and irreducible, show that $q(x)$ can be determined from $p(x)$ by checking for p^{th} powers and by computing greatest common divisors with derivatives.]

13. Let $g(x) \in \mathbb{F}_p[x]$ be any polynomial of degree $< n$. Denote by $R(h(x))$ the remainder of $h(x)$ after division by $f(x)$. Prove the following are equivalent:

(a) $R(g(x^p)) = g(x)$.

(b) $f(x)$ divides $[g(x)-0][g(x)-1]\ldots[g(x)-(p-1)]$. [Use the fact that $g(x^p) = g(x)^p$ together with the factorization of $x^p - x$ in $\mathbb{F}_p[x]$.]

(c) $p_i(x)$ divides the product in (b) for $i = 1, 2, \ldots, k$.

(d) For each i, $i = 1, 2, \ldots, k$ there is an $s_i \in \mathbb{F}_p$ such that $p_i(x)$ divides $g(x) - s_i$, i.e., $g(x) \equiv s_i \pmod{p_i(x)}$.

14. Prove that the polynomials $g(x)$ of degree $< n$ satisfying the equivalent conditions of the previous exercise form a vector space V over $\mathbb{F}_p$ of dimension k. [Use the Chinese Remainder Theorem applied to the p^k possible choices for the s_i in 13(d)].

15. Let $g(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \in V$. For $j = 0, 1, \ldots, n-1$ let

$$R(x^{pj}) = a_{0,j} + a_{1,j}x + \cdots + a_{n-1,j}x^{n-1}$$

and let A be the $n \times n$ matrix

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,0} & a_{n-1,1} & \cdots & a_{n-1,n-1} \end{pmatrix}. \qquad (*)$$

Show that condition (a) of Exercise 13 for $g(x) \in V$ is equivalent to

$$(A - I)B = 0 \qquad (**)$$

where B is the column matrix with entries $b_0, b_1, \ldots, b_{n-1}$. Conclude that the rank of the matrix $A - I$ is $n - k$. Note that this already suffices to determine if $f(x)$ is irreducible, without actually determining the factors.

16. Let $g_1(x), g_2(x), \ldots, g_k(x)$ be a basis of solutions to $(**)$ (so a basis for V), where we may take $g_1(x) = 1$. Beginning with $w(x) = f(x)$, compute the greatest common divisor $(w(x), g_i(x) - s)$ for $i = 2, 3, \ldots, k$ and $s \in \mathbb{F}_p$ for every factor of $f(x)$ already computed. Note by Exercise 13(d) that every factor $p_i(x)$ of $f(x)$ divides such a g.c.d. The process terminates when k relatively prime factors have been determined.

Prove that this procedure actually gives all the factors $p_1(x), p_2(x), \ldots, p_k(x)$, i.e., one can separate the individual factors $p_1(x), p_2(x), \ldots, p_k(x)$ by this procedure, as follows:

If this were not the case, then for two of the factors, say $p_1(x)$ and $p_2(x)$, for each $i = 1, 2, \ldots, k$ there would exist $s_i \in \mathbb{F}_p$ such that $g_i(x) - s_i$ is divisible by both $p_1(x)$ and $p_2(x)$. By the Chinese Remainder Theorem, choose a $g(x) \in V$ satisfying $g(x) \equiv 0 \pmod{p_1(x)}$ and $g(x) \equiv 1 \pmod{p_2(x)}$. Write $g(x) = \sum_{i=1}^{k} c_i g_i(x)$ in terms of the basis for V and let $s = \sum_{i=1}^{k} c_i s_i(x) \in \mathbb{F}_p$. Show that $s \equiv 0 \pmod{p_1(x)}$ so that $s = 0$ and $s \equiv 1 \pmod{p_2(x)}$ so that $s = 1$, a contradiction.

17. This exercise follows Berlekamp's Factorization Algorithm outlined in the previous exercises to determine the factorization of $f(x) = x^5 + x^2 + 4x + 6$ in $\mathbb{F}_7[x]$.

