

CHAPTER 6 GALOIS THEORY

6.1 Fixed Fields and Galois Groups

Galois theory is based on a remarkable correspondence between subgroups of the Galois group of an extension E/F and intermediate fields between E and F . In this section we will set up the machinery for the fundamental theorem. [A remark on notation: Throughout the chapter, the composition $\tau \circ \sigma$ of two automorphisms will be written as a product $\tau\sigma$.]

6.1.1 Definitions and Comments Let $G = \text{Gal}(E/F)$ be the Galois group of the extension E/F . If H is a subgroup of G , the *fixed field* of H is the set of elements fixed by every automorphism in H , that is,

$$\mathcal{F}(H) = \{x \in E : \sigma(x) = x \text{ for every } \sigma \in H\}.$$

If K is an intermediate field, that is, $F \leq K \leq E$, define

$$\mathcal{G}(K) = \text{Gal}(E/K) = \{\sigma \in G : \sigma(x) = x \text{ for every } x \in K\}.$$

I like the term “*fixing group of K*” for $\mathcal{G}(K)$, since $\mathcal{G}(K)$ is the group of automorphisms of E that leave K fixed. Galois theory is about the relation between fixed fields and fixing groups. In particular, the next result suggests that the smallest subfield F corresponds to the largest subgroup G .

6.1.2 Proposition Let E/F be a finite Galois extension with Galois group $G = \text{Gal}(E/F)$. Then

- (i) The fixed field of G is F ;
- (ii) If H is a proper subgroup of G , then the fixed field of H properly contains F .

Proof.

(i) Let F_0 be the fixed field of G . If σ is an F_0 -automorphism of E , then by definition of F_0 , σ fixes everything in F_0 . Thus the F_0 -automorphisms of E coincide with the G -automorphisms of E . Now by (3.4.7) and (3.5.8), E/F_0 is Galois. By (3.5.9), the size of the Galois group of a finite Galois extension is the degree of the extension. Thus $[E : F_0] = [E : F]$, so by (3.1.9), $F = F_0$.

(ii) Suppose that $F = \mathcal{F}(H)$. By the theorem of the primitive element (3.5.12), we have $E = F(\alpha)$ for some $\alpha \in E$. Define a polynomial $f(X) \in E[X]$ by

$$f(X) = \prod_{\sigma \in H} (X - \sigma(\alpha)).$$

If τ is any automorphism in H , then we may apply τ to f (that is, to the coefficients of f ; we discussed this idea in the proof of (3.5.2)). The result is

$$(\tau f)(X) = \prod_{\sigma \in H} (X - (\tau\sigma)(\alpha)).$$

But as σ ranges over all of H , so does $\tau\sigma$, and consequently $\tau f = f$. Thus each coefficient of f is fixed by H , so $f \in F[X]$. Now α is a root of f , since $X - \sigma(\alpha)$ is 0 when $X = \alpha$ and σ is the identity. We can say two things about the degree of f :

(1) By definition of f , $\deg f = |H| < |G| = [E : F]$, and, since f is a multiple of the minimal polynomial of α over F ,

(2) $\deg f \geq [F(\alpha) : F] = [E : F]$,

and we have a contradiction. ♣

There is a converse to the first part of (6.1.2).

6.1.3 Proposition Let E/F be a finite extension with Galois group G . If the fixed field of G is F , then E/F is Galois.

Proof. Let $G = \{\sigma_1, \dots, \sigma_n\}$, where σ_1 is the identity. To show that E/F is normal, we consider an irreducible polynomial $f \in F[X]$ with a root $\alpha \in E$. Apply each automorphism in G to α , and suppose that

there are r distinct images $\alpha = \alpha_1 = \sigma_1(\alpha), \alpha_2 = \sigma_2(\alpha), \dots, \alpha_r = \sigma_r(\alpha)$. If σ is any member of G , then σ will map each α_i to some α_j , and since σ is an injective map of the finite set $\{\alpha_1, \dots, \alpha_r\}$ to itself, it is surjective as well. To put it simply, σ permutes the α_i . Now we examine what σ does to the *elementary symmetric functions* of the α_i , which are given by

$$e_1 = \sum_{i=1}^n \alpha_i, \quad e_2 = \sum_{i < j} \alpha_i \alpha_j, \quad e_3 = \sum_{i < j < k} \alpha_i \alpha_j \alpha_k, \dots,$$

$$e_r = \prod_{i=1}^r \alpha_i.$$

Since σ permutes the α_i , it follows that $\sigma(e_i) = e_i$ for all i . Thus the e_i belong to the fixed field of G , which is F by hypothesis. Now we form a monic polynomial whose roots are the α_i :

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_r) = X^r - e_1 X^{r-1} + e_2 X^{r-2} - \cdots + (-1)^r e_r.$$

Since the e_i belong to F , $g \in F[X]$, and since the α_i are in E , g splits over E . We claim that g is the minimal polynomial of α over F . To see this, let $h(X) = b_0 + b_1 X + \cdots + b_m X^m$ be any polynomial in $F[X]$ having α as a root. Applying σ_i to the equation

$$b_0 + b_1 \alpha + \cdots + b_m \alpha^m = 0$$

we have

$$b_0 + b_1 \alpha_i + \cdots + b_m \alpha_i^m = 0,$$

so that each α_i is a root of h , hence g divides h and therefore $g = \min(\alpha, F)$. But our original polynomial $f \in F[X]$ is irreducible and has α as a root, so it must be a constant multiple of g . Consequently, f splits over E , proving that E/F is normal. Since the $\alpha_i, i = 1, \dots, r$, are distinct, g has no repeated roots. Thus α is separable over F , which shows that the extension E/F is separable. ♣

It is profitable to examine elementary symmetric functions in more detail.

6.1.4 Theorem Let f be a symmetric polynomial in the n variables X_1, \dots, X_n . [This means that if σ is any permutation in S_n and we replace X_i by $X_{\sigma(i)}$ for $i = 1, \dots, n$, then f is unchanged.] If e_1, \dots, e_n are the elementary symmetric functions of the X_i , then f can be expressed as a polynomial in the e_i .

Proof. We give an algorithm. The polynomial f is a linear combination of monomials of the form $X_1^{r_1} \cdots X_n^{r_n}$, and we order the monomials lexicographically: $X_1^{r_1} \cdots X_n^{r_n} > X_1^{s_1} \cdots X_n^{s_n}$ iff the first disagreement between r_i and s_i results in $r_i > s_i$. Since f is symmetric, all terms generated by applying a permutation $\sigma \in S_n$ to the subscripts of $X_1^{r_1} \cdots X_n^{r_n}$ will also contribute to f . The idea is to cancel the leading terms (those associated with the monomial that is first in the ordering) by subtracting an expression of the form

$$e_1^{t_1} e_2^{t_2} \cdots e_n^{t_n} = (X_1 + \cdots + X_n)^{t_1} \cdots (X_1 \cdots X_n)^{t_n}$$

which has leading term

$$X_1^{t_1} (X_1 X_2)^{t_2} (X_1 X_2 X_3)^{t_3} \cdots (X_1 \cdots X_n)^{t_n} = X_1^{t_1 + \cdots + t_n} X_2^{t_2 + \cdots + t_n} \cdots X_n^{t_n}.$$

This will be possible if we choose

$$t_1 = r_1 - r_2, \quad t_2 = r_2 - r_3, \quad \dots, \quad t_{n-1} = r_{n-1} - r_n, \quad t_n = r_n.$$

After subtraction, the resulting polynomial has a leading term that is below $X_1^{r_1} \cdots X_n^{r_n}$ in the lexicographical ordering. We can then repeat the procedure, which must terminate in a finite number of steps. ♣

6.1.5 Corollary If g is a polynomial in $F[X]$ and $f(\alpha_1, \dots, \alpha_n)$ is any symmetric polynomial in the roots $\alpha_1, \dots, \alpha_n$ of g , then $f \in F[X]$.

Proof. We may assume without loss of generality that g is monic. Then in a splitting field of g we have

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_n) = X^n - e_1 X^{n-1} + \cdots + (-1)^n e_n.$$

By (6.1.4), f is a polynomial in the e_i , and since the e_i are simply \pm the coefficients of g , the coefficients of f are in F . ♣

6.1.6 Dedekind's Lemma The result that the size of the Galois group of a finite Galois extension is the degree of the extension can be proved via Dedekind's lemma, which is of interest in its own right. Let G be a group and E a field. A *character* from G to E is a homomorphism from G to the multiplicative group E^* of nonzero elements of E . In particular, an automorphism of E defines a character with $G = E^*$, as does a monomorphism of E into a field L . Dedekind's lemma states that if $\sigma_1, \dots, \sigma_n$ are distinct characters from G to E , then the σ_i are linearly independent over E . The proof is given in Problems 3 and 4.

Problems For Section 6.1

- Express $X_1^2 X_2 X_3 + X_1 X_2^2 X_3 + X_1 X_2 X_3^2$ in terms of elementary symmetric functions.
- Repeat Problem 1 for $X_1^2 X_2 + X_1^2 X_3 + X_1 X_2^2 + X_1 X_3^2 + X_2^2 X_3 + X_2 X_3^2 + 4X_1 X_2 X_3$.
- To begin the proof of Dedekind's lemma, suppose that the σ_i are linearly dependent. By renumbering the σ_i if necessary, we have

$$a_1 \sigma_1 + \cdots + a_r \sigma_r = 0$$

where all a_i are nonzero and r is as small as possible. Show that for every h and $g \in G$, we have

$$\sum_{i=1}^r a_i \sigma_1(h) \sigma_i(g) = 0 \tag{1}$$

and

$$\sum_{i=1}^r a_i \sigma_i(h) \sigma_i(g) = 0. \tag{2}$$

[Equations (1) and (2) are not the same; in (1) we have $\sigma_1(h)$, not $\sigma_i(h)$.]

- Continuing Problem 3, subtract (2) from (1) to get

$$\sum_{i=1}^r a_i (\sigma_1(h) - \sigma_i(h)) \sigma_i(g) = 0. \tag{3}$$

With g arbitrary, reach a contradiction by an appropriate choice of h .

- If G is the Galois group of $\mathbb{Q}(\sqrt[3]{2})$ over \mathbb{Q} , what is the fixed field of G ?
- Find the Galois group of \mathbb{C}/\mathbb{R} .
- Find the fixed field of the Galois group of Problem 6.

6.2 The Fundamental Theorem

With the preliminaries now taken care of, we can proceed directly to the main result.

6.2.1 Fundamental Theorem of Galois Theory Let E/F be a finite Galois extension with Galois group G . If H is a subgroup of G , let $\mathcal{F}(H)$ be the fixed field of H , and if K is an intermediate field, let $\mathcal{G}(K)$ be $\text{Gal}(E/K)$, the fixing group of K (see (6.1.1)).

- \mathcal{F} is a bijective map from subgroups to intermediate fields, with inverse \mathcal{G} . Both maps are inclusion-reversing, that is, if $H_1 \leq H_2$ then $\mathcal{F}(H_1) \geq \mathcal{F}(H_2)$, and if $K_1 \leq K_2$, then $\mathcal{G}(K_1) \geq \mathcal{G}(K_2)$.
- Suppose that the intermediate field K corresponds to the subgroup H under the Galois correspondence. Then
 - E/K is always normal (hence Galois);
 - K/F is normal if and only if H is a normal subgroup of G , and in this case,
 - the Galois group of K/F is isomorphic to the quotient group G/H . Moreover, whether or not K/F is

normal,

$$(d) [K : F] = [G : H] \text{ and } [E : K] = |H|.$$

(3) If the intermediate field K corresponds to the subgroup H and σ is any automorphism in G , then the field $\sigma K = \{\sigma(x) : x \in K\}$ corresponds to the conjugate subgroup $\sigma H \sigma^{-1}$. For this reason, σK is called a *conjugate subfield* of K .

The following diagram may aid the understanding.

$$\begin{array}{ccc} E & & G \\ | & & | \\ K & & H \\ | & & | \\ F & & 1 \end{array}$$

As we travel up the left side from smaller to larger fields, we move down the right side from larger to smaller groups. A statement about K/F , an extension at the bottom of the left side, corresponds to a statement about G/H , located at the top of the right side. Similarly, a statement about E/K corresponds to a statement about $H/1 = H$.

Proof.

(1) First, consider the composite mapping $H \rightarrow \mathcal{F}(H) \rightarrow \mathcal{GF}(H)$. If $\sigma \in H$ then σ fixes $\mathcal{F}(H)$ by definition of fixed field, and therefore $\sigma \in \mathcal{GF}(H) = \text{Gal}(E/\mathcal{F}(H))$. Thus $H \subseteq \mathcal{GF}(H)$. If the inclusion is proper, then by (6.1.2) part (ii) with F replaced by $\mathcal{F}(H)$, we have $\mathcal{F}(H) > \mathcal{F}(H)$, a contradiction. [Note that E/K is a Galois extension for any intermediate field K , by (3.4.7) and (3.5.8).] Thus $\mathcal{GF}(H) = H$.

Now consider the mapping $K \rightarrow \mathcal{G}(K) \rightarrow \mathcal{FG}(K) = \mathcal{FGal}(E/K)$. By (6.1.2) part (i) with F replaced by K , we have $\mathcal{FG}(K) = K$. Since both \mathcal{F} and \mathcal{G} are inclusion-reversing by definition, the proof of (1) is complete.

