Section V.7. Cyclic Extensions

Note. In the last three sections of this chapter we consider specific types of Galois groups of Galois extensions and then study the properties of the associated extension field. In this section we consider cyclic Galois groups. The main results are Proposition V.7.7, Proposition V.7.8, and Theorem V.7.11. We need Lemma V.7.10 and Theorem V.7.11 in the proof of Theorem V.9.4 which in turn leads in Section V.9 to the proof of Galois' big result: Polynomial equation $f(x) = 0$ is solvable by radicals if and only if the Galois group of f is solvable (see Corollary V.9.7).

Definition V.7.1. Let F be a finite dimensional extension field of K and $\overline{K}$ an algebraic closure of K containing F. Let $\sigma_1, \sigma_2, \ldots, \sigma_r$ be all the distinct K-monomorphisms mapping $F \to \overline{K}$. If $u \in F$ then the *norm* of u, denoted ${N_K}^F(u)$ is the element of $\overline{K}$

$$ {N_K}^F(u) = (\sigma_1(u), \sigma_2(u), \ldots, \sigma_r(u))^{[F:K]_i} $$

where $[F : K]_i$ is the inseparable degree of F over K (see Definition V.6.10). The *trace* of u, denoted ${T_K}^F(u)$, is the element of $\overline{K}$

$$ {T_K}^F(u) = [F : K]_i(\sigma_1(u) + \sigma_2(u) + \cdots + \sigma_r(u)). $$

Note. The definition of norm and trace seem to depend on the choice of the algebraic closure of K, $\overline{K}$. However, in Theorem V.7.3 we show that the definition is independent of the choice of $\overline{K}$ (which is not surprising since any two algebraic closures of K are K-isomorphic by Theorem V.3.6).

Note. Exercise V.7.1 states that is, in Definition V.7.1, $\overline{K}$ is replaced by any normal extension N of K which contains F, then the same definition of norm and trace results—in particular, this new definition does not depend on the choice of N. Notice that $\overline{K}$ is a splitting field over K of the set of all (irreducible) polynomials in $K[x]$ by Theorem V.3.4 (the (i)⇒(ii) part) and $\overline{K}$ is then normal over K by Theorem V.3.14 (the (ii)⇒(i) part). Then, by Proposition V.6.12 (notice that F is finite dimensional over K in the definition of norm and trace) the number of K-monomorphisms mapping $F \to N$ (or equivalently, mapping $F \to \overline{K}$ by the above comments) is $r = [F : K]_s$.

Example. In the setting of fields $\mathbb{R}$ and $\mathbb{C}$, we find that the norm is familiar. Let $F = \mathbb{C}$ and $K = \mathbb{R}$. Then $\overline{K} = \overline{\mathbb{R}} = \mathbb{C}$. The only $\mathbb{R}$-monomorphism mapping $\mathbb{C} \to \mathbb{C}$ are the identity $\sigma_1(z) = z$ and complex conjugation $\sigma_2(x) = \overline{z}$. Also, $[F : K]_i = [\mathbb{C} : \mathbb{R}]_i = [\mathbb{C} : \mathbb{S}]$ where S is the largest subfield of $\mathbb{C}$ which is separable over $K = \mathbb{R}$ (so $S = \mathbb{C}$ since every polynomial over $\mathbb{R}$ can be factored into a product of linear terms and irreducible quadratics and hence the only irreducible polynomials over $\mathbb{R}$ are linear or irreducible quadratics and in either case the polynomials are separable [i.e., have roots in $\mathbb{C}$ of multiplicity 1]) and $[F : K]_i = [\mathbb{C} : \mathbb{C}] = 1$. Consequently, denoting ${N_K}^F = {N_\mathbb{R}}^\mathbb{C}$ as simply N, we have

$$N(a + bi) = (\sigma_1(a + bi)(\sigma_2(a + bi))^{[F:K]_i} = ((a + bi)(a - bi))^1 = a^2 + b^2.$$

Note. When F is Galois over K, there is a more concise representation of the norm and trace, as given next.

Theorem V.7.2. If F is a finite dimensional Galois extension field of K and $\text{Aut}_K(F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ then for any $u \in F$,

$$N_K{}^F(u) = \sigma_1(u)\sigma_2(u)\cdots\sigma_n(u); \text{ and}$$

$$T_K{}^F(u) = \sigma_1(u) + \sigma_2(u) + \cdots + \sigma_n(u).$$

Note. Suppose F is Galois over K and $\text{Aut}_K(F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Since $\text{Aut}_K(F)$ is a group, the elements $\sigma_i\sigma_1, \sigma_i\sigma_2, \ldots, \sigma_i\sigma_n$ are simply $\sigma_1, \sigma_2, \ldots, \sigma_n$ in a possible different order (multiplication by σ_i on the left permutes the elements of group $\text{Aut}_K(F)$). So for any $u \in F$, $N_K{}^F(u)$ and $T_K{}^F(u)$ are fixed by every $\sigma_i \in \text{Aut}_K(F)$. but this property implies that $N_K{}^F(u)$ and $T_K^F(u)$ must lie in K. The next result shows that this property holds even if F is not Galois over K. We will use parts (i) and (ii) of the next theorem often, but if we are short on time we might skip parts (iii) and (iv) since these are not used in what follows.

