Section X.53. Galois Theory

Note. I like the quote on page 448 of the text: “This section is perhaps the climax in elegance of the subject matter of the entire text.” So far, the highlights of Part X are:

1. Let $F \leq E \leq \overline{F}$, $\alpha \in E$, and let β be a conjugate of α over F (that is, $\mathrm{irr}(\alpha, F)$ has β as a zero also). Then there is an isomorphism $\psi_{\alpha,\beta}$ mapping $F(\alpha)$ onto $F(\beta)$ that leaves F fixed and maps α to β (this is half of Theorem 48.3, the Conjugation Isomorphism Theorem).

2. If $F \leq E \leq \overline{F}$ and $\alpha \in E$, then an automorphism σ of $\overline{F}$ that leaves F fixed must map α onto some conjugate of α over F (this is the first half of Corollary 48.5).

3. If $F \leq E$, the collection of all automorphisms of E leaving F fixed forms a group $G(E/F)$. For any subset S of $G(E/F)$, the set of all elements of E left fixed by all the elements of S is a field E_S. Also $F \leq E_{G(E/F)}$. (Theorem 48.15 and Theorem 48.11, respectively.)

4. A field E, where $F \leq E \leq \overline{F}$, is a splitting field over F if and only if every isomorphism of E onto a subfield of $\overline{F}$ leaving F fixed is an automorphism of E. If E is a finite extension and a splitting field over F, then $|G(E/F)| = \{E : F\}$ (Corollary 50.7).

5. If E is a finite extension of F, then $\{E : F\}$ divides $[E : F]$. If E is also separable over F, then $\{E : F\} = [E : F]$. Also, E is separable over F if and only if $\operatorname{irr}(\alpha, F)$ has all zeros of multiplicity 1 for every $\alpha \in E$ (Theorem 51.6, definition of "separable extension field," and Note 2 of Section 51).

6. If E is a finite extension of F and is a separable splitting field over F, then $|G(E/F)| = \{E : F\} = [E : F]$ (Corollary 50.7 and the definition of "separable extension field").

Definition 53.1. A finite extension K of F is a *finite normal extension of* F if K is a separable splitting field over F.

Note. If K is a finite normal extension of F, then by (4) we have $|G(K/F)| = \{K : F\}$ and by the definition of "finite normal extension" K is separable over F and we have $\{K : F\} = [K : F]$. So K satisfies $|G(K/F)| = \{K : F\} = [K : F]$. Conversely, if $|G(K/F)| = \{K : F\} = [K : F]$ where K is a finite extension of F, then K is a separable extension of F (by definition of "separable"). Since $\{K : F\}$ is the number of isomorphisms of K onto a subfield of $\overline{F}$ leaving F fixed and $G(K/F)$ is the set of all automorphisms of K leaving F fixed, then every isomorphism of K leaving F fixed is an automorphism of K. So by (4) above, K is a splitting field over F. That is, K is a finite normal extension of F. So K is a finite normal extension of F if and only if $|G(K/F)| = \{K : F\} = [K : F]$.

Theorem 53.2. Let K be a finite normal extension of F, and let E be an extension of F, where $F \leq E \leq K \leq \overline{F}$. Then

1. K is a finite normal extension of E, and
2. $G(K/E)$ is precisely the subgroup of $G(K/F)$ consisting of all those automorphisms that leave E fixed.
3. Moreover, two automorphisms σ and τ in $G(K/F)$ induce the same isomorphism of E onto a subfield of $\overline{F}$ if and only if they are in the same left coset of $G(K/E)$ in $G(K/F)$.

Note. Theorem 53.2 shows that there is a one-to-one correspondence between the left cosets of $G(K/E)$ in $G(K/F)$ and *isomorphisms* of E onto a subfield of K leaving F fixed. We cannot say that these left cosets correspond to *automorphisms* of E over F (i.e., elements of $G(E/F)$), since E may not be a splitting field over F (see Theorem 50.3). If E is a normal extension (and so by definition E is a splitting field over F) then these isomorphisms are automorphisms of E. In fact, this will occur if and only if $G(K/E)$ is a normal subgroup of $G(K/F)$ (so we get a relationship between finite normal extensions and normal subgroups). In this case, we can form the factor group $G(K/F)/G(K/E)$ and this factor group is isomorphic to $G(E/F)$. This is what is claimed and proved in Property 5 of the Main Theorem of Galois Theory (Theorem 53.6).

