CHAPTER IX

APPLICATIONS OF GALOIS THEORY

1. Finite Fields

Let F be a finite field. It is necessarily of nonzero characteristic p and its prime field is the field with p elements $\mathbf{F}_p$. Since F is a vector space over $\mathbf{F}_p$, it must have $q = p^r$ elements where $r = [F : \mathbf{F}_p]$. More generally, if $E \supseteq F$ are both finite, then E has q^d elements where $d = [E : F]$.

As we mentioned earlier, the multiplicative group F^* of F is cyclic (because it is a finite subgroup of the multiplicative group of a field), and clearly its order is $q - 1$. Hence each non-zero element of F is a root of the polynomial $X^{q-1} - 1$. Since 0 is the only root of the polynomial X, it follows that the q elements of F are roots of the polynomial $X^q - X = X(X^{q-1} - 1)$. Hence, that polynomial is separable and F consists of the set of its roots. (You can also see that it must be separable by finding its derivative which is -1.) We may now conclude that the finite field F is the splitting field over $\mathbf{F}_p$ of the separable polynomial $X^q - X$ where $q = |F|$. In particular, it is unique up to isomorphism. We have proved the first part of the following result.

PROPOSITION. *Let p be a prime. For each $q = p^r$, there is a unique (up to isomorphism) finite field F with $|F| = q$.*

PROOF. We have already proved the uniqueness. Suppose $q = p^r$, and consider the polynomial $X^q - X \in \mathbf{F}_p[X]$. As mentioned above $Df(X) = -1$ so $f(X)$ cannot have any repeated roots in any extension, i.e. it is separable. Let F be its splitting field over $\mathbf{F}_p$. We have $F = \mathbf{F}_p[x_1, \ldots, x_q]$ where $x_1, \ldots, x_q$ are the q distinct roots of $f(X)$. However, it is not hard to see that the set $\{x_1, \ldots, x_q\}$ is in fact already a field. For, x is a root of $f(X) = X^q - X$ if and only if $x^q = x$, and the fact that raising to the qth power is a ring homomorphism in characteristic p (i.e., $(x + y)^q = x^q + y^q$ and $(xy)^q = x^q y^q$) tells us that the set of roots is a subring. If $x \neq 0$, we have $(x^{-1})^q = (x^q)^{-1} = x^{-1}$, so every element in this subring is invertible in the subring. Hence F is the set of roots of $f(X)$ and has q elements as claimed. □

We want to fit all these finite fields in the same field and show how they are related to one another. To this end, we shall use a result to be proved later. Namely, if F is any field, then we shall show later that there is an algebraic extension $\overline{F}$ which is algebraically closed and which is unique up to F-isomorphism. Such an extension is called an *algebraic closure* of F, or with abuse of terminology *the* algebraic closure of F. Let Ω_p denote the algebraic closure of the prime field $\mathbf{F}_p$. For any $q = p^r$ there is a unique subfield of Ω_p isomorphic to every field with q elements, namely the splitting filed of $X^q - X$ over $\mathbf{F}_p$. We shall denote this instance of a field with q elements by $\mathbf{F}_q$.

The finite fields $\mathbf{F}_q$ are coherently related. Namely, first suppose that $\mathbf{F}_q \subseteq \mathbf{F}_{q'}$. The the latter may be viewed as a vector space over the former of dimension $d = [\mathbf{F}'_q : \mathbf{F}_q]$. That is, $\mathbf{F}'_q$ is isomorphic to a direct sum of d copies of $\mathbf{F}_q$a, whence $q' = |\mathbf{F}'_q| = |\mathbf{F}_q|^d = q^d$, or $p^{r'} = p^{rd}$. It follows that r divides r'.

Conversely, suppose r divides r', i.e. $r' = rd, q = p^r$, and $q' = p^{r'} = q^d$. We claim that $\mathbf{F}_q \subseteq \mathbf{F}_{q'}$. To see this note that the latter is the splitting field over $\mathbf{F}_p$ of $X^{q^d} - X$ and the former is the splitting field of $X^1 - X$. However, dividing yields

$$\frac{X^{q^d} - X}{X^q - X} = \frac{X^{q^d-1} - 1}{X^{q-1} - 1} = X^{(q-1)(k-1)} + X^{(q-1)(k-2)} + \cdots + X^{q-1} + 1$$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

where $k = (q^d - 1)/(q - 1) = q^{d-1} + q^{d-2} + \cdots + q + 1$. (Note the confusing double use of the formula for a geometric sum!) It follows that $X^q - X$ divides $X^{q'} - X$ so any splitting field of the latter contains a splitting field of the former. Hence, by the uniqueness of splitting fields in Ω_p, $\mathbf{F}_{q'} \supseteq \mathbf{F}_q$ as claimed.