Theorem V.7.3. Let F be a finite dimensional extension field of K. Then for all $u, v \in F$:

(i) $N_K{}^F(u)N_K{}^F(v) = N_K{}^F(uv)$ and $T_K{}^F(u) + T_K{}^F(v) = T_K{}^F(u+v)$;

(ii) if $u \in K$, then $N_K{}^F(u) = u^{[F:K]}$ and $T_K{}^F(u) = [F:K]u$;

(iii) ${N_K}^F(u)$ and ${T_K}^F(u)$ are elements of K. More precisely, ${N_K}^F = ((-1)^n a_0)^{[F:K(u)]} \in K$ and ${T_K}^F(u) = -[F : K(u)]a_{n-1} \in K$, where a_0 and a_{n-1} are determined by $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ is the irreducible polynomial of u;

(iv) if E is an intermediate field, then ${N_K}^E({N_E}^F(u)) = {N_K}^F(u)$ and ${T_K}^E({T_E}^F(u)) = {T_K}^F(u)$.

Definition V.7.4. Let S be a nonempty set of automorphisms of a field F. S is *linearly independent* provided that for any $a_1, a_2, \ldots, a_n \in F$ and $\sigma_1, \sigma_2, \ldots, \sigma_n \in S$ we have

$$a_1\sigma_1(u) + a_2\sigma_2(u) + \cdots + a_n\sigma(u) = 0 \text{ for all } u \in F$$

implies that $a_i = 0$ for all i.

Lemma V.7.5. If S is a set of distinct automorphisms of a field F, then S is linearly independent.

Definition. An extension field F of a field K is said to be *cyclic* (respectively, *abelian*) if F is algebraic and Galois over K and $\mathrm{Aut}_K(F)$ is a cyclic (respectively, abelian) group. If in this situation $\mathrm{Aut}_K(F)$ is a finite cyclic group of order n, then F is a *cyclic extension of degree* n (notice that $[F : K] = n$ by the Fundamental Theorem of Galois Theory, Theorem V.2.5 part (i)).

Note. The next result gives some properties of cyclic extensions in terms of the norm and trace.

Theorem V.7.6. Let F be a cyclic extension field of degree n, σ a generator of $\text{Aut}_K(F)$ and $u \in F$. Then

(i) ${T_K}^F(u) = 0$ if and only if $u = v - \sigma(v)$ for some $v \in F$;

(ii) (Hilbert's Theorem 90) ${N_K}^F(u) = 1_K$ if and only if $u = v\sigma^{-1}(v)$ for some nonzero $v \in F$.

Note. The reference to Theorem V.7.6(ii) as "Hilbert's Theorem 90" is based on the fact that it was Theorem 90 of David Hilbert's (1862–1943) *Die Theorie der algebraischen Zahlkörper* in 1897. An English translation appears as *The Theory of Algebraic Number Fields* in 1998 by Springer-Verlag. See page 105 in Chapter 15, "Cyclic Extension Fields of Prime Degree," Section 54, "Symbolic Powers. Theorem on Numbers with Relative Norm 1." However, the result was originally shown by Ernst Kummer (1810–1893) in 1855 and published in 1861 (reprinted in Kummer's *Collected papers. Volume 1: Contributions to Number Theory*, edited by André Weil, Springer-Verlag (1975), pages 699–839). A number of generalizations exist, including in the settings of group cohomology (a generalization by Emmy Noether) and Milnor K-Theory. (These comments are based on the website: https://en.wikipedia.org/wiki/Hilbert's_Theorem_90, accessed 7/3/2015.)

Note. We now use the results developed in this section to characterize some cyclic field extensions.

Proposition V.7.7. Let F be a cyclic extension field of K of degree n and suppose $n = mp^t$ where $0 \neq p = \text{char}(K)$ and $(m, p) = 1$. Then there is a chain of intermediate fields $F \supset E_0 \supset E_1 \supset \cdots \supset E_{t-1} \supset E_t = K$ such that F is a cyclic extension of E_0 of degree m and for each $0 \leq i \leq t$, E_{i-1} is a cyclic extension of E_i of degree p.