Note. Property 6 of the main Theorem of Galois Theory says that for K a finite normal extension of F, there is a one-to-one correspondence between the subgroups of $G(K/F)$ and the intermediate fields E where $F \le E \le K$. The subgroup of $G(K/F)$ corresponding to field E is $G(K/E)$ (and conversely, if we have a subgroup of $G(K/F)$ we can construct a corresponding intermediate field). Fraleigh does not actually *prove* Property 6, but "disposes" of it with the following example.

Example 53.3. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then K is a separable extension of $\mathbb{Q}$ by Example 51.8 ($\{K : \mathbb{Q}\} = [K : \mathbb{Q}] = 4$). Also, K is a splitting field over F of $\{x^2 - 2, x^2 - 3\}$ and so K is a finite separable splitting field, that is a finite normal extension, of $\mathbb{Q}$. By Example 48.17, there are 4 automorphisms of K leaving $\mathbb{Q}$ fixed because a basis for K over $\mathbb{Q}$ is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ (and such an automorphism must map a basis element to a conjugate and the automorphisms are ι, $\sigma_1 = \psi_{\sqrt{2},-\sqrt{2}}$, $\sigma_2 = \psi_{\sqrt{3},-\sqrt{3}}$, and $\sigma_3 = \psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{3},-\sqrt{3}}$); notice that $\psi_{\sqrt{2},-\sqrt{2}}(\sqrt{6}) = \psi_{\sqrt{3},-\sqrt{3}}(\sqrt{6}) = -\sqrt{6}$ but $(\psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{3},-\sqrt{3}})(\sqrt{6}) = \sqrt{6}$. In fact, $\{\iota, \sigma_1, \sigma_2, \sigma_3\}$ is isomorphic to Klein-4 (Example 48.17). We now find the one-to-one correspondence mentioned above. First, the group $\{\iota, \sigma_1, \sigma_2, \sigma_3\}$ only fixes $\mathbb{Q}$. The other elements of K (which are of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$) are not fixed by some element of $\{\iota, \sigma_1, \sigma_2, \sigma_3\}$. Next, the subgroup $\{\iota, \sigma_1\}$ of $\{\iota, \sigma_1, \sigma_2, \sigma_3\}$ only fixes elements of K of the form $a + c\sqrt{3}$—that is, $\{\iota, \sigma_1\}$ fixes $\mathbb{Q}(\sqrt{3})$. Similarly, we get the following correspondence between subgroups of $\{\iota, \sigma_1, \sigma_2\,\sigma_3\}$ and fixed intermediate fields:

$$
\begin{aligned}
\{\iota, \sigma_1, \sigma_2, \sigma_3\} &\longleftrightarrow \mathbb{Q} \\
\{\iota, \sigma_1\} &\longleftrightarrow \mathbb{Q}(\sqrt{3}) \\
\{\iota, \sigma_2\} &\longleftrightarrow \mathbb{Q}(\sqrt{2}) \\
\{\iota, \sigma_3\} &\longleftrightarrow \mathbb{Q}(\sqrt{6}) \\
\{\iota\} &\longleftrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})
\end{aligned}
$$

All subgroups of $G(K/\mathbb{Q}) = \{\iota, \sigma_1, \sigma_2, \sigma_3\}$ are normal (as guaranteed by Principle 5) and all intermediate fields are finite normal extensions (again, Property 5).

Note. In this setting of automorphisms and intermediate fields, if one subgroup is contained in another "larger" subgroup, then the larger subgroup (having more automorphisms) will have fewer elements fixed. So the larger subgroup will have a smaller corresponding fixed intermediate field. From the previous example, we have the following group diagram and field diagram:

$$\begin{tikzcd}
& \{\iota, \sigma_1, \sigma_2, \sigma_3\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{\iota, \sigma_1\} \arrow[dr, dash] & \{\iota, \sigma_2\} \arrow[d, dash] & \{\iota, \sigma_3\} \arrow[dl, dash] \\
& \{\iota\} &
\end{tikzcd}$$

$$\begin{tikzcd}
& K_{\{\iota\}} = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K_{\{\iota, \sigma_1\}} = \mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & K_{\{\iota, \sigma_2\}} = \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & K_{\{\iota, \sigma_3\}} = \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
& K_{\{\iota, \sigma_1, \sigma_2, \sigma_3\}} = \mathbb{Q} &
\end{tikzcd}$$