Remark. Ω_p is in fact the union of the finite subfields $\mathbf{F}_q$ where $q = p^r$. For, it is algebraic over $\mathbf{F}_p$ by definition, so any element is in a finite extension of $\mathbf{F}_p$, hence in a finite subfield of Ω_p. However, the above analysis assures us that the fields $\mathbf{F}_q$ are the only such subfields.

We are now in a position to calculate the Galois group $G(\mathbf{F}_{q'}/\mathbf{F}_q)$ in the case $q' = q^d$. First, define $\phi_q : \Omega_p \to \Omega_p$ by $\phi_q(x) = x^q$. It is not hard to see that ϕ_q is a ring homomorphism, so at the very least it is a monomorphism. It is in fact also an epimorphism and hence an automorphism of Ω_p. (See the exercises.)

THEOREM. *Let $q' = q^d$ where $q = p^r$ for a given prime p. The restriction of ϕ_q to $\mathbf{F}_{q'}$ is an automorphism of $\mathbf{F}_{q'}$ and it generates the Galois group $G(\mathbf{F}_{q'}/\mathbf{F}_q)$ which is cyclic of order d.*

PROOF. First note that ϕ_q fixes $\mathbf{F}_q$ which is the set of elements in Ω_p satisfying $x^q = x$. It is also not hard to see that it carries $\mathbf{F}_{q^d}$ into itself. Since it is a monomorphism and that field is finite, its restriction is an automorphism of $\mathbf{F}_{q^d}$. Moreover, we have

$$\phi_q^i(x) = x^{q^i} \text{ so } \phi_q = \mathrm{Id} \iff x^{q^i} = x \text{ for all } x \in \mathbf{F}_{q^d}.$$

If this were to happen for some $i < d$, $\mathbf{F}_q$ would in fact have q^i elements instead which is nonsense. Hence, the restriction of ϕ_q has order d. On the other hand, $[\mathbf{F}_{q'} : \mathbf{F}_q] = d$, so by Galois's main theorem $|G(\mathbf{F}_{q'}/\mathbf{F}_q)|$ has order d and hence is generated by ϕ_q. □

Exercises.

1. Verify explicitly that $\phi_q : \Omega_p \to \Omega_p$ preserves sums, products, and the identity element $1 \in \Omega_p$.

2. Show that $\phi_q : \Omega_p \to \Omega_p$ is an epimorphism, hence an automorphism. (You already know from the discussion in the text that it is a monomorphism.)

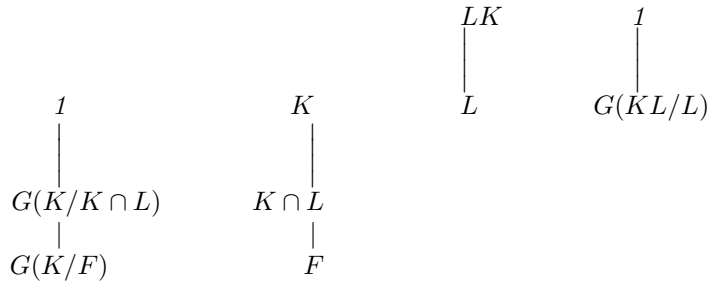
3. (a) An automorphism σ of Ω_p is specified if we know its restriction σ_d to every $\mathbf{F}_q$ with $q = p^d$. Also, if $d' = cd, q = p^d$, and $q' = p^{d'}$, then the restriction of $\sigma_{d'}$ to $\mathbf{F}_q$ must be σ_d. Suppose conversely, that we are given for each positive integer d an automorphism σ_d of $\mathbf{F}_{p^d}$, and that the family of all σ_d satisfies the consistency condition just enunciated. Show that there is an automorphism σ of Ω_p which restricts to σ_d on $\mathbf{F}_{p^d}$ for every d.

(b) Is every such σ a power of Φ; i.e., is $G(\Omega_p/\mathbf{F}_p)$ cyclic with generator Φ? Hint: This is not easy.