(3) The fixed field of $\sigma H \sigma^{-1}$ is the set of all $x \in E$ such that $\sigma \tau \sigma^{-1}(x) = x$ for every $\tau \in H$. Thus

$$\mathcal{F}(\sigma H \sigma^{-1}) = \{x \in E : \sigma^{-1}(x) \in \mathcal{F}(H)\} = \sigma(\mathcal{F}(H)).$$

(2a) This was observed in the proof of (1).

(2b) If σ is an F -monomorphism of K into E , then by (3.5.2) and (3.5.6), σ extends to an F -monomorphism of E into itself, in other words (see (3.5.6)), an F -automorphism of E . Thus each such σ is the restriction to K of a member of G . Conversely, the restriction of an automorphism in G to K is an F -monomorphism of K into E . By (3.5.5) and (3.5.6), K/F is normal iff for every $\sigma \in G$ we have $\sigma(K) = K$. But by (3), $\sigma(K)$ corresponds to $\sigma H \sigma^{-1}$ and K to H . Thus K/F is normal iff $\sigma H \sigma^{-1} = H$ for every $\sigma \in G$, i.e., $K \trianglelefteq G$.

(2c) Consider the homomorphism of $G = \text{Gal}(E/F)$ to $\text{Gal}(K/F)$ given by $\sigma \rightarrow \sigma|_K$. The map is surjective by the argument just given in the proof of (2b). The kernel is the set of all automorphisms in G that restrict to the identity on K , that is, $\text{Gal}(E/K) = H$. The result follows from the first isomorphism theorem.

(2d) By (3.1.9), $[E : F] = [E : K][K : F]$. The term on the left is $|G|$ by (3.5.9), and the first term on the right is $|\text{Gal}(E/K)|$ by (2a), and this in turn is $|H|$ since $H = \mathcal{G}(K)$. Thus $|G| = |H|[K : F]$, and the result follows from Lagrange's theorem. [If K/F is normal, the proof is slightly faster. The first statement follows from (2c). To prove the second, note that by (3.1.9) and (3.5.9),

$$[E : K] = \frac{[E : F]}{[K : F]} = \frac{|G|}{|G/H|} = |H|. \clubsuit$$

The next result is reminiscent of the second isomorphism theorem, and is best visualized via the diamond diagram of Figure 6.2.1. In the diagram, EK is the *composite* of the two fields E and K , that is, the smallest field containing both E and K .

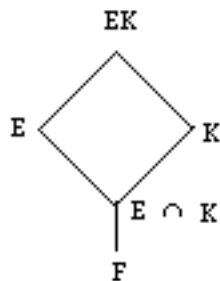


Figure 6.2.1

6.2.2 Theorem Let E/F be a finite Galois extension and K/F an arbitrary extension. Assume that E and K are both contained in a common field, so that it is sensible to consider the composite EK . Then

- (1) EK/K is a finite Galois extension;
- (2) $\text{Gal}(EK/K)$ is embedded in $\text{Gal}(E/F)$, where the embedding is accomplished by restricting automorphisms in $\text{Gal}(EK/K)$ to E ;
- (3) The embedding is an isomorphism if and only if $E \cap K = F$.

Proof.

(1) By the theorem of the primitive element (3.5.12), we have $E = F[\alpha]$ for some $\alpha \in E$, so $EK = KF[\alpha] = K[\alpha]$. The extension $K[\alpha]/K$ is finite because α is algebraic over F , hence over K . Since α , regarded as an element of EK , is separable over F and hence over K , it follows that EK/K is separable. [To avoid breaking the main line of thought, this result will be developed in the exercises (see Problems 1 and 2).]

Now let f be the minimal polynomial of α over F , and g the minimal polynomial of α over K . Since $f \in K[X]$ and $f(\alpha) = 0$, we have $g|f$, and the roots of g must belong to $E \subseteq EK = K[\alpha]$ because E/F is normal. Therefore $K[\alpha]$ is a splitting field for g over K , so by (3.5.7), $K[\alpha]/K$ is normal.

(2) If σ is an automorphism in $\text{Gal}(EK/K)$, restrict σ to E , thus defining a homomorphism from $\text{Gal}(EK/K)$ to $\text{Gal}(E/F)$. (Note that $\sigma|_E$ is an automorphism of E because E/F is normal.) Now σ fixes K , and if σ belongs to the kernel of the homomorphism, then σ also fixes E , so σ fixes $EK = K[\alpha]$. Thus σ is the identity, and the kernel is trivial, proving that the homomorphism is actually an embedding.

(3) The embedding of (2) maps $\text{Gal}(EK/K)$ to a subgroup H of $\text{Gal}(E/F)$, and we will find the fixed field of H . By (6.1.2), the fixed field of $\text{Gal}(EK/K)$ is K , and since the embedding just restricts automorphisms to E , the fixed field of H must be $E \cap K$. By the fundamental theorem, $H = \text{Gal}(E/(E \cap K))$. Thus

$$H = \text{Gal}(E/F) \text{ iff } \text{Gal}(E/(E \cap K)) = \text{Gal}(E/F),$$

and by applying the fixed field operator \mathcal{F} , we see that this happens if and only if $E \cap K = F$. ♣

Problems For Section 6.2

1. Let $E = F(\alpha_1, \dots, \alpha_n)$, where each α_i is algebraic and separable over F . We are going to show that E is separable over F . Without loss of generality, we can assume that the characteristic of F is a prime p , and since F/F is separable, the result holds for $n = 0$. To carry out the inductive step, let $E_i = F(\alpha_1, \dots, \alpha_i)$, so that $E_{i+1} = E_i(\alpha_{i+1})$. Show that $E_{i+1} = E_i(E_{i+1}^p)$. (See Section 3.4, Problems 4-8, for the notation.)
2. Continuing Problem 1, show that E is separable over F .
3. Let $E = F(\alpha_1, \dots, \alpha_n)$, where each α_i is algebraic over F . If for each $i = 1, \dots, n$, all the conjugates of α_i (the roots of the minimal polynomial of α_i over F) belong to E , show that E/F is normal.
4. Suppose that $F = K_0 \leq K_1 \leq \dots \leq K_n = E$, where E/F is a finite Galois extension, and that the intermediate field K_i corresponds to the subgroup H_i under the Galois correspondence. Show that K_i/K_{i-1} is normal (hence Galois) if and only if $H_i \trianglelefteq H_{i-1}$, and in this case, $\text{Gal}(K_i/K_{i-1})$ is isomorphic to H_{i-1}/H_i .
5. Let E and K be extensions of F , and assume that the composite EK is defined. If A is any set of generators for K over F (for example, $A = K$), show that $EK = E(A)$, the field formed from E by adjoining the elements of A .

6. Let E/F be a finite Galois extension with Galois group G , and let E'/F' be a finite Galois extension with Galois group G' . If τ is an isomorphism of E and E' with $\tau(F) = F'$, we expect intuitively that $G \cong G'$. Prove this formally.
7. Let K/F be a finite separable extension. Although K need not be a normal extension of F , we can form the normal closure N of K over F , as in (3.5.11). Then N/F is a Galois extension (see Problem 8 of Section 6.3); let G be its Galois group. Let $H = \text{Gal}(N/K)$, so that the fixed field of H is K . If H' is a normal subgroup of G that is contained in H , show that the fixed field of H' is N .
8. Continuing Problem 7, show that H' is trivial, and conclude that

$$\bigcap_{g \in G} gHg^{-1} = \{1\}$$

where 1 is the identity automorphism.

6.3 Computing a Galois Group Directly

6.3.1 Definitions and Comments Suppose that E is a splitting field of the separable polynomial f over F . The *Galois group of f* is the Galois group of the extension E/F . (The extension is indeed Galois; see Problem 8.) Given f , how can we determine its Galois group? It is not so easy, but later we will develop a systematic approach for polynomials of degree 4 or less. Some cases can be handled directly, and in this section we look at a typical situation. A useful observation is that the Galois group G of a finite Galois extension E/F acts *transitively* on the roots of any irreducible polynomial $h \in F[X]$ (assuming that one, hence every, root of h belongs to E). [Each $\sigma \in G$ permutes the roots by (3.5.1). If α and β are roots of h , then by (3.2.3) there is an F -isomorphism of $F(\alpha)$ and $F(\beta)$ carrying α to β . This isomorphism can be extended to an F -automorphism of E by (3.5.2), (3.5.5) and (3.5.6).]

6.3.2 Example Let d be a positive integer that is not a perfect cube, and let θ be the positive cube root of d . Let $\omega = e^{i2\pi/3} = -\frac{1}{2} + i\frac{1}{2}\sqrt{3}$, so that $\omega^2 = e^{-i2\pi/3} = -\frac{1}{2} - i\frac{1}{2}\sqrt{3} = -(1 + \omega)$. The minimal polynomial of θ over the rationals \mathbb{Q} is $f(X) = X^3 - d$, because if f were reducible then it would have a linear factor and d would be a perfect cube. The minimal polynomial of ω over \mathbb{Q} is $g(X) = X^2 + X + 1$. (If g were reducible, it would have a rational (hence real) root, so the discriminant would be nonnegative, a contradiction.) We will compute the Galois group G of the polynomial $f(X)g(X)$, which is the Galois group of $E = \mathbb{Q}(\theta, \omega)$ over \mathbb{Q} .

If the degree of E/\mathbb{Q} is the product of the degrees of f and g , we will be able to make progress. We have $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$ and, since ω , a complex number, does not belong to $\mathbb{Q}(\theta)$, we have $[\mathbb{Q}(\theta, \omega) : \mathbb{Q}(\theta)] = 2$. Thus $[\mathbb{Q}(\theta, \omega) : \mathbb{Q}] = 6$. But the degree of a finite Galois extension is the size of the Galois group by (3.5.9), so G has exactly 6 automorphisms. Now any $\sigma \in G$ must take θ to one of its conjugates, namely $\theta, \omega\theta$ or $\omega^2\theta$. Moreover, σ must take ω to a conjugate, namely ω or ω^2 . Since σ is determined by its action on θ and ω , we have found all 6 members of G . The results can be displayed as follows.

$$1 : \theta \rightarrow \theta, \omega \rightarrow \omega, \text{ order} = 1$$

$$\tau : \theta \rightarrow \theta, \omega \rightarrow \omega^2, \text{ order} = 2$$

$$\sigma : \theta \rightarrow \omega\theta, \omega \rightarrow \omega, \text{ order} = 3$$

$$\sigma\tau : \theta \rightarrow \omega\theta, \omega \rightarrow \omega^2, \text{ order} = 2$$

$$\sigma^2 : \theta \rightarrow \omega^2\theta, \omega \rightarrow \omega, \text{ order} = 3$$

$$\tau\sigma : \theta \rightarrow \omega^2\theta, \omega \rightarrow \omega^2, \text{ order} = 2$$

Note that $\tau\sigma^2$ gives nothing new since $\tau\sigma^2 = \sigma\tau$. Similarly, $\sigma^2\tau = \tau\sigma$. Thus

$$\sigma^3 = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} (= \sigma^2). \quad (1)$$

At this point we have determined the multiplication table of G , but much more insight is gained by observing that (1) gives a presentation of S_3 (Section 5.8, Problem 3). We conclude that $G \cong S_3$. The subgroups of G are

$$\{1\}, G, \langle \sigma \rangle, \langle \tau \rangle, \langle \tau\sigma \rangle, \langle \tau\sigma^2 \rangle$$

and the corresponding fixed fields are

$$E, \mathbb{Q}, \mathbb{Q}(\omega), \mathbb{Q}(\theta), \mathbb{Q}(\omega\theta), \mathbb{Q}(\omega^2\theta).$$

To show that the fixed field of $\langle \tau\sigma \rangle = \{1, \tau\sigma\}$ is $\mathbb{Q}(\omega\theta)$, note that $\langle \tau\sigma \rangle$ has index 3 in G , so by the fundamental theorem, the corresponding fixed field has degree 3 over \mathbb{Q} . Now $\tau\sigma$ takes $\omega\theta$ to $\omega^2\omega^2\theta = \omega\theta$ and $[\mathbb{Q}(\omega\theta) : \mathbb{Q}] = 3$ (because the minimal polynomial of $\omega\theta$ over \mathbb{Q} is f). Thus $\mathbb{Q}(\omega\theta)$ is the entire fixed field. The other calculations are similar.

Problems For Section 6.3

1. Suppose that $E = F(\alpha)$ is a finite Galois extension of F , where α is a root of the irreducible polynomial $f \in F[X]$. Assume that the roots of f are $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$. Describe, as best you can from the given information, the Galois group of E/F .
2. Let E/\mathbb{Q} be a finite Galois extension, and let x_1, \dots, x_n be a basis for E over \mathbb{Q} . Describe how you would find a primitive element, that is, an $\alpha \in E$ such that $E = \mathbb{Q}(\alpha)$. (Your procedure need not be efficient.)
3. Let G be the Galois group of a separable irreducible polynomial f of degree n . Show that G is isomorphic to a transitive subgroup H of S_n . [Transitivity means that if i and j belong to $\{1, 2, \dots, n\}$, then for some $\sigma \in H$ we have $\sigma(i) = j$. Equivalently, the *natural action* of H on $\{1, \dots, n\}$, given by $h \bullet x = h(x)$, is transitive.]
4. Use Problem 3 to determine the Galois group of an irreducible quadratic polynomial $aX^2 + bX + c \in F[X], a \neq 0$. Assume that the characteristic of F is not 2, so that the derivative of f is nonzero and f is separable.
5. Determine the Galois group of $(X^2 - 2)(X^2 - 3)$ over \mathbb{Q} .
6. In the Galois correspondence, suppose that K_i is the fixed field of the subgroup H_i , $i = 1, 2$. Identify the group corresponding to $K = K_1 \cap K_2$.
7. Continuing Problem 6, identify the fixed field of $H_1 \cap H_2$.
8. Suppose that E is a splitting field of a separable polynomial f over F . Show that E/F is separable. [Since the extension is finite by (3.2.2) and normal by (3.5.7), E/F is Galois.]
9. Let G be the Galois group of $f(X) = X^4 - 2$ over \mathbb{Q} . Thus if θ is the positive fourth root of 2, then G is the Galois group of $\mathbb{Q}(\theta, i)/\mathbb{Q}$. Describe all 8 automorphisms in G .
10. Show that G is isomorphic to the dihedral group D_8 .
11. Define $\sigma(\theta) = i\theta, \sigma(i) = i, \tau(\theta) = \theta, \tau(i) = -i$, as in the solution to Problem 10. Find the fixed field of the normal subgroup $N = \{1, \sigma\tau, \sigma^2, \sigma^3\tau\}$ of G , and verify that the fixed field is a normal extension of \mathbb{Q} .