Here we denote K_H as the intermediate field fixed by subgroup H of automorphisms of $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Comparing the group diagram to the field diagram, we see that one is the other "upside down." This is an illustration of the *inversion principle.*

Fraleigh uses this example as justification of Property 6 of the Main Theorem of Galois Theory.

Note. Recall that for F a subfield of K, we defined $G(K/F)$ to be the set (a group by Theorem 48.15) of automorphisms of K which leave F fixed (Definition 48.16). Originally, we put no restriction on the type of extension of F which K is. The following definition concerns the case when K is a finite normal extension.

Definition 53.5. If K is a finite normal extension of a field F, then $G(K/F)$ is the *Galois group* of K over F.

Theorem 53.6. The Main Theorem of Galois Theory.
Let K be a finite normal extension of a field F, with Galois group $G(K/F)$. For a field E, where $F \leq E \leq K$, let $\lambda(E)$ be the subgroup of $G(K/F)$ leaving E fixed. Then λ is a one to one map of the set of all such intermediate fields E onto the set of all subgroups of $G(K/F)$. The following properties hold for λ:

Property 1. $\lambda(E) = G(K/E)$.

Property 2. $E = K_{G(K/E)} = K_{\lambda(E)}$.

Property 3. For $H \leq G(K/F)$, we have $\lambda(K_H) = H$.

Property 4. $[K : E] = |\lambda(E)|$ and $[E : F] = (G(K/F) : \lambda(E))$, the number of left cosets of $\lambda(E)$ in $G(K/F)$. (See Definition 10.13 for the (:) notation; this is the *index* of a subgroup in a group.)

Property 5. E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. When $\lambda(E)$ is a normal subgroup of $G(K/F)$, then

$$G(E/F) \cong G(K/F)/G(K/E).$$

Property 6. The diagram of subgroups of $G(K/F)$ is the inverted diagram of intermediate fields of K over F.

Note. First, we prove some of the properties of Theorem 53.6. Notice that Property 1 follows from the definition of $\lambda(E)$.

Proof of Property 2. Recall that for $\{\sigma_i \mid i \in I\}$ a collection of automorphisms of field E, the set $E_{\{\sigma_i\}}$ of all $a \in E$ left fixed by all σ_i is a subfield of E (Theorem 48.11). By Theorem 48.15, we have $E \leq K_{G(K/E)}$. Next, let $\alpha \in K$ where $\alpha \notin E$. Since K is a normal extension of E, then (by definition) K is a splitting field over E. Consider $f(x) = \mathrm{irr}(\alpha, E)$. Since $\alpha \notin E$ then the degree of $f(x)$ is greater than 1 and there is $\beta \neq \alpha$ a zero of f in $\overline{F}$. By the Conjugation Isomorphism Theorem (Theorem 48.3) $\psi_{\alpha,\beta}$ is an isomorphism of $E(\alpha)$ to $E(\beta)$ which leaves F fixed. By the Isomorphism Extension Theorem (Theorem 49.3), $\psi_{\alpha,\beta}$ can be extended to an automorphism of K which leaves F fixed; denote it as σ. So $\sigma \in G(K/E)$ but $\sigma(\alpha) = \beta \neq \alpha$. So $\alpha \notin K_{G(K/E)}$; the contrapositive implying that if $\alpha \in K_{G(K/E)}$ then $\alpha \in E$. Hence, $K_{G(K/E)} \leq E$ and we have $K_{G(K/E)} = E$. By Property 1, $E = K_{\lambda(E)}$. ∎

Note. Properties 1 and 2 combine to establish the one to one claim for λ: If $\lambda(E_1) = \lambda(E_2)$ then

$$\begin{aligned} E_1 &= K_{G(K/E_1)} \text{ by Property 2} \\ &= K_{\lambda(E_1)} \text{ by Property 1} \\ &= K_{\lambda(E_2)} \text{ by hypothesis} \\ &= K_{G(K/E_2)} \text{ by Property 1} \\ &= E_2 \text{ by Property 2.} \end{aligned}$$