(a) Show that $x^7 \equiv x^2 + 3x^3 + 6x^4 \pmod{f(x)}$. Similarly compute x^{14}, x^{21}, and x^{28} modulo $f(x)$ (note that x^{14} can most easily be computed by squaring the result for

x^7 and then reducing, etc.) to show that in this case the matrix A in Exercise 15 is

$$\begin{pmatrix} 1 & 0 & 5 & 1 & 4 \\ 0 & 0 & 1 & 1 & 2 \\ 0 & 1 & 3 & 3 & 3 \\ 0 & 3 & 4 & 2 & 2 \\ 0 & 6 & 3 & 1 & 1 \end{pmatrix}.$$

(b) Show that the reduced row echelon form for $A - I$ is the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 6 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Conclude that $k = 2$ (so $f(x)$ is the product of precisely two factors which are powers of irreducible polynomials) and that $g_1(x) = 1$ and $g_2(x) = x^4 + 5x^3 + x^2 + x$ give a basis for the solutions to $(**)$ in Exercise 15.

(c) Following the procedure in Exercise 16, show that $(f(x), g_2(x) - 1) = x^2 + 3x + 5 = p_1(x)$, with $f(x)/p_1(x) = x^3 + 4x^2 + 4x + 4 = p_2(x)$, giving the powers of the irreducible polynomials dividing $f(x)$ in $\mathbb{F}_7[x]$. Show that neither factor is a 7^{th} power in $\mathbb{F}_7[x]$ and that each is relatively prime to its derivative to conclude that both factors are irreducible polynomials, giving the complete factorization of $f(x)$ into irreducible polynomials:

$$f(x) = (x^2 + 3x + 5)(x^3 + 4x^2 + 4x + 4) \in \mathbb{F}_7[x].$$

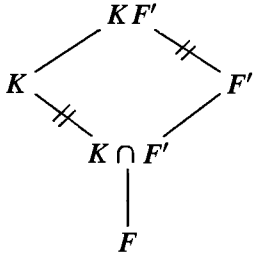
14.4 COMPOSITE EXTENSIONS AND SIMPLE EXTENSIONS

We now consider the effect of taking composites with Galois extensions. The first result states that "sliding up" a Galois extension gives a Galois extension.

Proposition 19. Suppose K/F is a Galois extension and F'/F is any extension. Then KF'/F' is a Galois extension, with Galois group

$$\text{Gal}(KF'/F') \cong \text{Gal}(K/K \cap F')$$

isomorphic to a subgroup of $\text{Gal}(K/F)$. Pictorially,



Proof: If K/F is Galois, then K is the splitting field of some separable polynomial $f(x)$ in $F[x]$. Then KF'/F' is the splitting field of $f(x)$ viewed as a polynomial in

$F'[x]$, hence this extension is Galois. Since K/F is Galois, every embedding of K fixing F is an automorphism of K, so the map

$$\varphi : \mathrm{Gal}(KF'/F') \to \mathrm{Gal}(K/F)$$
$$\sigma \mapsto \sigma|_K$$

defined by restricting an automorphism σ to the subfield K is well defined. It is clearly a homomorphism, with kernel

$$\ker \varphi = \{\sigma \in \mathrm{Gal}(KF'/F') \mid \sigma|_K = 1\}.$$

Since an element in $\mathrm{Gal}(KF'/F')$ is trivial on F', the elements in the kernel are trivial both on K and on F', hence on their composite, so the kernel consists only of the identity automorphism. Hence φ is injective.

Let H denote the image of φ in $\mathrm{Gal}(K/F)$ and let K_H denote the corresponding fixed subfield of K containing F. Since every element in H fixes F', K_H contains $K \cap F'$. On the other hand, the composite $K_H F'$ is fixed by $\mathrm{Gal}(KF'/F')$ (any $\sigma \in \mathrm{Gal}(KF'/F')$ fixes F' and acts on $K_H \subseteq K$ via its restriction $\sigma|_K \in H$, which fixes K_H by definition). By the Fundamental Theorem it follows that $K_H F' = F'$, so that $K_H \subseteq F'$, which gives the reverse inclusion $K_H \subseteq K \cap F'$. Hence $K_H = K \cap F'$, so again by the Fundamental Theorem, $H = \mathrm{Gal}(K/K \cap F')$, completing the proof.