2. Extension of the base field

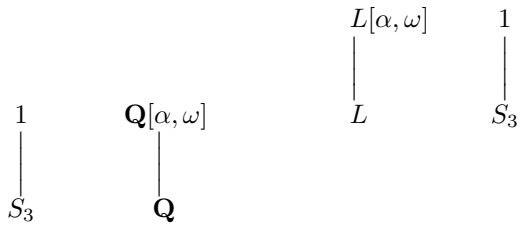
Let $K \supseteq F$ be a finite, normal separable extension. We often want to know what happens to the Galois group when we extend F to a larger field L which may not even be algebraic over F. For example, the extension $\mathbf{Q}[i] \supseteq \mathbf{Q}$ is normal and separable with Galois group cyclic of order 2. Similarly, we can say the same for $\mathbf{R}[i] \supseteq \mathbf{R}$, and in fact there is a natural way to identify the two Galois groups. The first problem in dealing with this situation in general is that there is no reason even to assume that K and L can be imbedded in the same field. Assume then that there is a field Ω which contains both K and L. (In the example, all the fields are contained in $\mathbf{C}$.) We denote by KL the smallest *subring* of Ω which contains both K and L. (This definition is not quite standard!) KL as before is the set of finite sums $\sum x_i y_i$ with $x_i \in K$ and $y_i \in L$ and it would ordinarily not be a subfield of Ω; we would have to form fractions in order to get a field. However, if $K \supseteq F$ is finite then $K = F[x_1, \ldots, x_n]$ for appropriate elements of K, so $KL = L[x_1, \ldots, x_n]$ is in fact finite over L and is thereby a field. In this case we shall call KL the *compositum* of K and L. Note that we could have extensions $K' \supseteq F$ and $L' \supseteq F$ which are F-isomorphic to the previous extensions with K' and L' contained in some field Ω' but with $K'L'$ not isomorphic to KL. This seems paradoxical, but it can happen since the construction of KL depends to some extent on the common enclosing field Ω. We shall analyze this situation in more detail when we discuss ring theory later in this course.

THEOREM. *(Natural Irrationalities). Let $K \supseteq F$ be a finite, normal, separable extension, and let L be an extension of F such that K and L are contained in a common field. Then $KL \supseteq L$ is a finite, normal, separable extension. Moreover, restricting L-automorphisms of KL to K yields a monomorphism $G(KL/L) \to G(K/L)$, and the image is $G(K/K \cap L)$.*



PROOF. First note that KL is normal over L. For, we can write $K = F[x_1, \ldots, x_k]$ as generated by the roots of a separable polynomial with coefficients in F; hence $KL = L[x_1, \ldots, x_k]$ is also such a splitting field over L. Let $\sigma \in G(KL/L)$. The restriction of σ to K certainly fixes F and by normality it must carry K into itself; so it is an element $\sigma' \in G(K/F)$. σ is certainly completely determined by its effect on $x_1, \ldots, x_k$ and since these are in K, it is determined by its restriction σ' to K. Hence $\sigma \mapsto \sigma'$ is a monomorphism. An element $x \in K$ is fixed by the subgroup which is the image of this monomorphism if and only if it is fixed by all $\sigma \in G(KL/L)$, i.e., if and only if $x \in L$. But since $x \in K$ in any case, this holds if and only if $x \in K \cap L$. By Galois's Main Theorem, the image subgroup must be $G(K/K \cap L)$. □

EXAMPLE 1. Let $\alpha = \sqrt[3]{2}$ and let $\omega = e^{(2\pi i)/3}$ as earlier. Let $L = \mathbf{Q}(\pi)$. We use the fact that π is not algebraic to conclude that $L \cap K = \mathbf{Q}$ in this case. (Can you prove it?) Hence the diagram looks like



EXAMPLE 2. Let $K \supseteq \mathbf{Q}$ be a finite, normal, separable extension contained in $\mathbf{C}$. Then $K \cap \mathbf{R}$ is the maximal real subfield of K. If K is real then $K\mathbf{R} = \mathbf{R}$ and nothing interesting occurs. If K is not contained in $\mathbf{R}$, then we must have $K\mathbf{R} = \mathbf{C}$ since it its a proper extension of $\mathbf{R}$ and $\mathbf{C}$ is the only such algebraic extension. It follows that $G(K/\mathbf{Q})$ has a subgroup of order 2 generated by the restriction of complex conjugation.

Exercises.

1. (a) Let K be a field and let P and Q be groups of automorphisms of K. Show that $K^{PQ} = K^P \cap K^Q$.

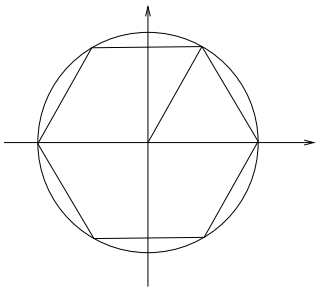
(b) Let $K \supseteq F$ be a field extension and let L and M be intermediate fields. Show that $G(K/LM) = G(K/L) \cap G(K/M)$.

(c) Suppose that $K \supseteq F$ is a finite normal separable extension. Conclude that in the Galois correspondence between subgroups of $G(K/F)$ and intermediate subfields, intersections of subgroups correspond to composita of subfields and products of subgroups correspond to intersections of subfields.

2. Prove that if K and N are finite normal extensions of F both contained in the same field Ω, then the compositum KN is normal over F.

3. Cyclotomic extensions

A root of the polynomial $X^n - 1$ for some $n > 0$ is called a *root of unity*. For example, in $\mathbf{C}$, if we put $\theta = 2\pi/n$, then $X^n - 1$ has the n roots $e^{ik\theta}$, $k = 0, 1, \ldots, n-1$. These appear in the complex plane as the vertices of a regular n-gon inscribed in the unit circle.