Proof of Property 4. Since K is a finite normal extension fo F, then (by definition) K is a separable extension of F and (by definition of "separable") $\{K : F\} = [K : F]$. Since E satisfies $F \le E \le K$, by Theorem 51.9, K is separable over E and E is separable over F. That is (by definition) $\{K : E\} = [K : E]$ and $\{E : F\} = [E : F]$. Therefore $[K : E] = \{K : E\} = |G(K/E)| = \lambda(E)$ (by definition of $\{K : E\}$ and Property 1). Fields F, E, and K satisfy the hypotheses of Theorem 53.2, and by part (3) of Theorem 53.2 two automorphisms in $G(K/F)$ induce the same isomorphism of E onto a subfield of $\overline{F}$ (such automorphisms are isomorphisms of E which leave F fixed and there are [by definition] $\{E : F\}$ of these automorphisms) if and only if the two automorphisms lie in the same left coset of $G(K/E)$ in $G(K/F)$. So the number of such automorphisms, $\{E : F\}$, equals the number of left cosets, denoted $(G(K/F) : G(K/E))$. Since $\{E : F\} = [E : F]$ by above and $G(K/E) = \lambda(E)$ by Property 1, we have $[E : F] = (G(K/F) : \lambda(E))$. ∎

Note. We gloss over a detailed proof of Property 6 and instead appeal to Example 53.3. So this leaves Properties 3 and 5. We prove these at the end of this section, but first we explore some related topics.

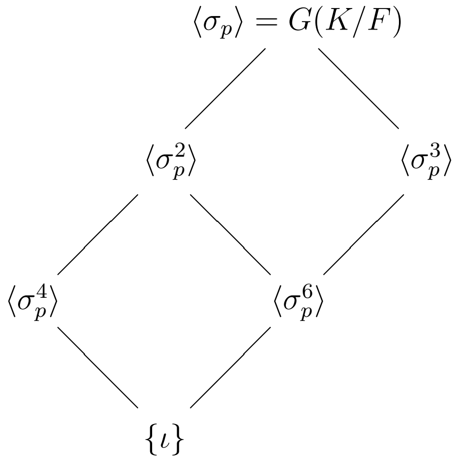
Note. If $f(x) \in F[x]$ is such that every irreducible factor of $f(x)$ is separable over F (and so by Note 3 of Section X.51, every zero of each irreducible factor is of multiplicity 1), then the splitting field K of $f(x)$ over F is separable (this follows by extending F by the zeros of each irreducible factor of f in turn and applying Theorem 51.9 at each stage). Therefore, K is a finite normal extension of F (by definition of "normal extension"). Hence, the Main Theorem of Galois Theory holds in this setting.

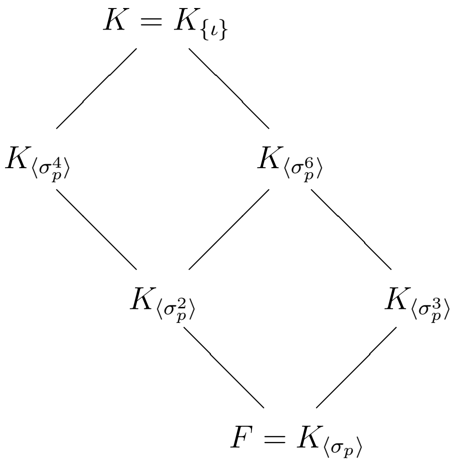
Definition. Let $f(x) \in F[x]$ and let K be the splitting field for $f(x)$ over F. The Galois group $G(K/F)$ is the *group of the polynomial* $f(x)$ over F.

Note. The structure of the group of polynomial $f(x)$ is related to the algebraic solvability of $f(x)$, as we see in Section X.56 in our *final goal.*

Theorem 53.7. Let K be a finite extension of degree n of a finite field F of p^r elements. Then $G(K/F)$ is cyclic of order n and is generated by σ_{p^r}, where for $\alpha \in K$ we have $\sigma_{p^r}(\alpha) = \alpha^{pr}$.

