots (x-a_n) = x^n + \ell_{n-1}x^{n-1} +$

$\ldots + \ell_0$ with a_1 = a and $a_1, \ldots, a_n$ pairwise different. Assume Gal(F|K); then

$$0 = (0) = \pi(a^n + \ell_{n-1}a^n + \ldots + \ell_0)$$
$$= (\pi(a))^n + \pi(\ell_{n-1})(\pi(a))^{n-1} + \ldots + \pi(\ell_1)\pi(a^1) + \pi(\ell_0)$$
$$= (\pi(a))^n + \ell_{n-1}(\pi(a))^{n-1} + \ldots + \ell_1(\pi(a)) + \ell_0.$$

E. note: Let F|K be a normal extension of finite degree. We denote Gal(F|K) by G (Herman, 7).

1. For a subfield K$\leq$L$\leq$F set S(L) = $\{\theta \in G|$ (any $\ell \in$L)$\theta(\ell) = \ell\}$
2. For a subgroup H$\leq$G set (H) = $\{b\in F|$(any n$\in$H)$\pi(b) = b\}$.

F. Corollary: S(L)$\leq$G, K$\leq$ π(H)$\leq$F, S(K) = G, S(F) = $\{e\}$, $\pi(\{e\})$ = F. π(S(L)$\geq$L and S(π(H))$\geq$H. If K$\leq L_1 \leq L_2 \leq$F, then $S(L_1) \geq S(L_2)$

and similarly, if $H_1 \leq H_2 \leq$G, then $\pi(H_1) \geq (H_2)$ (Herman, 7).

----

key:

defn= definition
dfn= define
iff= if and only if
pf= proof
s.t. = such that

Work's Cited

Gallian, Joseph A. Contemporary Abstract Algebra (5th ed.). Houghton Mifflin Company: Boston, Mass: 2002.
Herman, Peter, 2001.
Stewart, Ian. Galois Theory (2nd ed.). Chapman & Hall/CRC: New York, NY: 1998.