6.4 Finite Fields

Finite fields can be classified precisely. We will show that a finite field must have p^n elements, where p is a prime and n is a positive integer. In addition, there is (up to isomorphism) only one finite field with p^n elements. We sometimes use the notation $GF(p^n)$ for this field; GF stands for “Galois field”. Also, the field with p elements will be denoted by \mathbb{F}_p rather than \mathbb{Z}_p , to emphasize that we are working with fields.

6.4.1 Proposition Let E be a finite field of characteristic p . Then $|E| = p^n$ for some positive integer n . Moreover, E is a splitting field for the separable polynomial $f(X) = X^{p^n} - X$ over \mathbb{F}_p , so that any finite field with p^n elements is isomorphic to E . Not only is E generated by the roots of f , but in fact E coincides with the set of roots of f .

Proof. Since E contains a copy of \mathbb{F}_p (see (2.1.3), Example 2), we may view E as a vector space over \mathbb{F}_p . If the dimension of this vector space is n , then since each coefficient in a linear combination of basis vectors can be chosen in p ways, we have $|E| = p^n$.

Now let E^* be the multiplicative group of nonzero elements of E . If $\alpha \in E^*$, then $\alpha^{p^n-1} = 1$ by Lagrange’s theorem, so $\alpha^{p^n} = \alpha$ for every $\alpha \in E$, including $\alpha = 0$. Thus each element of E is a root of f , and f is separable by (3.4.5). Now f has at most p^n distinct roots, and as we have already identified the p^n elements of E as roots of f , in fact f has p^n distinct roots and every root of f must belong to E . ♣

6.4.2 Corollary If E is a finite field of characteristic p , then E/\mathbb{F}_p is a Galois extension. The Galois group is cyclic and is generated by the Frobenius automorphism $\sigma(x) = x^p, x \in E$.

Proof. E is a splitting field of a separable polynomial over \mathbb{F}_p , so E/\mathbb{F}_p is Galois; see (6.3.1). Since $x^p = x$ for each $x \in \mathbb{F}_p$, \mathbb{F}_p is contained in the fixed field $\mathcal{F}(\langle \sigma \rangle)$. But each element of the fixed field is a root of $X^p - X$, so $\mathcal{F}(\langle \sigma \rangle)$ has at most p elements. Consequently, $\mathcal{F}(\langle \sigma \rangle) = \mathbb{F}_p$. Now $\mathbb{F}_p = \mathcal{F}(\text{Gal}(E/\mathbb{F}_p))$ by (6.1.2), so by the fundamental theorem, $\text{Gal}(E/\mathbb{F}_p) = \langle \sigma \rangle$. ♣

6.4.3 Corollary Let E/F be a finite extension of a finite field, with $|E| = p^n$, $|F| = p^m$. Then E/F is a Galois extension. Moreover, m divides n , and $\text{Gal}(E/F)$ is cyclic and is generated by the automorphism $\tau(x) = x^{p^m}$, $x \in E$. Furthermore, F is the only subfield of E of size p^m .

Proof. If the degree of E/F is d , then as in (6.4.1), $(p^m)^d = p^n$, so $d = n/m$ and $m|n$. We may then reproduce the proof of (6.4.2) with \mathbb{F}_p replaced by F , σ by τ , x^p by x^{p^m} , and X^p by X^{p^m} . Uniqueness of F as a subfield of E with p^m elements follows because there is only one splitting field over \mathbb{F}_p for $X^{p^m} - X$ inside E ; see (3.2.1). ♣

How do we know that finite fields (other than the \mathbb{F}_p) exist? There is no problem. Given any prime p and positive integer n , we can construct $E = GF(p^n)$ as a splitting field of $X^{p^n} - X$ over \mathbb{F}_p . We have just seen that if E contains a subfield F of size p^m , then m is a divisor of n . The converse is also true, as a consequence of the following basic result.

6.4.4 Theorem The multiplicative group of a finite field is cyclic. More generally, if G is a finite subgroup of the multiplicative group of an arbitrary field, then G is cyclic.

Proof. G is a finite abelian group, hence contains an element g whose order r is the *exponent* of G , that is, the least common multiple of the orders of all elements of G ; see Section 1.1, Problem 9. Thus if $x \in G$ then the order of x divides r , so $x^r = 1$. Therefore each element of G is a root of $X^r - 1$, so $|G| \leq r$. But $|G|$ is a multiple of the order of every element, so $|G|$ is at least as big as the least common multiple, so $|G| \geq r$. We conclude that the order and the exponent are the same. But then g has order $|G|$, so $G = \langle g \rangle$ and G is cyclic. ♣

6.4.5 Proposition $GF(p^m)$ is a subfield of $E = GF(p^n)$ if and only if m is a divisor of n .

Proof. The “only if” part follows from (6.4.3), so assume that m divides n . If t is any positive integer greater than 1, then $m|n$ iff $(t^m - 1)|(t^n - 1)$. (A formal proof is not difficult, but I prefer to do an ordinary long division of $t^n - 1$ by $t^m - 1$. The successive quotients are t^{n-m} , t^{n-2m} , t^{n-3m} , ..., so the division will be successful iff $n - rm = 0$ for some positive integer r .) Taking $t = p$, we see that $p^m - 1$ divides $|E^*|$, so by (6.4.4) and (1.1.4), E^* has a subgroup H of order $p^m - 1$. By Lagrange’s theorem, each $x \in H \cup \{0\}$ satisfies $x^{p^m} = x$. As in the proof of (6.4.1), $H \cup \{0\}$ coincides with the set of roots of $X^{p^m} - X$. Thus we may construct entirely inside $GF(p^n)$ a splitting field of $X^{p^m} - X$ over \mathbb{F}_p . But this splitting field is a copy of $GF(p^m)$. ♣

In practice, finite fields are constructed by adjoining roots of carefully selected irreducible polynomials over \mathbb{F}_p . The following result is very helpful.

6.4.6 Theorem Let p be a prime and n a positive integer. Then $X^{p^n} - X$ is the product of all monic irreducible polynomials over \mathbb{F}_p whose degree divides n .

Proof. Let us do all calculations inside $E = GF(p^n)$ = the set of roots of $f(X) = X^{p^n} - X$. If $g(X)$ is any monic irreducible factor of $f(X)$, and $\deg g = m$, then all roots of g lie in E . If α is any root of g , then $\mathbb{F}_p(\alpha)$ is a finite field with p^m elements, so m divides n by (6.4.5) or (6.4.3). Conversely, let $g(X)$ be a monic irreducible polynomial over \mathbb{F}_p whose degree m is a divisor of n . Then by (6.4.5), E contains a subfield with p^m elements, and this subfield must be isomorphic to $\mathbb{F}_p(\alpha)$. If $\beta \in E$ corresponds to α under this isomorphism, then $g(\beta) = 0$ (because $g(\alpha) = 0$) and $f(\beta) = 0$ (because $\beta \in E$). Since g is the minimal polynomial of β over \mathbb{F}_p , it follows that $g(X)$ divides $f(X)$. By (6.4.1), the roots of f are distinct, so no irreducible factor can appear more than once. The theorem is proved. ♣

6.4.7 The Explicit Construction of a Finite Field

By (6.4.4), the multiplicative group E^* of a finite field $E = GF(p^n)$ is cyclic, so E^* can be generated by a single element α . Thus $E = \mathbb{F}_p(\alpha) = \mathbb{F}_p[\alpha]$, so that α is a primitive element of E . The minimal polynomial of α over \mathbb{F}_p is called a *primitive polynomial*. The key point is that the nonzero elements of E are not

simply the nonzero polynomials of degree at most $n - 1$ in α , they are the *powers of α* . This is significant in applications to coding theory. Let's do an example over \mathbb{F}_2 .

The polynomial $g(X) = X^4 + X + 1$ is irreducible over \mathbb{F}_2 . One way to verify this is to factor $X^{16} - 1 = X^{16} + 1$ over \mathbb{F}_2 ; the factors are the (necessarily monic) irreducible polynomials of degrees 1, 2 and 4. To show that g is primitive, we compute powers of α :

$$\alpha^0 = 1, \alpha^1 = \alpha, \alpha^2 = \alpha^2, \alpha^3 = \alpha^3, \alpha^4 = 1 + \alpha \text{ (since } g(\alpha) = 0),$$

$$\alpha^5 = \alpha + \alpha^2, \alpha^6 = \alpha^2 + \alpha^3, \alpha^7 = \alpha^3 + \alpha^4 = 1 + \alpha + \alpha^3, \alpha^8 = \alpha + \alpha^2 + \alpha^4 = 1 + \alpha^2 \text{ (since } 1+1=0 \text{ in } \mathbb{F}_2),$$

$$\alpha^9 = \alpha + \alpha^3, \alpha^{10} = 1 + \alpha + \alpha^2, \alpha^{11} = \alpha + \alpha^2 + \alpha^3, \alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3, \alpha^{13} = 1 + \alpha^2 + \alpha^3, \alpha^{14} = 1 + \alpha^3,$$

and at this point we have all $2^4 - 1 = 15$ nonzero elements of $GF(16)$. The pattern now repeats, beginning with $\alpha^{15} = \alpha + \alpha^4 = 1$.

For an example of a non-primitive polynomial, see Problem 1.

Problems For Section 6.4

1. Verify that the irreducible polynomial $X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$ is not primitive.
2. Let F be a finite field and d a positive integer. Show that there exists an irreducible polynomial of degree d in $F[X]$.
3. In (6.4.5) we showed that $m|n$ iff $(t^m - 1)|(t^n - 1)$ ($t = 2, 3, \dots$). Show that an equivalent condition is $(X^m - 1)$ divides $(X^n - 1)$.

If E is a finite extension of a finite field, or more generally a finite separable extension of a field F , then by the theorem of the primitive element, $E = F(\alpha)$ for some $\alpha \in E$. We now develop a condition equivalent to the existence of a primitive element.

4. Let E/F be a finite extension, with $E = F(\alpha)$ and $F \leq L \leq E$. Suppose that the minimal polynomial of α over L is $g(X) = \sum_{i=0}^{r-1} b_i X^i + X^r$, and let $K = F(b_0, \dots, b_{r-1})$. If h is the minimal polynomial of α over K , show that $g = h$, and conclude that $L = K$.
5. Continuing Problem 4, show that there are only finitely many intermediate fields L between E and F .
6. Conversely, let $E = F(\alpha_1, \dots, \alpha_n)$ be a finite extension with only finitely many intermediate fields between E and F . We are going to show by induction that E/F has a primitive element. If $n = 1$ there is nothing to prove, so assume the result holds for all integers less than n . If $L = F(\alpha_1, \dots, \alpha_{n-1})$, show that $E = F(\beta, \alpha_n)$ for some $\beta \in L$.
7. Now assume (without loss of generality) that F is infinite. Show that there are distinct elements $c, d \in F$ such that $F(c\beta + \alpha_n) = F(d\beta + \alpha_n)$.
8. Continuing Problem 7, show that $E = F(c\beta + \alpha_n)$. Thus a finite extension has a primitive element iff there are only finitely many intermediate fields.
9. Let α be an element of the finite field $GF(p^n)$. Show that α and α^p have the same minimal polynomial over F_p .
10. Suppose that α is an element of order 13 in the multiplicative group of nonzero elements in $GF(3^n)$. Partition the integers $\{0, 1, \dots, 12\}$ into disjoint subsets such that if i and j belong to the same subset, then α^i and α^j have the same minimal polynomial. Repeat for α an element of order 15 in $GF(2^n)$. [Note that elements of the specified orders exist, because 13 divides $26 = 3^3 - 1$ and $15 = 2^4 - 1$.]

6.5 Cyclotomic Fields

6.5.1 Definitions and Comments Cyclotomic extensions of a field F are formed by adjoining n^{th} roots of unity. Formally, a *cyclotomic extension* of F is a splitting field E of $f(X) = X^n - 1$ over F . The roots of f are called *n^{th} roots of unity*, and they form a multiplicative subgroup of the group E^* of nonzero elements of E . This subgroup must be cyclic by (6.4.4). A *primitive n^{th} root of unity* is one whose order in E^* is n .