Let the base field have characteristic p. If $p \mid n$ then

$$D(X^n - 1) = nX^{n-1} = 0$$

so $X^n - 1$ is not separable. Conversely, if p does not divide n, then $X^n - 1$ and nX^{n-1} clearly have no roots in common, so $X^n - 1$ is separable. For this reason, we shall always assume when discussing nth roots of unity that $\gcd(p, n) = 1$ if $p > 0$. Of course, if the characteristic is 0, there is no need for any extra assumption.

Let K be an extension of F. The roots of $X^n - 1$ in K are distinct (assuming as above that $\gcd(p, n) = 1$), and it is clear that they form a subgroup of K^* under multiplication. Hence, the set of roots forms a cyclic group of order $\leq n$. Assume further that $X^n - 1$ splits completely in K. Then, the order of this group is n. In that case, a generator ζ of the group of nth roots of unity in K is called a *primitive* nth root of unity. Every root is then a power ζ^i with $0 \leq i \leq n-1$, and such a power is also primitive (i.e. a generator) if and only if $\gcd(i, n) = 1$. It follows that the number of primitive roots is $\phi(n)$ where ϕ is the Euler ϕ– function. Moreover, again since the roots are all powers of ζ, we have in $K[X]$

$$X^n - 1 = \prod_{i=0}^{n-1} (X - \zeta^i)$$

Note that this splitting already takes place in $F[\zeta]$ which is a splitting field for $X^n - 1$. $F[\zeta]$ is called a *cyclotomic* extension of F. Notice that the existence of a primitive nth root of unity in some extension of F implies that $X^n - 1$ has distinct roots, so it is separable and necessarily n is relatively prime to the characteristic of F.

THEOREM. *Let n be relatively prime to the characteristic of F. Let ζ be a primitive nth root of unity. Then $G(F[\zeta]/F)$ is isomorphic to a subgroup of $U(\mathbf{Z}/n\mathbf{Z})$ (the group of units of $\mathbf{Z}/n\mathbf{Z}$) and hence is abelian of order dividing $\phi(n)$.*

PROOF. $\sigma \in G = G(F[\zeta]/F)$ is completely determined by its effect on ζ. Since σ is an automorphism, $\sigma(\zeta)$ must also be a primitive root so we have $\sigma(\zeta) = \zeta^i$ where $i = i_\sigma$ is relatively prime to n. Define a map $\nu : G \to U(\mathbf{Z}/n\mathbf{Z})$ by $\nu(\sigma) = i_\sigma \bmod n$. As just noted, ν is one-to-one. It is also a homomorphism since if $\sigma(\zeta) = \zeta^i$ and $\tau(\zeta) = \zeta^j$, then $\tau\sigma(\zeta) = \tau(\zeta^i) = \tau(\zeta)^i = (\zeta^j)^i = \zeta^{ji}$. Hence $\nu(\tau\sigma) = ji \bmod n = \nu(\tau)\nu(\sigma)$. □

REMARKS. As we discovered last quarter (in an exercise), $U(\mathbf{Z}/n\mathbf{Z})$ is often *cyclic*. In fact that will be true if n is an odd prime power or twice an odd prime power or if $n = 2$ or 4. Hence, in those cases the Galois group of the cyclotomic extension is also cyclic. In all other cases, the group of units is abelian but non-cyclic, so the Galois group need not be cyclic. (Of course, depending on F, it could turn out to be cyclic.)

THEOREM. *If ζ is a primitive nth root of unity in some extension of $\mathbf{Q}$, then $G(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong U(\mathbf{Z}/n\mathbf{Z})$. In particular, it is of order $\phi(n)$.*

PROOF. By Galois's Main Theorem, it suffices to show that $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \phi(n)$. This turns out to be rather difficult.

Let $\Phi(X)$ denote the minimal polynomial of ζ over $\mathbf{Q}$. Since ζ is a root of $X^n - 1$, it follows that $X^n - 1 = \Phi(X)\Psi(X)$ where by Gauss's Lemma, we may assume that $\Phi(X)$ and $\Psi(X)$ are monic with coefficients in $\mathbf{Z}$. We shall show that every primitive root ζ^i (with $\gcd(i, n) = 1$) is also a root of $\Phi(X)$. It will follow that $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \deg \Phi(X) \geq \phi(n)$. Since we already know $[\mathbf{Q}(\zeta) : \mathbf{Q}] \mid \phi(n)$ from the theorem just proved, it will follow that $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \phi(n)$ as claimed.

First note that it suffices to show that for each q prime and not dividing n, ζ^q is a root of $\Phi(X)$. For, let $i = qi'$ where q is such a prime. If we already know ζ^q is a (primitive) root, then we can apply the same reasoning to it and conclude by induction on i that $(\zeta^q)^{i'} = \zeta^i$ is such a root.