Corollary 20. Suppose K/F is a Galois extension and F'/F is any finite extension. Then

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}.$$

Proof: This follows by the proposition from the equality $[KF' : F'] = [K : K \cap F']$ given by the orders of the Galois groups in the proposition.

The example $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$, $F' = \mathbb{Q}(\rho\sqrt[3]{2})$, ρ a primitive 3rd root of unity, shows that the formula of Corollary 20 does not hold in general if neither of the two extensions is Galois.

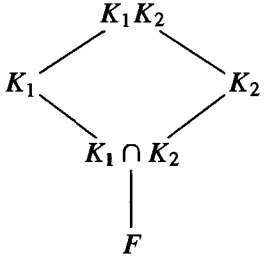
Proposition 21. Let K_1 and K_2 be Galois extensions of a field F. Then

(1) The intersection $K_1 \cap K_2$ is Galois over F.

(2) The composite K_1K_2 is Galois over F. The Galois group is isomorphic to the subgroup

$$H = \{(\sigma, \tau) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$$

of the direct product $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ consisting of elements whose restrictions to the intersection $K_1 \cap K_2$ are equal.



Proof: (1) Suppose $p(x)$ is an irreducible polynomial in $F[x]$ with a root α in $K_1 \cap K_2$. Since $\alpha \in K_1$ and K_1/F is Galois, all the roots of $p(x)$ lie in K_1. Similarly all the roots lie in K_2, hence all the roots of $p(x)$ lie in $K_1 \cap K_2$. It follows easily that $K_1 \cap K_2$ is Galois as in Theorem 13.

(2) If K_1 is the splitting field of the separable polynomial $f_1(x)$ and K_2 is the splitting field of the separable polynomial $f_2(x)$ then the composite is the splitting field for the squarefree part of the polynomial $f_1(x)f_2(x)$, hence is Galois over F.

The map

$$\varphi : \mathrm{Gal}(K_1K_2/F) \to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$
$$\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

is clearly a homomorphism. The kernel consists of the elements σ which are trivial on both K_1 and K_2, hence trivial on the composite, so the map is injective. The image lies in the subgroup H, since

$$(\sigma|_{K_1})|_{K_1\cap K_2} = \sigma|_{K_1\cap K_2} = (\sigma|_{K_2})|_{K_1\cap K_2}.$$

The order of H can be computed by observing that for every $\sigma \in \mathrm{Gal}(K_1/F)$ there are $|\mathrm{Gal}(K_2/K_1 \cap K_2)|$ elements $\tau \in \mathrm{Gal}(K_2/F)$ whose restrictions to $K_1 \cap K_2$ are $\sigma|_{K_1\cap K_2}$. Hence

$$|H| = |\mathrm{Gal}(K_1/F)| \cdot |\mathrm{Gal}(K_2/K_1 \cap K_2)|$$
$$= |\mathrm{Gal}(K_1/F)| \frac{|\mathrm{Gal}(K_2/F)|}{|\mathrm{Gal}(K_1 \cap K_2/F)|}.$$

By Corollary 20 and the diagram above we see that the orders of H and $\mathrm{Gal}(K_1K_2/F)$ are then both equal to

$$[K_1K_2 : F] = \frac{[K_1 : F][K_2 : F]}{[K_1 \cap K_2 : F]}.$$

Hence the image of φ is precisely H, completing the proof.

Corollary 22. Let K_1 and K_2 be Galois extensions of a field F with $K_1 \cap K_2 = F$. Then

$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Conversely, if K is Galois over F and $G = \mathrm{Gal}(K/F) = G_1 \times G_2$ is the direct product of two subgroups G_1 and G_2, then K is the composite of two Galois extensions K_1 and K_2 of F with $K_1 \cap K_2 = F$.

Proof: The first part follows immediately from the proposition. For the second, let K_1 be the fixed field of $G_1 \subset G$ and let K_2 be the fixed field of $G_2 \subset G$. Then $K_1 \cap K_2$ is the field corresponding to the subgroup G_1G_2, which is all of G in this case, so $K_1 \cap K_2 = F$. The composite K_1K_2 is the field corresponding to the subgroup $G_1 \cap G_2$, which is the identity here, so $K_1K_2 = K$, completing the proof.