It is tempting to say “obviously, primitive n^{th} roots of unity must exist, just take a generator of the cyclic subgroup”. But suppose that F has characteristic p and p divides n , say $n = mp$. If ω is an n^{th} root of unity, then

$$0 = \omega^n - 1 = (\omega^m - 1)^p$$

so the order of ω must be less than n . To avoid this difficulty, we assume that the characteristic of F does not divide n . Then $f'(X) = nX^{n-1} \neq 0$, so by (3.4.2), f is separable, and consequently E/F is Galois. Since there are n distinct n^{th} roots of unity, there must be a primitive n^{th} root of unity ω , and for any such ω , we have $E = F(\omega)$.

If σ is any automorphism in the Galois group $\text{Gal}(E/F)$, then σ must take a primitive root of unity ω to another primitive root of unity ω^r , where r and n are relatively prime. (See (1.1.5).) We can identify σ with r , and this shows that $\text{Gal}(E/F)$ is isomorphic to a subgroup of U_n , the group of units mod n . Consequently, the Galois group is abelian.

Finally, by the fundamental theorem (or (3.5.9)), $[E : F] = |\text{Gal}(E/F)|$, which is a divisor of $|U_n| = \varphi(n)$.

Cyclotomic fields are of greatest interest when the underlying field F is \mathbb{Q} , the rational numbers, and from now on we specialize to that case. The primitive n^{th} roots of unity are $e^{i2\pi r/n}$ where r and n are relatively prime. Thus there are $\varphi(n)$ primitive n^{th} roots of unity. Finding the minimal polynomial of a primitive n^{th} root of unity requires some rather formidable equipment.

6.5.2 Definition The n^{th} cyclotomic polynomial is defined by

$$\Psi_n(X) = \prod_i (X - \omega_i)$$

where the ω_i are the primitive n^{th} roots of unity in the field \mathbb{C} of complex numbers. Thus the degree of $\Psi_n(X)$ is $\varphi(n)$.

From the definition, we have $\Psi_1(X) = X - 1$ and $\Psi_2(X) = X + 1$. In general, the cyclotomic polynomials can be calculated by the following recursion formula, in which d runs through all positive divisors of n .

6.5.3 Proposition

$$X^n - 1 = \prod_{d|n} \Psi_d(X).$$

In particular, if p is prime, then

$$\Psi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Proof. If ω is an n^{th} root of unity, then its order in \mathbb{C}^* is a divisor d of n , and in this case, ω is a primitive d^{th} root of unity, hence a root of $\Psi_d(X)$. Conversely, if $d|n$, then any root of $\Psi_d(X)$ is a d^{th} , hence an n^{th} , root of unity. ♣

From (6.5.3) we have

$$\Psi_3(X) = X^2 + X + 1,$$

$$\Psi_4(X) = X^2 + 1,$$

$$\Psi_5(X) = X^4 + X^3 + X^2 + X + 1,$$

$$\Psi_6(X) = \frac{X^6 - 1}{(X-1)(X+1)(X^2+X+1)} = \frac{X^6 - 1}{(X^3 - 1)(X + 1)} = \frac{X^3 + 1}{X + 1} = X^2 - X + 1.$$

It is a natural conjecture that all coefficients of the cyclotomic polynomials are integers, and this turns out to be correct.

6.5.4 Proposition $\Psi_n(X) \in \mathbb{Z}[X]$.

Proof. By (6.5.3), we have

$$X^n - 1 = \left[\prod_{d|n, d < n} \Psi_d(X) \right] \Psi_n(X).$$

By definition, the cyclotomic polynomials are monic, and by induction hypothesis, the expression in brackets is a monic polynomial in $\mathbb{Z}[X]$. Thus $\Psi_n(X)$ is the quotient of two monic polynomials with integer coefficients.

At this point, all we know for sure is that the coefficients of $\Psi_n(X)$ are complex numbers. But if we apply ordinary long division, even in \mathbb{C} , we know that the process will terminate, and this forces the quotient $\Psi_n(X)$ to be in $\mathbb{Z}[X]$. ♣

We now show that the n^{th} cyclotomic polynomial is the minimal polynomial of each primitive n^{th} root of unity.

6.5.5 Theorem $\Psi_n(X)$ is irreducible over \mathbb{Q} .

Proof. Let ω be a primitive n^{th} root of unity, with minimal polynomial f over \mathbb{Q} . Since ω is a root of $X^n - 1$, we have $X^n - 1 = f(X)g(X)$ for some $g \in \mathbb{Q}[X]$. Now it follows from (2.9.2) that if a monic polynomial over \mathbb{Z} is the product of two monic polynomials f and g over \mathbb{Q} , then in fact the coefficients of f and g are integers.

If p is a prime that does not divide n , we will show that ω^p is a root of f . If not, then it is a root of g . But $g(\omega^p) = 0$ implies that ω is a root of $g(X^p)$, so $f(X)$ divides $g(X^p)$, say $g(X^p) = f(X)h(X)$. As above, $h \in \mathbb{Z}[X]$. But by the binomial expansion modulo p , $g(X)^p \equiv g(X^p) = f(X)h(X) \pmod{p}$. Reducing the coefficients of a polynomial $k(X) \pmod{p}$ is equivalent to viewing it as an element $\bar{k} \in \mathbb{F}_p[X]$, so we may write $\bar{g}(X)^p = \bar{f}(X)\bar{h}(X)$. Then any irreducible factor of \bar{f} must divide \bar{g} , so \bar{f} and \bar{g} have a common factor. But then $X^n - 1$ has a multiple root, contradicting (3.4.2). [This is where we use the fact that p does not divide n .]

Now we claim that every primitive n^{th} root of unity is a root of f , so that $\deg f \geq \varphi(n) = \deg \Psi_n$, and therefore $f = \Psi_n$ by minimality of f . The best way to visualize this is via a concrete example with all the features of the general case. If ω is a primitive n^{th} root of unity where $n = 175$, then ω^{72} is a primitive n^{th} root of unity because 72 and 175 are relatively prime. Moreover, since $72 = 2^3 \times 3^2$, we have

$$\omega^{72} = (((((\omega)^2)^2)^2)^3)^3$$

and the result follows. ♣

6.5.6 Corollary The Galois group G of the n^{th} cyclotomic extension $\mathbb{Q}(\omega)/\mathbb{Q}$ is isomorphic to the group U_n of units mod n .

Proof. By the fundamental theorem, $|G| = [\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \Psi_n = \varphi(n) = |U_n|$. Thus the isomorphism of G and a subgroup of U_n (see (6.5.1)) is surjective. ♣

Problems For Section 6.5

1. If p is prime and p divides n , show that $\Psi_{pn}(X) = \Psi_n(X^p)$. (This formula is sometimes useful in computing the cyclotomic polynomials.)
2. Show that the group of automorphisms of a cyclic group of order n is isomorphic to the group U_n of units mod n . (This can be done directly, but it is easier to make use of the results of this section.)

We now do a detailed analysis of subgroups and intermediate fields associated with the cyclotomic extension $\mathbb{Q}_7 = \mathbb{Q}(\omega)/\mathbb{Q}$ where $\omega = e^{i2\pi/7}$ is a primitive 7th root of unity. The Galois group G consists of automorphisms σ_i , $i = 1, 2, 3, 4, 5, 6$, where $\sigma_i(\omega) = \omega^i$.

3. Show that σ_3 generates the cyclic group G .
4. Show that the subgroups of G are $\langle 1 \rangle$ (order 1), $\langle \sigma_6 \rangle$ (order 2), $\langle \sigma_2 \rangle$ (order 3), and $G = \langle \sigma_3 \rangle$ (order 6).
5. The fixed field of $\langle 1 \rangle$ is \mathbb{Q}_7 and the fixed field of G is \mathbb{Q} . Let K be the fixed field of $\langle \sigma_6 \rangle$. Show that $\omega + \omega^{-1} \in K$, and deduce that $K = \mathbb{Q}(\omega + \omega^{-1}) = \mathbb{Q}(\cos 2\pi/7)$.
6. Let L be the fixed field of $\langle \sigma_2 \rangle$. Show that $\omega + \omega^2 + \omega^4$ belongs to L but not to \mathbb{Q} .
7. Show that $L = \mathbb{Q}(\omega + \omega^2 + \omega^4)$.
8. If $q = p^r$, p prime, show that

$$\Psi_q(X) = t^{p-1} + t^{p-2} + \cdots + 1$$

where $t = X^{p^{r-1}}$.

9. Assuming that the first 6 cyclotomic polynomials are available [see after (6.5.3)], calculate $\Psi_{18}(X)$ in an effortless manner.

6.6 The Galois Group of a Cubic

Let f be a polynomial over F , with distinct roots x_1, \dots, x_n in a splitting field E over F . The Galois group G of f permutes the x_i , but which permutations belong to G ? When f is a quadratic, the analysis is straightforward, and is considered in Section 6.3, Problem 4. In this section we look at cubics (and some other manageable cases), and the appendix to Chapter 6 deals with the quartic.

6.6.1 Definitions and Comments Let f be a polynomial with distinct roots x_1, \dots, x_n as above. Define

$$\Delta(f) = \prod_{i < j} (x_i - x_j).$$

The *discriminant* of f is defined by

$$D(f) = \Delta^2 = \prod_{i < j} (x_i - x_j)^2.$$

Let's look at a quadratic polynomial $f(X) = X^2 + bX + c$, with roots $\frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$. In order to divide by 2, we had better assume that the characteristic of F is not 2, and this assumption is usually made before defining the discriminant. In this case we have $(x_1 - x_2)^2 = b^2 - 4c$, a familiar formula. Here are some basic properties of the discriminant.

6.6.2 Proposition Let E be a splitting field of the separable polynomial f over F , so that E/F is Galois.

- (a) $D(f)$ belongs to the base field F .
- (b) Let σ be an automorphism in the Galois group G of f . Then σ is an even permutation (of the roots of f) iff $\sigma(\Delta) = \Delta$, and σ is odd iff $\sigma(\Delta) = -\Delta$.
- (c) $G \subseteq A_n$, that is, G consists entirely of even permutations, iff $D(f)$ is the square of an element of F (for short, $D \in F^2$).

Proof. Let us examine the effect of a transposition $\sigma = (i, j)$ on Δ . Once again it is useful to consider a concrete example with all the features of the general case. Say $n = 15$, $i = 7$, $j = 10$. Then

$$\begin{aligned} x_3 - x_7 &\rightarrow x_3 - x_{10}, & x_3 - x_{10} &\rightarrow x_3 - x_7 \\ x_{10} - x_{12} &\rightarrow x_7 - x_{12}, & x_7 - x_{12} &\rightarrow x_{10} - x_{12} \\ x_7 - x_8 &\rightarrow x_{10} - x_8, & x_8 - x_{10} &\rightarrow x_8 - x_7 \\ x_7 - x_{10} &\rightarrow x_{10} - x_7. \end{aligned}$$

The point of the computation is that the net effect of (i, j) on Δ is to take $x_i - x_j$ to its negative. Thus $\sigma(\Delta) = -\Delta$ when σ is a transposition. Thus if σ is any permutation, we have $\sigma(\Delta) = \Delta$ if Δ is even, and $\sigma(\Delta) = -\Delta$ if σ is odd. Consequently, $\sigma(\Delta^2) = (\sigma(\Delta))^2 = \Delta^2$, so D belongs to the fixed field of G , which is F . This proves (a), and (b) follows because $\Delta \neq -\Delta$ (remember that the characteristic of F is not 2). Finally $G \subseteq A_n$ iff $\sigma(\Delta) = \Delta$ for every $\sigma \in G$ iff $\Delta \in \mathcal{F}(G) = F$. ♣

6.6.3 The Galois Group of a Cubic In the appendix to Chapter 6, it is shown that the discriminant of the abbreviated cubic $X^3 + pX + q$ is $-4p^3 - 27q^2$, and the discriminant of the general cubic $X^3 + aX^2 + bX + c$ is

$$a^2(b^2 - 4ac) - 4b^3 - 27c^2 + 18abc.$$

Alternatively, the change of variable $Y = X + \frac{a}{3}$ eliminates the quadratic term without changing the discriminant.

We now assume that the cubic polynomial f is irreducible as well as separable. Then the Galois group G is isomorphic to a transitive subgroup of S_3 (see Section 6.3, Problem 3). By direct enumeration, G must be A_3 or S_3 , and by (6.6.2(c)), $G = A_3$ iff the discriminant D is a square in F .

If $G = A_3$, which is cyclic of order 3, there are no proper subgroups except $\{1\}$, so there are no intermediate fields strictly between E and F . However, if $G = S_3$, then the proper subgroups are

$$\{1, (2, 3)\}, \{1, (1, 3)\}, \{1, (1, 2)\}, A_3 = \{1, (1, 2, 3), (1, 3, 2)\}.$$

If the roots of f are α_1, α_2 and α_3 , then the corresponding fixed fields are

$$F(\alpha_1), F(\alpha_2), F(\alpha_3), F(\Delta)$$

where A_3 corresponds to $F(\Delta)$ because only even permutations fix Δ .

6.6.4 Example Let $f(X) = X^3 - 31X + 62$ over \mathbb{Q} . An application of the rational root test (Section 2.9, Problem 1) shows that f is irreducible. The discriminant is $-4(-31)^3 - 27(62)^2 = 119164 - 103788 = 15376 = (124)^2$, which is a square in \mathbb{Q} . Thus the Galois group of f is A_3 .

We now develop a result that can be applied to certain cubics, but which has wider applicability as well. The preliminary steps are also of interest.

6.6.5 Some Generating Sets of S_n

(i) S_n is generated by the transpositions $(1, 2), (1, 3), \dots, (1, n)$.