Suppose then that $\Phi(\zeta^q) \neq 0$ (where q is a prime not dividing n). It follows that ζ^q is a root of $\Psi(X)$ (since it is certainly a root of $X^n - 1$) so ζ is a root of $\Psi(X^q)$. Since $\Phi(X)$ is the minimal polynomial of ζ, we have $\Psi(X^q) = \Phi(X)H(X)$, and as above $H(X)$ is monic with coefficients in $\mathbf{Z}$. Hence,

$$\Psi(X)^q \equiv \Psi(X^q) \equiv \Phi(X)H(X) \mod q.$$

Consider the images of the polynomials $\Phi(X)$ and $\Psi(X)$ in $\mathbf{Z}/q\mathbf{Z}[X]$. Because of the above congruence, they must have a common irreducible factor in $\mathbf{Z}/q\mathbf{Z}[X]$ so the image of the product $\Phi(X)\Psi(X)$ has a repeated irreducible factor in $\mathbf{Z}/q\mathbf{Z}[X]$ so it is not separable. However, this product is $X^n - 1$ which is separable in $\mathbf{Z}/q\mathbf{Z}[X]$ since q does not divide n. It follows that $\Phi(\zeta^q) = 0$ as claimed. □

COROLLARY. *The minimal polynomial over $\mathbf{Q}$ of a primitive nth root of unity is*

$$\Phi_n(X) = \prod_{\substack{0<i<n \\ (i,n)=1}} (X - \zeta^i)$$

NOTE. $\Phi_n(X)$ is called the nth cyclotomic polynomial.

PROOF. The argument in the proof shows that $\Phi_n(X)$ divides the minimal polynomial $\Phi(X)$, but they have the same degree. □

COROLLARY. *Let ζ_n be a primitive nth root of unity. Then if $\gcd(n, m) = 1$, we have $\mathbf{Q}(\zeta_{nm}) = \mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m)$ and $\mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_m) = \mathbf{Q}$.*

PROOF.
Exercise.

Exercises.

1. Let $\gcd(n, m) = 1$.
(a) Show that $\mathbf{Q}(\zeta_{nm}) = \mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m)$. Hint: Show that the compositum contains a primitive nth root of unity.
(b) Show that $\mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}$. Hint: Use $U(\mathbf{Z}/nm\mathbf{Z}) \cong U(\mathbf{Z}/n\mathbf{Z}) \times U(\mathbf{Z}/m\mathbf{Z})$.

4. Radical Extension

Let F be a field of characteristic relatively prime to n and consider the polynomial $X^n - a$ where $a \in F$ is not zero. Note that with this assumption on n, that polynomial is separable. Let K be a splitting field of $X^n - a$ over F. We want to determine the Galois group $G(K/F)$.

Let $\alpha \in K$ be one root of $X^n - a$. If $\beta \in K$ is any other root, $\alpha^n = \beta^n = a \Rightarrow \beta/\alpha$ is an nth root of unity. Since K contains n distinct roots of $X^n - a$, it must contain n distinct nth roots of unity, so it contains a primitive nth root of unity ζ. Clearly, $K = F(\alpha, \zeta)$, and the roots of $X^n - a$ are α, $\alpha\zeta$, $\alpha\zeta^2$, ... , $\alpha\zeta^{n-1}$.

$$F(\alpha,\zeta)$$

$$F(\alpha) \qquad\qquad F(\zeta)$$

$$F$$

The relation among the subfields may be somewhat different than the diagram suggests. For example, we could have $\alpha \in F(\zeta)$. For example, take $F = \mathbf{Q}, n = 4$, and $a = -4$. Then

$$X^4 + 4 = (X^2 - 2x + 2)(X^2 + 2x + 2)$$

so we may take $\alpha = 1 + i$ which is a root of the first factor. However, in this case $\zeta = i$ is a primitive 4th root of unity. More trivially, we could have $\alpha \in F$. At the other extreme, we could have $\zeta \in F$, and this is the case we now investigate.

THEOREM. *Let F contain a primitive nth root of unity ζ. If α is a root of $X^n - a$ where $a \neq 0$ is in F, then $F(\alpha)$ is normal and separable over F, $[F(\alpha) : F] \,|\, n$, and $G(F(\alpha)/F)$ is cyclic. Conversely, if K is finite, normal, and separable over F (containing a primitive nth root of unity) and $G(K/F)$ is cyclic of order $d \,|\, n$, then $K = F(\alpha)$ where $\alpha^d \in F$.*

PROOF. Suppose α is a root of $X^n - a$ as in the statement of the theorem. Let $\sigma \in G(F(\alpha)/F)$; since $\sigma(\alpha)$ is another root of $X^n - a$, and since we know all its roots by the above analysis, it follows that $\sigma(\alpha) = \alpha\zeta^{i(\sigma)}$ where $0 \leq i(\sigma) \leq n - 1$. Define $\Gamma : G(F(\alpha)/F) \to \mathbf{Z}/n\mathbf{Z}$ by $\Gamma(\sigma) = i(\sigma) \bmod n$. It follows easily from the fact that $\zeta \in F$ that Γ is a group homomorphism, and since σ is completely determined on $F(\alpha)$ by $\sigma(\alpha)$, Γ is a monomorphism. Hence, $G(F(\alpha)/F)$ is cyclic of order dividing n.