Note. Proposition V.7.7 allows us to reduce the analysis of cyclic extensions F of degree n over K to just two cases:

(i) $n = \text{char}(K) = p \neq 0$ (in which case $t = 0$ in Proposition V.7.7), and

(ii) $\text{char}(K) = 0$ or $\text{char}(K) = p \neq 0$ and $(p, n) = 1$ (that is, $\text{char}(K) \nmid n$).

The first case is treated next.

Proposition V.7.8. Let K be a field of characteristic $p \neq 0$. F is a cyclic extension field of K of degree p if and only if F is a splitting field over K of an irreducible polynomial of the form $x^p - x - a \in K[x]$. In this case $F = K(u)$ where u is any root of $x^p - x - a$.

Corollary V.7.9. If K is a field of characteristic $p \neq 0$ and $x^p - x - a \in K[x]$, then $x^p - x - a$ is either irreducible of splits in $K[x]$.

Note. In the notation of Proposition V.7.7, we have that all fields F which are cyclic extension fields of K where $n = \text{char}(K) = p$ are splitting fields of irreducible $x^p - x - a$, and conversely (by Proposition V.7.8). This still leaves the classification of cyclic extensions where either $\text{char}(K) = 0$ or $\text{hcar}(K) = p \neq 0$ and $(p, n) = 1$. For this second classification we must introduce an additional assumption on field K.

Definition. Let K be a field and $n \in \mathbb{N}$. An element $\zeta \in K$ is an *nth root of unity* if $\zeta^n = 1_K$ (that is, ζ is a root of $x^n - 1_K$). $\zeta \in K$ is a *primitive nth root of unity* if ζ is an nth root of unity and ζ has order n in the multiplicative group of nth roots of unity. (Notice that a primitive nth root of unity generates the cyclic group of all nth roots of unity.)

Example. For $n \in \mathbb{N}$, the group of nth roots of unity in $\mathbb{C}$ is $\{e^{2k\pi i/n} \mid k = 0, 1, 2, \ldots, n-1\}$. The primitive nth roots of unity in $\mathbb{C}$ are $e^{2k\pi i/n}$ where k and n are relatively prime, $(k, n) = 1$. Of course, this multiplicative group is isomorphic to the additive group $\mathbb{Z}_n$.

Note. Roots of unity can be more abstract than the previous example might lead us to believe. If $\text{char}(K) = p$ and $p \mid n$ then $n = p^k m$ with $(p, m) = 1$ and $m < n$ (by the Division Algorithm). Thus $x^n - 1_K = (x^m - 1_K)^{p^k}$ (by the Freshman's Dream, Exercise III.1.11). Consequently the nth roots of unity in K coincide with the mth roots of unity in K. Since $m < n$ there can be no primitive nth root of unity in K (because all mth roots of unity are of order at most m).

Note. We need one final result before we classify cyclic extensions of fields which contain nth roots of unity. The next result will also be used in the proof of Theorem V.9.4 which concerns radical extensions and solvable groups.

Lemma V.7.10. Let $n \in \mathbb{N}$ and K a field which contains a primitive nth root of unity ζ.

(i) If $d \mid n$, then $\zeta^{n/d} = \eta$ is a primitive dth root of unity in K.

(ii) If $d \mid n$ and u is a nonzero root of $x^d - a \in K[x]$, then $x^d - a$ had d distinct roots, namely $u, \eta u, \eta^2 u, \ldots, \eta^{d-1} u$, where $\eta \in K$ is a primitive dth root of unity. Furthermore $K(u)$ is a splitting field of $x^d - a$ over K and is Galois over K.

Note. The following result puts no condition on $\text{char}(K)$, and so addresses the second category of cyclic extensions. However, it does require the additional assumption that K contains a primitive root of unity. The next result will be used in the proof of Theorem V.9.4 which concerns radical extensions and solvable groups.

Theorem V.7.11. Let $n \in \mathbb{N}$ and K a field which contains a primitive nth root of unity ζ. Then the following conditions on an extension field F of K are equivalent.

(i) F is cyclic of degree d, where $d \mid n$;

(ii) F is a splitting field over K of a polynomial of the form $x^n - a \in K[x]$ (in which case $F = K(u)$, for any root u of $x^n - a$);

(iii) F is a splitting field over K of an irreducible polynomial of the form $x^d - b \in K[x]$, where $d \mid n$ (in which case $F = K(v)$, for any root v of $x^d - b$).

Note. Instead of viewing Theorem V.7.11 as a classification of cyclic extensions, we could view it as a classification of splitting fields of polynomials of the form $x^n - a$ (in terms of cyclic extensions in the setting of fields containing a primitive root of unity). Without the presence of the primitive root this is "considerably more difficult" (Hungerford, page 296). The content of the next section addresses this question in the case when $a = 1_K$.

Revised: 12/30/2015