[An arbitrary transposition (i, j) can be written as $(1, i)(1, j)(1, i)$.]

(ii) S_n is generated by transpositions of adjacent digits, i.e.,

$$(1, 2), (2, 3), \dots, (n-1, n).$$

[Since $(1, j-1)(j-1, j)(1, j-1) = (1, j)$, we have $(1, 2)(2, 3)(1, 2) = (1, 3)$, $(1, 3)(3, 4)(1, 3) = (1, 4)$, etc., and the result follows from (i).]

(iii) S_n is generated by the two permutations $\sigma_1 = (1, 2)$ and $\tau = (1, 2, \dots, n)$.

[If $\sigma_2 = \tau\sigma_1\tau^{-1}$, then σ_2 is obtained by applying τ to the symbols of σ_1 (see Section 5.2, Problem 1). Thus $\sigma_2 = (2, 3)$. Similarly, $\sigma_3 = \tau\sigma_2\tau^{-1} = (3, 4), \dots, \sigma_{n-1} = \tau\sigma_{n-2}\tau^{-1} = (n-1, n)$, and the result follows from (ii).]

(iv) S_n is generated by $(1, 2)$ and $(2, 3, \dots, n)$.

[(1, 2)(2, 3, \dots, n) = (1, 2, 3, \dots, n), and (iii) applies.]

6.6.6 Lemma If f is an irreducible separable polynomial over F of degree n , and G is the Galois group of f , then n divides $|G|$. If n is a prime number p , then G contains a p -cycle.

Proof. If α is any root of f , then $[F(\alpha) : F] = n$, so by the fundamental theorem, G contains a subgroup whose index is n . By Lagrange's theorem, n divides $|G|$. If $n = p$, then by Cauchy's theorem, G contains an element σ of order p . We can express σ as a product of disjoint cycles, and the length of each cycle must divide the order of σ . Since p is prime, σ must consist of disjoint p -cycles. But a single p -cycle already uses up all the symbols to be permuted, so σ is a p -cycle. ♣

6.6.7 Proposition If f is irreducible over \mathbb{Q} and of prime degree p , and f has exactly two nonreal roots in the complex field \mathbb{C} , then the Galois group G of f is S_p .

Proof. By (6.6.6), G contains a p -cycle σ . Now one of the elements of G must be complex conjugation τ , which is an automorphism of \mathbb{C} that fixes \mathbb{R} (hence \mathbb{Q}). Thus τ permutes the two nonreal roots and leaves the $p-2$ real roots fixed, so τ is a transposition. Since p is prime, σ^k is a p -cycle for $k = 1, \dots, p-1$. It follows that by renumbering symbols if necessary, we can assume that $(1, 2)$ and $(1, 2, \dots, p)$ belong to G . By (6.6.5) part (iii), $G = S_p$. ♣

Problems For Section 6.6

In Problems 1-4, all polynomials are over the rational field \mathbb{Q} , and in each case, you are asked to find the Galois group G .

1. $f(X) = X^3 - 2$ (do it two ways)
2. $f(X) = X^3 - 3X + 1$
3. $f(X) = X^5 - 10X^4 + 2$
4. $f(X) = X^3 + 3X^2 - 2X + 1$ (calculate the discriminant in two ways)
5. If f is a separable cubic, not necessarily irreducible, then there are other possibilities for the Galois group G of f besides S_3 and A_3 . What are they?
6. Let f be an irreducible cubic over \mathbb{Q} with exactly one real root. Show that $D(f) < 0$, and conclude that the Galois group of f is S_3 .
7. Let f be an irreducible cubic over \mathbb{Q} with 3 distinct real roots. Show that $D(f) > 0$, so that the Galois group is A_3 or S_3 according as $\sqrt{D} \in \mathbb{Q}$ or $\sqrt{D} \notin \mathbb{Q}$.

6.7 Cyclic and Kummer Extensions

The problem of solving a polynomial equation by radicals is thousands of years old, but it can be given a modern flavor. We are looking for roots of $f \in F[X]$, and we are only allowed to use algorithms that do ordinary arithmetic plus the extraction of n^{th} roots. The idea is to identify those polynomials whose roots can be found in this way. Now if $a \in F$ and our algorithm computes $\theta = \sqrt[n]{a}$ in some extension field of F , then θ is a root of $X^n - a$, so it is natural to study splitting fields of $X^n - a$.

6.7.1 Assumptions, Comments and a Definition

- Assume
- (i) E is a splitting field for $f(X) = X^n - a$ over F , where $a \neq 0$.
 - (ii) F contains a primitive n^{th} root of unity ω .

These are natural assumption if we want to allow the computation of n^{th} roots. If θ is any root of f in E , then the roots of f are $\theta, \omega\theta, \dots, \omega^{n-1}\theta$. (The roots must be distinct because a , hence θ , is nonzero.) Therefore $E = F(\theta)$. Since f is separable, the extension E/F is Galois (see (6.3.1)). If $G = \text{Gal}(E/F)$, then $|G| = [E : F]$ by the fundamental theorem (or by (3.5.9)).

In general, a *cyclic extension* is a Galois extension whose Galois group is cyclic.

6.7.2 Theorem Under the assumptions of (6.7.1), E/F is a cyclic extension and the order of the Galois group G is a divisor of n . We have $|G| = n$ if and only if $f(X)$ is irreducible over F .

Proof. Let $\sigma \in G$; since σ permutes the roots of f by (3.5.1), we have $\sigma(\theta) = \omega^{u(\sigma)}\theta$. We identify integers $u(\sigma)$ with the same residue mod n . If $\sigma_i(\theta) = \omega^{u(\sigma_i)}\theta$, $i = 1, 2$, then

$$\sigma_1(\sigma_2(\theta)) = \omega^{u(\sigma_1)+u(\sigma_2)}\theta,$$

so

$$u(\sigma_1\sigma_2) = u(\sigma_1) + u(\sigma_2)$$

and u is a group homomorphism from G to \mathbb{Z}_n . If $u(\sigma)$ is 0 mod n , then $\sigma(\theta) = \theta$, so σ is the identity and the homomorphism is injective. Thus G is isomorphic to a subgroup of \mathbb{Z}_n , so G is cyclic and $|G|$ divides n .

If f is irreducible over F , then $|G| = [E : F] = [F(\theta) : F] = \deg f = n$. If f is not irreducible over F , let g be a proper irreducible factor. If β is a root of g in E , then β is also a root of f , so $E = F(\beta)$ and $|G| = [E : F] = [F(\beta) : F] = \deg g < n$. ♣

Thus splitting fields of $X^n - a$ give rise to cyclic extensions. Conversely, we can prove that a cyclic extension comes from such a splitting field.

6.7.3 Theorem Let E/F be a cyclic extension of degree n , where F contains a primitive n^{th} root of unity ω . Then for some nonzero $a \in F$, $f(X) = X^n - a$ is irreducible over F and E is a splitting field for f over F .

Proof. Let σ be a generator of the Galois group of the extension. By Dedekind's lemma (6.1.6), the distinct automorphisms $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are linearly independent over E . Thus $1 + \omega\sigma + \omega^2\sigma^2 + \dots + \omega^{n-1}\sigma^{n-1}$ is not identically 0, so for some $\beta \in E$ we have

$$\theta = \beta + \omega\sigma(\beta) + \dots + \omega^{n-1}\sigma^{n-1}(\beta) \neq 0.$$

Now

$$\sigma(\theta) = \sigma(\beta) + \omega\sigma^2(\beta) + \cdots + \omega^{n-2}\sigma^{n-1}(\beta) + \omega^{n-1}\sigma^n(\beta) = \omega^{-1}\theta$$

since $\sigma^n(\beta) = \beta$. We take $a = \theta^n$. To prove that $a \in F$, note that

$$\sigma(\theta^n) = (\sigma(\theta))^n = (\omega^{-1}\theta)^n = \theta^n$$

hence a belongs to the fixed field of $\text{Gal}(E/F)$, which is F .

Now by definition of a , θ is a root of $f(X) = X^n - a$, so the roots of $X^n - a$ are $\theta, \omega\theta, \dots, \omega^{n-1}\theta$. Therefore $F(\theta)$ is a splitting field for f over F . Since $\sigma(\theta) = \omega^{-1}\theta$, the automorphisms $1, \sigma, \dots, \sigma^{n-1}$ are still distinct when restricted to $F(\theta)$. Consequently,

$$n \leq |\text{Gal}(F(\theta)/F)| = [F(\theta) : F] \leq \deg f = n$$

so $[F(\theta) : F] = n$. It follows that $E = F(\theta)$ and (since f must be the minimal polynomial of θ over F) f is irreducible over F . ♣

A finite abelian group is a direct product of cyclic groups (or direct sum, in additive notation; see (4.6.4)). It is reasonable to expect that our analysis of cyclic Galois groups will help us to understand abelian Galois groups.

6.7.4 Definition A *Kummer extension* is a finite Galois extension with an abelian Galois group.

6.7.5 Theorem Let E/F be a finite extension, and assume that F contains a primitive n^{th} root of unity ω . Then E/F is a Kummer extension whose Galois group G has an exponent dividing n if and only if there are nonzero elements $a_1, \dots, a_r \in F$ such that E is a splitting field of $(X^n - a_1) \cdots (X^n - a_r)$ over F . [For short, $E = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$.]

Proof. We do the “if” part first. As in (6.7.1), we have $E = F(\theta_1, \dots, \theta_r)$ where θ_i is a root of $X^n - a_i$. If $\sigma \in \text{Gal}(E/F)$, then σ maps θ_i to another root of $X^n - a_i$, so

$$\sigma(\theta_i) = \omega^{u_i(\sigma)}\theta_i.$$

Thus if σ and τ are any two automorphisms in the Galois group G , then $\sigma\tau = \tau\sigma$ and G is abelian. [The u_i are integers, so $u_i(\sigma) + u_i(\tau) = u_i(\tau) + u_i(\sigma)$.] Now restrict attention to the extension $F(\theta_i)$. By (6.7.2), the Galois group of $F(\theta_i)/F$ has order dividing n , so $\sigma^n(\theta_i) = \theta_i$ for all $i = 1, \dots, r$. Thus σ^n is the identity, and the exponent of G is a divisor of n .

For the “only if” part, observe that since G is a finite abelian group, it is a direct product of cyclic groups C_1, \dots, C_r . For each $i = 1, \dots, r$, let H_i be the product of the C_j for $j \neq i$; by (1.5.3), $H_i \trianglelefteq G$. We have $G/H_i \cong C_i$ by the first isomorphism theorem. (Consider the projection mapping $x_1 \cdots x_r \rightarrow x_i \in C_i$.) Let K_i be the fixed field of H_i . By the fundamental theorem, K_i/F is a Galois extension and its Galois group is isomorphic to G/H_i , hence isomorphic to C_i . Thus K_i/F is a cyclic extension of degree $d_i = |C_i|$, and d_i is a divisor of n . (Since G is the direct product of the C_i , some element of G has order d_i , so d_i divides the exponent of G and therefore divides n .) We want to apply (6.7.3) with n replaced by d_i , and this is possible because F contains a primitive d_i^{th} root of unity, namely ω^{n/d_i} . We conclude that $K_i = F(\theta_i)$, where $\theta_i^{d_i}$ is a nonzero element $b_i \in F$. But $\theta_i^n = \theta_i^{d_i(n/d_i)} = b_i^{n/d_i} = a_i \in F$.

Finally, in the Galois correspondence, the intersection of the H_i is paired with the composite of the K_i , which is $F(\theta_1, \dots, \theta_r)$; see Section 6.3, Problem 7. But $\bigcap_{i=1}^r H_i = 1$, so $E = F(\theta_1, \dots, \theta_r)$, and the result follows. ♣

Problems For Section 6.7

1. Find the Galois group of the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$ [the splitting field of $(X^2 - 2)(X^2 - 3)(X^2 - 5)(X^2 - 7)$] over \mathbb{Q} .
2. Suppose that E is a splitting field for $f(X) = X^n - a$ over F , $a \neq 0$, but we drop the second assumption in (6.7.1) that F contains a primitive n^{th} root of unity. Is it possible for the Galois group of E/F to be

cyclic?

3. Let E be a splitting field for $X^n - a$ over F , where $a \neq 0$, and assume that the characteristic of F does not divide n . Show that E contains a primitive n^{th} root of unity.

We now assume that E is a splitting field for $f(X) = X^p - c$ over F , where $c \neq 0$, p is prime and the characteristic of F is not p . Let ω be a primitive p^{th} root of unity in E (see Problem 3). Assume that f is not irreducible over F , and let g be an irreducible factor of f of degree d , where $1 \leq d < p$. Let θ be a root of g in E .

4. Let g_0 be the product of the roots of g . (Since g_0 is \pm the constant term of g , $g_0 \in F$.) Show that $g_0^p = \theta^{dp} = c^d$.

5. Since d and p are relatively prime, there are integers a and b such that $ad + bp = 1$. Use this to show that if $X^p - c$ is not irreducible over F , then it must have a root in F .

6. Continuing Problem 5, show that if $X^p - c$ is not irreducible over F , then $E = F(\omega)$.

7. Continuing Problem 6, show that if $X^p - c$ is not irreducible over F , then $X^p - c$ splits over F if and only if F contains a primitive p^{th} root of unity.