Conversely, suppose that $G(K/F)$ is cyclic of order $d \,|\, n$. Let $\eta = \zeta^{n/d}$. η is a primitive dth root of unity. (Why?) Let σ generate $G(K/F)$ and for each $x \in K$ form

$$\langle x, \eta\rangle = x + \eta^{-1}\sigma(x) + \eta^{-2}\sigma^2(x) + \cdots + \eta^{-(d-1)}\sigma^{d-1}(x)$$

(called the Lagrange resolvent of x.) We have

$$\begin{aligned}
\sigma(\langle x, \eta\rangle) &= \sigma(x) + \eta^{-1}\sigma^2(x) + \eta^{-2}\sigma^3(x) + \cdots + \eta^{-(d-1)}\sigma^d(x) \\
&= \sigma(x) + \eta^{-1}\sigma^2(x) + \eta^{-2}\sigma^3(x) + \cdots + \eta^{-(d-1)}x \\
&= (\eta^{-1}\sigma(x) + \eta^{-2}\sigma^2(x) + \eta^{-2}\sigma^3(x) + \cdots + \eta^{-(d)}x)\eta \\
&= (x + \eta^{-1}\sigma(x) + \eta^{-2}\sigma^2(x) + \cdots + \eta^{-(d-1)}\sigma^{d-1}(x))\eta
\end{aligned}$$

i.e. $\sigma(\langle x, \eta\rangle) = \langle x, \eta\rangle\eta$. Thus if $\alpha = \langle x, \eta\rangle$ then $\sigma(\alpha) = \alpha\eta$ so $\sigma(\alpha^d) = (\alpha\eta)^d = \alpha^d$ so since σ generates $G(K/F)$, $\alpha^d \in F$. Hence, α is a root of $X^d - a$ where $a = \alpha^d$.

Suppose that $\alpha \neq 0$. Let $m(X)$ be the minimal polynomial of α over F. We have $\sigma^i(\alpha) = \alpha\eta^i$ is a root of $m(X)$ for every $i = 0,1, \ldots, d-1$, and since these are all distinct, $\deg m(X) \geq d$. However, $m(X) \,|\, X^d - a$ so $\deg m(X) = d$, and $K = F(\alpha)$ as claimed. (Note also that this shows that $X^d - a = m(X)$ is irreducible.)

To complete the proof, it suffices to show that $\alpha = \langle x, \eta\rangle \neq 0$ for at least one $x \in K$. But, this follows from Artin's Theorem on independence of characters because if

$$x + \eta^{-1}\sigma(x) + \eta^{-2}\sigma^2(x) + \cdots + \eta^{-(d-1)}\sigma^{d-1}(x) = 0$$

for all $x \in K$, the automorphisms $\mathrm{Id}, \sigma, \sigma^2, \ldots, \sigma^{d-1}$ form a dependent set of characters. □

If we start with the polynomial $X^n - a$, it might not be irreducible over F so that $|G(F(\alpha)/F)|$ could be a proper divisor of n. However, if n is prime, either $X^n - a$ splits completely in F or it is irreducible. This follows from

PROPOSITION. *Let p be prime. Let $a \in F$ and suppose $a \neq b^p$ for any $b \in F$. Then $X^p - a$ is irreducible over F.*

PROOF. First suppose that p is not the characteristic of F. Let $K = F(\alpha, \zeta)$ be a splitting field of $X^p - a$ where $\alpha^p = a$ and ζ is a primitive pth root of unity as above. In $K[X]$, we have

$$X^p - a = \prod_{i=0}^{p-1} (X - \alpha\zeta^i)$$

so the minimal polynomial $m(X)$ of α is a product of factors of the form $X - \alpha\zeta^i$. Hence, the product of its roots (except for sign, its constant term) which is in F is of the form $c = \alpha^r\zeta^k$ for some r and k. If $r < p$ (i.e. $m(X) \neq X^p - a$), then we can find s and t such that $ps + rt = 1$. Hence,

$$\alpha = \alpha^{ps}\alpha^{rt} = a^s(c/\zeta^k)^t = a^s c^t \zeta^{-kt}$$

so it follows that $\alpha\zeta^{kt} \in F$, and since $(\alpha\zeta^{kt})^p = \alpha^p = a$, this contradicts the hypothesis of the Proposition.