Example 53.8. Theorem 53.7 makes it easy to recognize $G(K/F)$ when dealing with finite extensions of finite fields, because $G(K/F)$ is cyclic and we have (up to isomorphism) classified all finite cyclic groups (Theorem 6.10). For example, let $F = \mathbb{Z}_p$ and let $[K : F] = 12$. Then $K = GF(p^{12})$ and by Theorem 53.7, $G(K/F) \cong \langle \mathbb{Z}_{12}, + \rangle$. We then have the group diagram for $G(K/F)$ and the field diagram of $K = GF(p^{12})$ as follows:


$\langle \sigma_p \rangle = G(K/F)$
$\langle \sigma_p^2 \rangle$
$\langle \sigma_p^3 \rangle$
$\langle \sigma_p^4 \rangle$
$\langle \sigma_p^6 \rangle$
$\{\iota\}$


$K = K_{\{\iota\}}$
$K_{\langle \sigma_p^4 \rangle}$
$K_{\langle \sigma_p^6 \rangle}$
$K_{\langle \sigma_p^2 \rangle}$
$K_{\langle \sigma_p^3 \rangle}$
$F = K_{\langle \sigma_p \rangle}$

Note. Let F be a field and let $f(x) \in F[x]$ be a polynomial of degree n with zeros $-r_1, -r_2, \ldots, -r_n \in \overline{F}$. Then by the Factor Theorem (Theorem 23.3), we have that $f(x) = a \prod_{i=1}^n (x + r_i)$ for some $a \in F$. We suppose $a = 1$ and then $f(x) = \prod_{i=1}^n (x + r_i)$. Multiplying this out to get the coefficients of the powers of x

we have:

$$f(x) = x^n + \underbrace{(r_1 + r_2 + \cdots + r_n)}_{\text{all zeros}} x^{n-1}$$

$$+ \underbrace{(r_1r_2 + r_1r_3 + \cdots + r_{n-1}r_n)}_{\text{all products of pairs of zeros}} x^{n-2}$$

$$+ \underbrace{(r_1r_2r_3 + r_1r_2r_4 + \cdots + r_{n-2}r_{n-1}r_n)}_{\text{all products of triples of zeros}} x^{n-3}$$

$$+ \cdots + \underbrace{(r_1r_2 \ldots r_k + \cdots + r_{n-k+1}r_{n-k+2} \cdots r_n)}_{\text{all products of } k\text{-tuples of zeros}} x^{n-k}$$

$$+ \cdots + \underbrace{(r_1r_2 \cdots r_{n-1} + r_1r_2 \cdots r_{n-2}r_n + \cdots + r_2r_3 \cdots r_n)}_{\text{all products of } (n-1)\text{-tuples of zeros}} x$$

$$+ \qquad \underbrace{(r_1r_2 \cdots r_n)}_{\text{product of all } n \text{ zeros}}$$

Notice that if we permute the zeros (for example, if we interchange r_1 and r_2) then the coefficients remain unchanged. Since the permutations of the zeros fixes the coefficients, the coefficients are said to be *symmetric* expressions of the zeros. **This is where permutation groups enter the scene of algebraic solutions of polynomial equations!!!**

Property 3. Let K be a finite normal extension of field F with Galois group $G(K/F)$. For a field E where $F \leq E \leq K$, let $\lambda(E)$ denote the subgroup of $G(K/F)$ leaving E fixed. For $H \leq G(K/F)$, denote as K_H the field fixed by group H of automorphisms of K (so $F \leq K_H$ by definition). THEN for $H \leq G(K/F)$ we have $\lambda(K_H) = H$.

Note. Now for the proof of Property 3.

Property 5. Let K be a finite normal extension of field F with Galois group $G(K/F)$. For a field E where $F \leq E \leq K$, let $\lambda(E)$ denote the subgroup of $G(K/F)$ leaving E fixed. For $H \leq G(K/F)$, denote as K_H the field fixed by group H of automorphisms of K. THEN E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. When $\lambda(E)$ is a normal subgroup of $G(K/F)$ then

$$G(E/F) \cong G(K/F)/G(K/E).$$

Note. Now for the proof of Property 5.

Revised: 4/17/2014