Let E/F be a cyclic Galois extension of prime degree p , where p is the characteristic of F . Let σ be a generator of $G = \text{Gal}(E/F)$. It is a consequence of Hilbert's Theorem 90 (see the Problems for Section 7.3) that there is an element $\theta \in E$ such that $\sigma(\theta) = \theta + 1$. Prove the *Artin-Schreier theorem*:

8. $E = F(\theta)$.

9. θ is a root of $f(X) = X^p - X - a$ for some $a \in F$.

10. f is irreducible over F (hence $a \neq 0$).

Conversely, Let F be a field of prime characteristic p , and let E be a splitting field for $f(X) = X^p - X - a$, where a is a nonzero element of F .

11. If θ is any root of f in E , show that $E = F(\theta)$ and that f is separable.

12. Show that every irreducible factor of f has the same degree d , where $d = 1$ or p . Thus if $d = 1$, then $E = F$, and if $d = p$, then f is irreducible over F .

13. If f is irreducible over F , show that the Galois group of f is cyclic of order p .

6.8 Solvability By Radicals

6.8.1 Definitions and Comments We wish to solve the polynomial equation $f(X) = 0$, $f \in F[X]$, under the restriction that we are only allowed to perform ordinary arithmetic operations (addition, subtraction, multiplication and division) on the coefficients, along with extraction of n^{th} roots (for any $n = 2, 3, \dots$). A sequence of operations of this type gives rise to a sequence of extensions

$$F \leq F(\alpha_1) \leq F(\alpha_1, \alpha_2) \leq \dots \leq F(\alpha_1, \dots, \alpha_r) = E$$

where $\alpha_1^{n_1} \in F$ and $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$, $i = 2, \dots, r$. Equivalently, we have

$$F = F_0 \leq F_1 \leq \dots \leq F_r = E$$

where $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{n_i} \in F_{i-1}$, $i = 1, \dots, r$. We say that E is a *radical extension* of F . It is convenient (and legal) to assume that $n_1 = \dots = n_r = n$. (Replace each n_i by the product of all the n_i . To justify this, observe that if α^j belongs to a field L , then $\alpha^{mj} \in L$, $m = 2, 3, \dots$) Unless otherwise specified, we will make this assumption in all hypotheses, conclusions and proofs.

We have already seen three explicit classes of radical extensions: cyclotomic, cyclic and Kummer. (In the latter two cases, we assume that the base field contains a primitive n^{th} root of unity.)

We say that the polynomial $f \in F[X]$ is *solvable by radicals* if the roots of f lie in some radical extension of F , in other words, there is a radical extension E of F such that f splits over E .

Since radical extensions are formed by successively adjoining n^{th} roots, it follows that the transitivity property holds: If E is a radical extension of F and L is a radical extension of E , then L is a radical extension of F .

A radical extension is always finite, but it need not be normal or separable. We will soon specialize to characteristic 0, which will force separability, and we can achieve normality by taking the normal closure (see (3.5.11)).

6.8.2 Proposition Let E/F be a radical extension, and let N be the normal closure of E over F . Then N/F is also a radical extension.

Proof. E is obtained from F by successively adjoining $\alpha_1, \dots, \alpha_r$, where α_i is the n^{th} root of an element in F_{i-1} . On the other hand, N is obtained from F by adjoining not only the α_i , but their conjugates $\alpha_{i1}, \dots, \alpha_{im(i)}$. For any fixed i and j , there is an automorphism $\sigma \in \text{Gal}(N/F)$ such that $\sigma(\alpha_i) = \alpha_{ij}$ (see (3.2.3), (3.5.5) and (3.5.6)). Thus

$$\alpha_{ij}^n = \sigma(\alpha_i)^n = \sigma(\alpha_i^n)$$

and since α_i^n belongs to $F(\alpha_1, \dots, \alpha_{i-1})$, it follows from (3.5.1) that $\sigma(\alpha_i^n)$ belongs to the splitting field K_i of $\prod_{j=1}^{i-1} \min(\alpha_j, F)$ over F . [Take $K_1 = F$, and note that since $\alpha_1^n = b_1 \in F$, we have $\sigma(\alpha_1^n) = \sigma(b_1) = b_1 \in F$. Alternatively, observe that by (3.5.1), σ must take a root of $X^n - b_1$ to another root of this polynomial.] Thus we can display N as a radical extension of F by successively adjoining

$$\alpha_{11}, \dots, \alpha_{1m(1)}, \dots, \alpha_{r1}, \dots, \alpha_{rm(r)}. \clubsuit$$

6.8.3 Preparation for the Main Theorem If F has characteristic 0, then a primitive n^{th} root of unity ω can be adjoined to F to reach an extension $F(\omega)$; see (6.5.1). If E is a radical extension of F and $F = F_0 \leq F_1 \leq \dots \leq F_r = E$, we can replace F_i by $F_i(\omega)$, $i = 1, \dots, r$, and $E(\omega)$ will be a radical extension of F . By (6.8.2), we can pass from $E(\omega)$ to its normal closure over F . Here is the statement we are driving at:

Let $f \in F[X]$, where F has characteristic 0. If f is solvable by radicals, then there is a Galois radical extension $N = F_r \geq \dots \geq F_1 \geq F_0 = F$ containing a splitting field K for f over F , such that each intermediate field F_i , $i = 1, \dots, r$, contains a primitive n^{th} root of unity ω . We can assume that $F_1 = F(\omega)$ and for $i > 1$, F_i is a splitting field for $X^n - b_i$ over F_{i-1} . [(Look at the end of the proof of (6.8.2).] By (6.5.1), F_1/F is a Kummer (Galois) extension, and by (6.7.2), each F_i/F_{i-1} , $i = 2, \dots, r$ is a cyclic (Galois) extension.

We now do some further preparation. Suppose that K is a splitting field for f over F , and that the Galois group of K/F is solvable, with

$$\text{Gal}(K/F) = H_0 \supseteq H_1 \supseteq \dots \supseteq H_r = 1$$

with each H_{i-1}/H_i abelian. By the fundamental theorem, we have the corresponding sequence of fixed fields

$$F = K_0 \leq K_1 \leq \dots \leq K_r = K$$

with K_i/K_{i-1} Galois and $\text{Gal}(K_i/K_{i-1})$ isomorphic to H_{i-1}/H_i . Let us adjoin a primitive n^{th} root of unity ω to each K_i , so that we have fields $F_i = K_i(\omega)$ with

$$F \leq F_0 \leq F_1 \leq \dots \leq F_r.$$

We take $n = |\text{Gal}(K/F)|$. Since F_i can be obtained from F_{i-1} by adjoining everything in $K_i \setminus K_{i-1}$, we have

$$F_i = F_{i-1}K_i = K_iF_{i-1}$$

the composite of F_{i-1} and K_i , $i = 1, \dots, r$. We may now apply Theorem 6.2.2. In the diamond diagram of Figure 6.2.1, at the top of the diamond we have F_i , on the left K_i , on the right F_{i-1} , and on the bottom $K_i \cap F_{i-1} \supseteq K_{i-1}$ (see Figure 6.8.1). We conclude that F_i/F_{i-1} is Galois, with a Galois group isomorphic to a subgroup of $\text{Gal}(K_i/K_{i-1})$. Since $\text{Gal}(K_i/K_{i-1}) \cong H_{i-1}/H_i$, it follows that $\text{Gal}(F_i/F_{i-1})$

is abelian. Moreover, the exponent of this Galois group divides the order of H_0 , which coincides with the size of $\text{Gal}(K/F)$. (This explains our choice of n .)

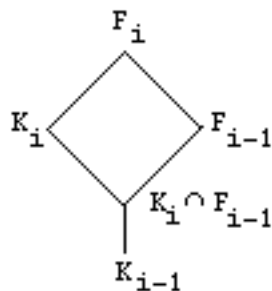


Figure 6.8.1

6.8.4 Galois' Solvability Theorem Let K be a splitting field for f over F , where F has characteristic 0. Then f is solvable by radicals if and only if the Galois group of K/F is solvable.

Proof. If f is solvable by radicals, then as in (6.8.3), we have

$$F = F_0 \leq F_1 \leq \cdots \leq F_r = N$$

where N/F is Galois, N contains a splitting field K for f over F , and each F_i/F_{i-1} is Galois with an abelian Galois group. By the fundamental theorem, the corresponding sequence of subgroups is

$$1 = H_r \trianglelefteq H_{r-1} \trianglelefteq \cdots \trianglelefteq H_0 = G = \text{Gal}(N/F)$$

with each H_{i-1}/H_i abelian. Thus G is solvable, and since

$$\text{Gal}(K/F) \cong \frac{\text{Gal}(N/F)}{\text{Gal}(N/K)}$$

[map $\text{Gal}(N/F) \rightarrow \text{Gal}(K/F)$ by restriction; the kernel is $\text{Gal}(N/K)$], $\text{Gal}(K/F)$ is solvable by (5.7.4).

Conversely, assume that $\text{Gal}(K/F)$ is solvable. Again as in (6.8.3), we have

$$F \leq F_0 \leq F_1 \leq \cdots \leq F_r$$

where $K \leq F_r$, each F_i contains a primitive n^{th} root of unity, with $n = |\text{Gal}(K/F)|$, and $\text{Gal}(F_i/F_{i-1})$ is abelian with exponent dividing n for all $i = 1, \dots, r$. Thus each F_i/F_{i-1} is a Kummer extension whose Galois group has an exponent dividing n . By (6.7.5) (or (6.5.1) for the case $i = 1$), each F_i/F_{i-1} is a radical extension. By transitivity (see (6.8.1)), F_r is a radical extension of F . Since $K \subseteq F_r$, f is solvable by radicals. ♣

6.8.5 Example Let $f(X) = X^5 - 10X^4 + 2$ over the rationals. The Galois group of f is S_5 , which is not solvable. (See Section 6.6, Problem 3 and Section 5.7, Problem 5.) Thus f is not solvable by radicals.

There is a fundamental idea that needs to be emphasized. The significance of Galois' solvability theorem is not simply that there are some examples of bad polynomials. The key point is there is no *general* method for solving a polynomial equation over the rationals by radicals, if the degree of the polynomial is 5 or more. If there were such a method, then in particular it would work on Example (6.8.5), a contradiction.

Problems For Section 6.8

In the exercises, we will sketch another classical problem, that of constructions with ruler and compass. In Euclidean geometry, we start with two points $(0,0)$ and $(1,0)$, and we are allowed the following constructions.

- (i) Given two points P and Q , we can draw a line joining them;
- (ii) Given a point P and a line L , we can draw a line through P parallel to L ;
- (iii) Given a point P and a line L , we can draw a line through P perpendicular to L ;
- (iv) Given two points P and Q , we can draw a circle with center at P passing through Q ;
- (v) Let A , and similarly B , be a line or a circle. We can generate new points, called *constructible points*, by forming the intersection of A and B . If $(c, 0)$ (equivalently $(0, c)$) is a constructible point, we call c a *constructible number*. It follows from (ii) and (iii) that (a, b) is a constructible point iff a and b are constructible numbers. It can be shown that every rational number is constructible, and that the constructible numbers form a field. Now in (v), the intersection of A and B can be found by ordinary arithmetic plus at worst the extraction of a square root. Therefore c is constructible iff there are fields $\mathbb{Q} = F_0 \leq F_1 \cdots \leq F_r$ such that $c \in F_r$ and each $[F_i : F_{i-1}]$ is 1 or 2. Thus if c is constructible, then c is algebraic over \mathbb{Q} and $[\mathbb{Q}(c) : \mathbb{Q}]$ is a power of 2.

1. (Trisecting the angle) If it is possible to trisect any angle with ruler and compass, then in particular a 60° degree angle can be trisected, so that $\alpha = \cos 20^\circ$ is constructible. Using the identity

$$e^{i3\theta} = \cos 3\theta + i \sin 3\theta = (\cos \theta + i \sin \theta)^3,$$

reach a contradiction.

- 2. (Duplicating the cube) Show that it is impossible to construct, with ruler and compass, a cube whose volume is exactly 2. (The side of such a cube would be $\sqrt[3]{2}$.)
- 3. (Squaring the circle) Show that if it were possible to construct a square with area π , then π would be algebraic over \mathbb{Q} . (It is known that π is transcendental over \mathbb{Q} .)

To construct a regular n -gon, that is, a regular polygon with n sides, $n \geq 3$, we must be able to construct an angle of $2\pi/n$; equivalently, $\cos 2\pi/n$ must be a constructible number. Let $\omega = e^{i2\pi/n}$, a primitive n^{th} root of unity.

- 4. Show that $[\mathbb{Q}(\omega) : \mathbb{Q}(\cos 2\pi/n)] = 2$.
- 5. Show that if a regular n -gon is constructible, then the Euler phi function $\varphi(n)$ is a power of 2.

Conversely, assume that $\varphi(n)$ is a power of 2.

- 6. Show that $\text{Gal}(\mathbb{Q}(\cos 2\pi/n)/\mathbb{Q})$ is a 2-group, that is, a p -group with $p = 2$.
- 7. By Section 5.7, Problem 7, every nontrivial finite p -group has a subnormal series in which every factor has order p . Use this (with $p = 2$) to show that a regular n -gon is constructible.
- 8. From the preceding, a regular n -gon is constructible if and only if $\varphi(n)$ is a power of 2. Show that an equivalent condition is that $n = 2^s q_1 \cdots q_t$, $s, t = 0, 1, \dots$, where the q_i are distinct *Fermat primes*, that is, primes of the form $2^m + 1$ for some positive integer m .
- 9. Show that if $2^m + 1$ is prime, then m must be a power of 2. The only known Fermat primes have $m = 2^a$, where $a = 0, 1, 2, 3, 4$ ($2^{32} + 1$ is divisible by 641). [The key point is that if a is odd, then $X + 1$ divides $X^a + 1$ in $\mathbb{Z}[X]$; the quotient is $X^{a-1} - X^{a-2} + \cdots - X + 1$ (since $a - 1$ is even).]