Suppose instead that p is the characteristic of F. Then we know that $X^p - a$ splits in its spitting field into $(X - \alpha)^p$. The minimal polynomial of α must be of the form $(X - \alpha)^i$ for some i. If $i < p$, then considering the term $-i\alpha X^{i-1}$ in $(X - \alpha)^i$, we can see that $\alpha \in F$, contrary to the hypothesis. □

In the case $n = p$ is prime and α is not in F, we can extend the analysis a bit further.

$$F(\alpha, \zeta)$$

$$F(\alpha) \qquad\qquad F(\zeta)$$

$$F$$

In the above diagram, $[F(\alpha) : F] = p$, and by our previous discussion of cyclotomic extensions, $[F(\zeta) : F] \mid \phi(p) = p - 1$. It follows that $F(\alpha) \cap F(\zeta) = F$ (since its degree must divide both p and $p - 1$.) Let H be the subgroup of the Galois group with fixed field $F(\zeta)$, and let K be the subgroup with fixed field $F(\alpha)$. The first is normal, but the second need not be normal. (See the Exercises.)) The subgroup $H \cap K$ fixes both α and ζ so it fixes $F(\alpha, \zeta)$. Hence $H \cap K = \{\mathrm{Id}\}$. On the other hand, the fixed field of HK must be contained both in $F(\alpha)$ and $F(\zeta)$ so it is F; hence $HK = G(F(\alpha, \zeta)/F)$. It follows that if ζ is not in F, the Galois group is the semidirect product of the normal subgroup H with the non-normal subgroup K. Furthermore, by natural irrationalities, H is isomorphic to $G(F(\zeta)/F)$ which we know to be cyclic of order dividing $p - 1$. In addition, by the theorem proved at the beginning of this section $G(F(\alpha, \zeta)/F(\zeta))$ is necessarily cyclic of order p.

Exercises.

1. Let p be a prime other than the characteristic of of F. Let $a \neq 0$ be an element of F which is not a pth power of an element of F. Consider a splitting field $L = F(\alpha, \zeta)$ of $X^p - a$ where $\alpha^p = a$ and ζ is a primitive pth root of unity. Show that $F(\alpha)$ is normal over F if and only if $\zeta \in F$.

2. Find the Galois groups of each of the splitting field of each of the following polynomials over the indicated base fields. You need not restrict your attention just to the results in the preceding section.
   (a) $X^4 - 2$ over $\mathbf{Q}$, $\mathbf{Q}[\sqrt{2}]$, and $\mathbf{F}_3$.
   (b) $(X^3 - 2)(X^3 - 5)$ over $\mathbf{Q}$, $\mathbf{Q}[\omega]$ (where ω is a primitive third root of unity), and $\mathbf{R}$.
   (c) $X^4 + X^2 + 1$ over $\mathbf{Q}$.

5. Solvability by Radicals

Cubic Equations.

If $f(X) = X^3 + aX^2 + bX + c$ is an irreducible cubic polynomial with coefficients in $\mathbf{Q}$, then by using a transformation of the type $X \to X - u$ with suitable u, we may assume the coefficient of X^2 is 0. (See the Exercises.) Hence, we shall suppose $f(X) = X^3 + pX + q$ is irreducible in $\mathbf{Q}[X]$. Let K be the splitting field of $f(X)$ over $\mathbf{Q}$. $G = G(K/\mathbf{Q})$ must be a isomorphic to a subgroup of S_3 which is *transitive* on the roots x_1, x_2, x_3 of $f(X)$. Identify G with that subgroup. Since the only such transitive subgroups of S_3 are S_3 itself and the alternating group A_3 (which is cyclic of order 3), it follows that these are the only possibilities for G. Let

$$\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3).$$

δ is fixed by every element of A_3, and its square $D = \delta^2$ is fixed by every element of S_3. In fact, using

$$\begin{aligned} x_1x_2 + x_1x_3 + x_2x_3 &= p \\ -x_1x_2x_3 &= q \end{aligned}$$

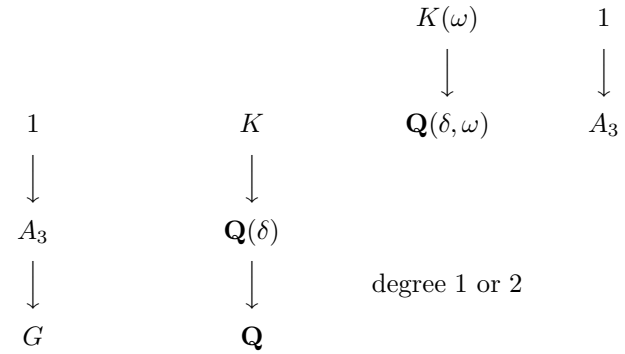
one may verify the identity

$$D = -(4p^3 + 27q^2).$$

(Simply expand both sides in terms of x_1, x_2, x_3.)