Let F be the field of rational functions in n variables e_1, \dots, e_n over a field k with characteristic 0, and let $f(X) = X^n - e_1 X^{n-1} + e_2 X^{n-2} - \cdots + (-1)^n e_n \in F[X]$. If $\alpha_1, \dots, \alpha_n$ are the roots of f in a splitting field over F , then the e_i are the elementary symmetric functions of the α_i . Let $E = F(\alpha_1, \dots, \alpha_n)$, so that E/F is a Galois extension and $G = \text{Gal}(E/F)$ is the Galois group of f .

- 10. Show that $G \cong S_n$.
- 11. What can you conclude from Problem 10 about solvability of equations?

6.9 Transcendental Extensions

6.9.1 Definitions and Comments An extension E/F such that at least one $\alpha \in E$ is not algebraic over F is said to be *transcendental*. An idea analogous to that of a basis of an arbitrary vector space V turns out to be profitable in studying transcendental extensions. A basis for V is a subset of V that is linearly independent and spans V . A key result, whose proof involves the Steinitz exchange, is that if $\{x_1, \dots, x_m\}$ spans V and S is a linearly independent subset of V , then $|S| \leq m$. We are going to replace linear independence by algebraic independence and spanning by algebraic spanning. We will find that every transcendental extension has a

transcendence basis, and that any two transcendence bases for a given extension have the same cardinality. All these terms will be defined shortly. The presentation in the text will be quite informal; I believe that this style best highlights the strong connection between linear and algebraic independence. An indication of how to formalize the development is given in a sequence of exercises. See also Morandi, “Fields and Galois Theory”, pp.173-182.

Let E/F be an extension. The elements $t_1, \dots, t_n \in E$ are *algebraically dependent over F* (or the set $\{t_1, \dots, t_n\}$ is algebraically dependent over F) if there is a nonzero polynomial $f \in F[X_1, \dots, X_n]$ such that $f(t_1, \dots, t_n) = 0$; otherwise the t_i are *algebraically independent over F* . Algebraic independence of an infinite set means algebraic independence of every finite subset.

Now if a set T spans a vector space V , then each x in V is a linear combination of elements of T , so that x depends on T in a linear fashion. Replacing “linear” by “algebraic”, we say that the element $t \in E$ *depends algebraically on T* over F if t is algebraic over $F(T)$, the field generated by T over F (see Section 3.1, Problem 1). We say that T *spans E algebraically over F* if each t in E depends algebraically on T over F , that is, E is an algebraic extension of $F(T)$. A *transcendence basis* for E/F is a subset of E that is algebraically independent over F and spans E algebraically over F . (From now on, we will frequently regard F as fixed and drop the phrase “over F ”.)

6.9.2 Lemma If S is a subset of E , the following conditions are equivalent.

- (i) S is a transcendence basis for E/F ;
- (ii) S is a maximal algebraically independent set;
- (iii) S is a minimal algebraically spanning set.

Thus by (ii), S is a transcendence basis for E/F iff S is algebraically independent and E is algebraic over $F(S)$.

Proof.

(i) implies (ii) If $S \subset T$ where T is algebraically independent, let $u \in T \setminus S$. Then u cannot depend on S algebraically (by algebraic independence of T), so S cannot span E algebraically.

(ii) implies (i) If S does not span E algebraically, then there exists $u \in E$ such that u does not depend algebraically on S . But then $S \cup \{u\}$ is algebraically independent, contradicting maximality of S .

(i) implies (iii) If $T \subset S$ and T spans E algebraically, let $u \in S \setminus T$. Then u depends algebraically on T , so $T \cup \{u\}$, hence S , is algebraically dependent, a contradiction.

(iii) implies (i) If S is algebraically dependent, then some $u \in S$ depends algebraically on $T = S \setminus \{u\}$. But then T spans E algebraically, a contradiction. ♣

6.9.3 Proposition Every transcendental extension has a transcendence basis.

Proof. The standard argument via Zorn’s lemma that an arbitrary vector space has a maximal linearly independent set (hence a basis) shows that an arbitrary transcendental extension has a maximal algebraically independent set, which is a transcendence basis by (6.9.2). ♣

For completeness, if E/F is an algebraic extension, we can regard \emptyset as a transcendence basis.

6.9.4 The Steinitz Exchange If $\{x_1, \dots, x_m\}$ spans E algebraically and S is algebraically independent, then $|S| \leq m$.

Proof. Suppose that S has at least $m + 1$ elements y_1, \dots, y_{m+1} . Since the x_i span E algebraically, y_1 depends algebraically on x_1, \dots, x_m . The algebraic dependence relation must involve at least one x_i , say x_1 . (Otherwise, S would be algebraically dependent.) Then x_1 depends algebraically on y_1, x_2, \dots, x_m , so $\{y_1, x_2, \dots, x_m\}$ spans E algebraically. We claim that for every $i = 1, \dots, m$, $\{y_1, \dots, y_i, x_{i+1}, \dots, x_m\}$ spans E algebraically. We have just proved the case $i = 1$. If the result holds for i , then y_{i+1} depends algebraically on $\{y_1, \dots, y_i, x_{i+1}, \dots, x_m\}$, and the dependence relation must involve at least one x_j , say x_{i+1} for convenience. (Otherwise, S would be algebraically dependent.) Then x_{i+1} depends algebraically on $y_1, \dots, y_{i+1}, x_{i+2}, \dots, x_m$, so $\{y_1, \dots, y_{i+1}, x_{i+2}, \dots, x_m\}$ spans E algebraically, completing the induction.

Since there are more y ’s than x ’s, eventually the x ’s disappear, and y_1, \dots, y_m span E algebraically. But then y_{m+1} depends algebraically on y_1, \dots, y_m , contradicting the algebraic independence of S . ♣

6.9.5 Corollary Let S and T be transcendence bases of E . Then either S and T are both finite or they are both infinite; in the former case, $|S| = |T|$.

Proof. Assume that one of the transcendence bases, say T , is finite. By (6.9.4), $|S| \leq |T|$, so S is finite also. By a symmetrical argument, $|T| \leq |S|$, so $|S| = |T|$. ♣

6.9.6 Proposition If S and T are arbitrary transcendence bases for E , then $|S| = |T|$. [The common value is called the *transcendence degree* of E/F .]

Proof. By (6.9.5), we may assume that S and T are both infinite. Let $T = \{y_i : i \in I\}$. If $x \in S$, then x depends algebraically on finitely many elements y_{i_1}, \dots, y_{i_r} in T . Define $I(x)$ to be the set of indices $\{i_1, \dots, i_r\}$. It follows that $I = \cup\{I(x) : x \in S\}$. For if j belongs to none of the $I(x)$, then we can remove y_j from T and the resulting set will still span E algebraically, contradicting (6.9.2) part (iii). Now an element of $\cup\{I(x) : x \in S\}$ is determined by selecting an element $x \in S$ and then choosing an index in $I(x)$. Since $I(x)$ is finite, we have $|I(x)| \leq \aleph_0$. Thus

$$|I| = |\bigcup\{I(x) : x \in S\}| \leq |S|\aleph_0 = |S|$$

since S is infinite. Thus $|T| \leq |S|$. By symmetry, $|S| = |T|$. ♣

6.9.7 Example Let $E = F(X_1, \dots, X_n)$ be the field of rational functions in the variables X_1, \dots, X_n with coefficients in F . If $f(X_1, \dots, X_n) = 0$, then f is the zero polynomial, so $S = \{X_1, \dots, X_n\}$ is an algebraically independent set. Since $E = F(S)$, E is algebraic over $F(S)$ and therefore S spans E algebraically. Thus S is a transcendence basis.

Now let $T = \{X_1^{u_1}, \dots, X_n^{u_n}\}$, where u_1, \dots, u_n are arbitrary positive integers. We claim that T is also a transcendence basis. As above, T is algebraically independent. Moreover, each X_i is algebraic over $F(T)$. To see what is going on, look at a concrete example, say $T = \{X_1^5, X_2^3, X_3^4\}$. If $f(Z) = Z^3 - X_2^3 \in F(T)[Z]$, then X_2 is a root of f , so X_2 , and similarly each X_i , is algebraic over $F(T)$. By (3.3.3), E is algebraic over $F(T)$, so T is a transcendence basis.

Problems For Section 6.9

1. If S is an algebraically independent subset of E over F , T spans E algebraically over F , and $S \subseteq T$, show that there is a transcendence basis B such that $S \subseteq B \subseteq T$.
2. Show that every algebraically independent set can be extended to a transcendence basis, and that every algebraically spanning set contains a transcendence basis.
3. Prove carefully, for an extension E/F and a subset $T = \{t_1, \dots, t_n\} \subseteq E$, that the following conditions are equivalent.
 - (i) T is algebraically independent over F ;
 - (ii) For every $i = 1, \dots, n$, t_i is transcendental over $F(T \setminus \{t_i\})$;
 - (iii) For every $i = 1, \dots, n$, t_i is transcendental over $F(t_1, \dots, t_{i-1})$ (where the statement for $i = 1$ is that t_1 is transcendental over F).
4. Let S be a subset of E that is algebraically independent over F . Show that if $t \in E$, then t is transcendental over $F(S)$ if and only if $S \cup \{t\}$ is algebraically independent over F .

[Problems 3 and 4 suggest the reasoning that is involved in formalizing the results of this section.]

5. Let $F \leq K \leq E$, with S a subset of K that is algebraically independent over F , and T a subset of E that is algebraically independent over K . Show that $S \cup T$ is algebraically independent over F , and $S \cap T = \emptyset$.
6. Let $F \leq K \leq E$, with S a transcendence basis for K/F and T a transcendence basis for E/K . Show that $S \cup T$ is a transcendence basis for E/F . Thus if tr deg abbreviates transcendence degree, then by Problem 5,

$$\text{tr deg}(E/F) = \text{tr deg}(K/F) + \text{tr deg}(E/K).$$

7. Let E be an extension of F , and $T = \{t_1, \dots, t_n\}$ a finite subset of E . Show that $F(T)$ is F -isomorphic to the rational function field $F(X_1, \dots, X_n)$ if and only if T is algebraically independent over F .
8. An *algebraic function field* F in one variable over K is a field F/K such that there exists $x \in F$

transcendental over K with $[F : K(x)] < \infty$. If $z \in F$, show that z is transcendental over K iff $[F : K(z)] < \infty$.

9. Find the transcendence degree of the complex field over the rationals.

Appendix To Chapter 6

We will develop a method for calculating the discriminant of a polynomial and apply the result to a cubic. We then calculate the Galois group of an arbitrary quartic.

A6.1 Definition If x_1, \dots, x_n ($n \geq 2$) are arbitrary elements of a field, the *Vandermonde determinant* of the x_i is

$$\det V = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$$

A6.2 Proposition

$$\det V = \prod_{i < j} (x_j - x_i).$$

Proof. $\det V$ is a polynomial h of degree $1 + 2 + \cdots + (n-1) = \binom{n}{2}$ in the variables x_1, \dots, x_n , as is $g = \prod_{i < j} (x_j - x_i)$. If $x_i = x_j$ for $i < j$, then the determinant is 0, so by the remainder theorem (2.5.2), each factor of g , hence g itself, divides h . Since h and g have the same degree, $h = cg$ for some constant c . Now look at the leading terms of h and g , i.e., those terms in which x_n appears to as high a power as possible, and subject to this constraint, x_{n-1} appears to as high a power as possible, etc. In both cases, the leading term is $x_2 x_3^2 \cdots x_n^{n-1}$, and therefore c must be 1. (For this step it is profitable to regard the x_i as abstract variables in a polynomial ring. Then monomials $x_1^{r_1} \cdots x_n^{r_n}$ with different sequences (r_1, \dots, r_n) of exponents are linearly independent.) ♣

A6.3 Corollary If f is a polynomial in $F[X]$ with roots x_1, \dots, x_n in some splitting field over F , then the discriminant of f is $(\det V)^2$.

Proof. By definition of the discriminant D of f (see 6.6.1), we have $D = \Delta^2$ where $\Delta = \pm \det V$. ♣

A6.4 Computation of the Discriminant

The square of the determinant of V is $\det(VV^t)$, which is the determinant of

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{bmatrix} \begin{bmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{bmatrix}$$

and this in turn is

$$\begin{vmatrix} t_0 & t_1 & \cdots & t_{n-1} \\ t_1 & t_2 & \cdots & t_n \\ \vdots & \vdots & \ddots & \vdots \\ t_{n-1} & t_n & \cdots & t_{2n-2} \end{vmatrix}$$

where the *power sums* t_r are given by

$$t_0 = n, \quad t_r = \sum_{i=1}^n x_i^r, \quad r \geq 1.$$

We must express the power sums in terms of the coefficients of the polynomial f . This will involve, improbably, an exercise in differential calculus. We have

$$F(z) = \prod_{i=1}^n (1 - x_i z) = \sum_{i=0}^n c_i z^i \quad \text{with } c_0 = 1;$$

the variable z ranges over real numbers. Take the logarithmic derivative of F to obtain

$$\frac{F'(z)}{F(z)} = \frac{d}{dz} \log F(z) = \sum_{i=1}^n \frac{-x_i}{1-x_i z} = - \sum_{i=1}^n \sum_{j=0}^{\infty} x_i^{j+1} z^j = - \sum_{j=0}^{\infty} t_{j+1} z^j.$$

Thus

$$F'(z) + F(z) \sum_{j=0}^{\infty} t_{j+1} z^j = 0,$$

that is,

$$\sum_{i=1}^n i c_i z^{i-1} + \sum_{i=0}^n c_i z^i \sum_{j=1}^{\infty} t_j z^{j-1} = 0.$$

Equating powers of z^{r-1} , we have, assuming that $n \geq r$,

$$r c_r + c_0 t_r + c_1 t_{r-1} + \cdots + c_{r-1} t_1 = 0; \quad (1)$$

if $r > n$, the first summation does not contribute, and we get

$$t_r + c_1 t_{r-1} + \cdots + c_n t_{r-n} = 0. \quad (2)$$

Our situation is a bit awkward here because the roots of $F(z)$ are the reciprocals of the x_i . The x_i are the roots of $\sum_{i=0}^n a_i z^i$ where $a_i = c_{n-i}$ (so that $a_n = c_0 = 1$). The results can be expressed as follows.

A6.5 Newton's Identities If $f(X) = \sum_{i=0}^n a_i X^i$ (with $a_n = 1$) is a polynomial with roots x_1, \dots, x_n , then the power sums t_i satisfy

$$t_r + a_{n-1} t_{r-1} + \cdots + a_{n-r+1} t_1 + r a_{n-r} = 0, \quad r \leq n \quad (3)$$

and

$$t_r + a_{n-1} t_{r-1} + \cdots + a_0 t_{r-n} = 0, \quad r > n. \quad (4)$$

A6.6 The Discriminant of a Cubic First consider the case where the X^2 term is missing, so that $f(X) = X^3 + pX + q$. Then $n = t_0 = 3$, $a_0 = q$, $a_1 = p$, $a_2 = 0$ ($a_3 = 1$). Newton's identities yield

$$t_1 + a_2 = 0, t_1 = 0; \quad t_2 + a_2 t_1 + 2a_1 = 0, t_2 = -2p;$$

$$t_3 + a_2 t_2 + a_1 t_1 + 3a_0 = 0, t_3 = -3a_0 = -3q;$$

$$t_4 + a_2 t_3 + a_1 t_2 + a_0 t_1 = 0, t_4 = -p(-2p) = 2p^2$$

$$D = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} = -4p^3 - 27q^2.$$

We now go to the general case $f(X) = X^3 + aX^2 + bX + c$. The quadratic term can be eliminated by the substitution $Y = X + \frac{a}{3}$. Then

$$\begin{aligned} f(X) &= g(Y) = (Y - \frac{a}{3})^3 + a(Y - \frac{a}{3})^2 + b(Y - \frac{a}{3}) + c \\ &= Y^3 + pY + q \quad \text{where} \quad p = b - \frac{a^2}{3}, q = \frac{2a^3}{27} - \frac{ba}{3} + c. \end{aligned}$$

Since the roots of f are translations of the roots of g by the same constant, the two polynomials have the same discriminant. Thus $D = -4p^3 - 27q^2$, which simplifies to

$$D = a^2(b^2 - 4ac) - 4b^3 - 27c^2 + 18abc.$$

We now consider the Galois group of a quartic $X^4 + aX^3 + bX^2 + cX + d$, assumed irreducible and separable over a field F . As above, the translation $Y = X + \frac{a}{4}$ eliminates the cubic term without changing the Galois group, so we may assume that $f(X) = X^4 + qX^2 + rX + s$. Let the roots of f be x_1, x_2, x_3, x_4 (distinct by separability), and let V be the four group, realized as the subgroup of S_4 containing the permutations $(1,2)(3,4)$, $(1,3)(2,4)$ and $(1,4)(2,3)$, along with the identity. By direct verification (i.e., brute force), $V \trianglelefteq S_4$. If G is the Galois group of f (regarded as a group of permutations of the roots), then $V \cap G \trianglelefteq G$ by the second isomorphism theorem.

A6.7 Lemma $\mathcal{F}(V \cap G) = F(u, v, w)$, where

$$u = (x_1 + x_2)(x_3 + x_4), \quad v = (x_1 + x_3)(x_2 + x_4), \quad w = (x_1 + x_4)(x_2 + x_3).$$

Proof. Any permutation in V fixes u, v and w , so $\mathcal{G}F(u, v, w) \supseteq V \cap G$. If $\sigma \in G$ but $\sigma \notin V \cap G$ then (again by direct verification) σ moves at least one of u, v, w . For example, $(1,2,3)$ sends u to w , and $(1,2)$ sends v to w . Thus $\sigma \notin \mathcal{G}F(u, v, w)$. Therefore $\mathcal{G}F(u, v, w) = V \cap G$, and an application of the fixed field operator \mathcal{F} completes the proof. ♣

A6.8 Definition The *resolvent cubic* of $f(X) = X^4 + qX^2 + rX + s$ is $g(X) = (X - u)(X - v)(X - w)$.

To compute g , we must express its coefficients in terms of q, r and s . First note that $u - v = -(x_1 - x_4)(x_2 - x_3)$, $u - w = -(x_1 - x_3)(x_2 - x_4)$, $v - w = -(x_1 - x_2)(x_3 - x_4)$. Thus f and g have the same discriminant. Now

$$X^4 + qX^2 + rX + s = (X^2 + kX + l)(X^2 - kX + m)$$

where the appearance of k and $-k$ is explained by the missing cubic term. Equating coefficients gives $l + m - k^2 = q$, $k(m - l) = r$, $lm = s$. Solving the first two equations for m and adding, we have $2m = k^2 + q + r/k$, and solving the first two equations for l and adding, we get $2l = k^2 + q - r/k$. Multiply the last two equations and use $lm = s$ to get a cubic in k^2 , namely

$$k^6 + 2qk^4 + (q^2 - 4s)k^2 - r^2 = 0.$$

(This gives a method for actually finding the roots of a quartic.) To summarize,

$$f(X) = (X^2 + kX + l)(X^2 - kX + m)$$

where k^2 is a root of

$$h(X) = X^3 + 2qX^2 + (q^2 - 4s)X - r^2.$$

We claim that the roots of h are simply $-u, -v, -w$. For if we arrange the roots of f so that x_1 and x_2 are the roots of $X^2 + kX + l$, and x_3 and x_4 are the roots of $X^2 - kX + m$, then $k = -(x_1 + x_2)$, $-k = -(x_3 + x_4)$, so $-u = k^2$. The argument for $-v$ and $-w$ is similar. Therefore to get g from h , we simply change the sign of the quadratic and constant terms, and leave the linear term alone.

A6.9 An Explicit Formula For The Resolvent Cubic:

$$g(X) = X^3 - 2qX^2 + (q^2 - 4s)X + r^2.$$

We need some results concerning subgroups of S_n , $n \geq 3$.

A6.10 Lemma

- (i) A_n is generated by 3-cycles, and every 3-cycle is a commutator.
- (ii) The only subgroup of S_n with index 2 is A_n .

Proof. For the first assertion of (i), see Section 5.6, Problem 4. For the second assertion of (i), note that

$$(a, b)(a, c)(a, b)^{-1}(a, c)^{-1} = (a, b)(a, c)(a, b)(a, c) = (a, b, c).$$

To prove (ii), let H be a subgroup of S_n with index 2; H is normal by Section 1.3, Problem 6. Thus S_n/H has order 2, hence is abelian. But then by (5.7.2), part 5, $S'_n \leq H$, and since A_n also has index 2, the same argument gives $S'_n \leq A_n$. By (i), $A_n \leq S'_n$, so $A_n = S'_n \leq H$. Since A_n and H have the same finite number of elements $n!/2$, it follows that $H = A_n$. ♣

A6.11 Proposition Let G be a subgroup of S_4 whose order is a multiple of 4, and let V be the four group (see the discussion preceding A6.7). Let m be the order of the quotient group $G/(G \cap V)$. Then

- (a) If $m = 6$, then $G = S_4$;
- (b) If $m = 3$, then $G = A_4$;
- (c) If $m = 1$, then $G = V$;
- (d) If $m = 2$, then $G = D_8$ or \mathbb{Z}_4 or V ;
- (e) If G acts transitively on $\{1, 2, 3, 4\}$, then the case $G = V$ is excluded in (d). [In all cases, equality is up to isomorphism.]

Proof. If $m = 6$ or 3 , then since $|G| = m|G \cap V|$, 3 is a divisor of $|G|$. By hypothesis, 4 is also a divisor, so $|G|$ is a multiple of 12. By A6.10 part (ii), G must be S_4 or A_4 . But

$$|S_4/(S_4 \cap V)| = |S_4/V| = 24/4 = 6$$

and

$$|A_4/(A_4 \cap V)| = |A_4/V| = 12/4 = 3$$

proving both (a) and (b). If $m = 1$, then $G = G \cap V$, so $G \leq V$, and since $|G|$ is a multiple of 4 and $|V| = 4$, we have $G = V$, proving (c).

If $m = 2$, then $|G| = 2|G \cap V|$, and since $|V| = 4$, $|G \cap V|$ is 1, 2 or 4. If it is 1, then $|G| = 2 \times 1 = 2$, contradicting the hypothesis. If it is 2, then $|G| = 2 \times 2 = 4$, and $G = \mathbb{Z}_4$ or V (the only groups of order 4). Finally, assume $|G \cap V| = 4$, so $|G| = 8$. But a subgroup of S_4 of order 8 is a Sylow 2-subgroup, and all such subgroups are conjugate and therefore isomorphic. One of these subgroups is D_8 , since the dihedral group of order 8 is a group of permutations of the 4 vertices of a square. This proves (d).

If $m = 2$, G acts transitively on $\{1, 2, 3, 4\}$ and $|G| = 4$, then by the orbit-stabilizer theorem, each stabilizer subgroup $G(x)$ is trivial (since there is only one orbit, and its size is 4). Thus every permutation in G except the identity moves every integer 1, 2, 3, 4. Since $|G \cap V| = 2$, G consists of the identity, one other element of V , and two elements not in V , which must be 4-cycles. But a 4-cycle has order 4, so G must be cyclic, proving (e). ♣

A6.12 Theorem Let f be an irreducible separable quartic, with Galois group G . Let m be the order of the Galois group of the resolvent cubic. Then:

- (a) If $m = 6$, then $G = S_4$;
- (b) If $m = 3$, then $G = A_4$;
- (c) If $m = 1$, then $G = V$;
- (d) If $m = 2$ and f is irreducible over $L = F(u, v, w)$, where u, v and w are the roots of the resolvent cubic, then $G = D_8$;
- (e) If $m = 2$ and f is reducible over L , then $G = \mathbb{Z}_4$.

Proof. By A6.7 and the fundamental theorem, $[G : G \cap V] = [L : F]$. Now the roots of the resolvent cubic g are distinct, since f and g have the same discriminant. Thus L is a splitting field of a separable polynomial, so L/F is Galois. Consequently, $[L : F] = m$ by (3.5.9). To apply (A6.11), we must verify that $|G|$ is a multiple of 4. But this follows from the orbit-stabilizer theorem: since G acts transitively on the roots of f , there is only one orbit, of size $4 = |G|/|G(x)|$. Now (A6.11) yields (a), (b) and (c), and if $m = 2$, then $G = D_8$ or \mathbb{Z}_4 .

To complete the proof, assume that $m = 2$ and $G = D_8$. Thinking of D_8 as the group of symmetries of a square with vertices 1, 2, 3, 4, we can take D_8 to be generated by $(1, 2, 3, 4)$ and $(2, 4)$, with $V = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$. The elements of V are symmetries of the square, hence belong to D_8 ; thus $V = G \cap V = \text{Gal}(E/L)$ by (A6.7). [E is a splitting field for f over F .] Since V is transitive, for each $i, j = 1, 2, 3, 4, i \neq j$, there is an L -automorphism τ of E such that $\tau(x_i) = x_j$. Applying τ to the

equation $h(x_i) = 0$, where h is the minimal polynomial of x_i over L , we see that each x_j is a root of h , and therefore $f|h$. But $h|f$ by minimality of h , so $h = f$, proving that f is irreducible over L .

Finally, assume $m = 2$ and $G = \mathbb{Z}_4$, which we take as $\{1, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)\}$. Then $G \cap V = \{1, (1, 3)(2, 4)\}$, which is not transitive. Thus for some $i \neq j$, x_i and x_j are not roots of the same irreducible polynomial over L . In particular, f is reducible over L . ♣

A6.13 Example Let $f(X) = X^4 + 3X^2 + 2X + 1$ over \mathbb{Q} , with $q = 3, r = 2, s = 1$. The resolvent cubic is, by (A6.9), $g(X) = X^3 - 6X^2 + 5X + 4$. To calculate the discriminant of g , we can use the general formula in (A6.6), or compute $g(X + 2) = (X + 2)^3 - 6(X + 2)^2 + 5(X + 2) + 4 = X^3 - 7X - 2$. [The rational root test gives irreducibility of g and restricts a factorization of f to $(X^2 + aX \pm 1)(X^2 - aX \pm 1)$, $a \in \mathbb{Z}$, which is impossible. Thus f is irreducible as well.] We have $D(g) = -4(-7)^3 - 27(-2)^2 = 1264$, which is not a square in \mathbb{Q} . Thus $m = 6$, so the Galois group of f is S_4 .