D is called the *discriminant* of the polynomial $f(X)$.

Since δ is fixed under A_3, it follows that $\mathbf{Q}(\delta)$ is the fixed field of $A_3 \cap G$. Hence, we conclude that $\delta \in \mathbf{Q} \Leftrightarrow G = A_3$. Otherwise, it is S_3. In any case $G(K/\mathbf{Q}(\delta)) = A_3$ is cyclic of order 3. Extend $\mathbf{Q}(\delta)$ by adjoining ω, a primitive cube root of unity. $[\mathbf{Q}(\delta, \omega) : \mathbf{Q}(\delta)]$ is 1 or 2 since ω satisfies a quadratic equation over $\mathbf{Q}$. Since $[K : \mathbf{Q}(\delta)] = 3$, it follows that $[K \cap \mathbf{Q}(\delta, \omega) : \mathbf{Q}(\delta)]$ divides both 2 and 3, so it equals 1. Hence, $K \cap \mathbf{Q}(\delta, \omega) = \mathbf{Q}(\delta)$, and by natural irrationalities $G(K(\omega)/\mathbf{Q}(\delta, \omega))$ is also cyclic of order 3.



It now follows from our theorem on cyclic extensions that $K(\omega)$ can be obtained from $\mathbf{Q}(\delta, \omega)$ by adjoining an element α where $\alpha^3 \in \mathbf{Q}(\delta, \omega)$. Hence, every root of $f(X)$ can be expressed as a polynomial in δ, ω, and α.

Such a description of the roots is called a solution by radicals because each constituent in the solution is either a root of unity or a cube root of something already obtained. But note that we may need to go beyond the splitting field of $f(X)$ to express it that way.

(Note also that in this case ω is actually a root of a quadratic equation, so it may be expressed in terms of the quadratic radical $\sqrt{-3}$.)

A method for solving of cubic equations by radicals was obtained by Italian mathematicians in the 16th century. It is called Cardano's method because he included it in what was probably the first relatively modern algebra textbook, although it had been discovered earlier by the mathematicians del Ferro and Tartaglia. Cardano himself never claimed credit for the method, which he attributed to Tartaglia, but he incurred the latter's wrath for making it public. Thus Cardano treated mathematics in the modern fashion, as knowledge which should be freely available with suitable credit being given to those who made the discoveries, while

Tartaglia treated it a a proprietary product to be used for his commercial benefit. (He ran a school to teach the children of merchants elementary arithmetic, and being able to solve cubics added to his prestige and presumably his profits.) We find echoes of such attitudes in modern society's use of science and technology.

Here is the method. First, let

$$\Delta = \sqrt{(p/3)^3 + (q/2)^2} = \sqrt{-D/108} = \sqrt{-3}\ \delta/18.$$

(Since there are two square roots of any rational number, choose the positive square root if Δ is real and a positive multiple of i if Δ is imaginary.) Next, choose α and α' in $\mathbf{C}$ such that

$$\alpha^3 = -(q/2) + \Delta,$$
$$(\alpha')^3 = -(q/2) - \Delta.$$

There are of course three choices for α since each of $\omega\alpha$ and $\omega^2\alpha$ would do as well, and similarly for α'. Note however that

$$(\alpha\alpha')^3 = (q/2)^2 - \Delta^2 = (-p/3)^3$$

so again given the freedom we have to vary a cube root, we may as well assume $\alpha\alpha' = -p/3$ or $\alpha' = -p/3\alpha$ Then the three roots of $X^3 + pX + q = 0$ in $\mathbf{C}$ are

$$x_1 = \alpha + \alpha'$$
$$x_2 = \omega\alpha + \omega^2\alpha'$$
$$x_3 = \omega^2\alpha + \omega\alpha'$$

One way to prove this is to show that with the given values of the roots, the coefficients of

$$(X - x_1)(X - x_2)(X - x_3)$$

are the same as the coefficients of $f(X)$. The algebra necessary to accomplish this is rather involved and might better be postponed until we have discussed elementary symmetric functions in a later section. However, a more direct derivation of these formulas is outlined in the exercises.

It is interesting to note in this connection that since D could be positive, the formulas could easily involve non-real complex radicals even if ultimately the solutions are real. (See the exercises.) This observation may have been the first convincing evidence that mathematics really required imaginary numbers for further progress.

A related more complicated method for solving quartics by radicals was discovered subsequently by Ferrara, who was a student of Cardano.

The general case.

In general, let F be a field of characteristic 0. (Some of the theory will still work in characteristic p.) We say $f(X) \in F[X]$ is *solvable by radicals* if there is a tower of fields

$$F = F_1 \subseteq F_2 = F_1(\alpha_2) \subseteq F_3 = F_2(\alpha_3) \subseteq \cdots \subseteq F_k = F_{k-1}(\alpha_k)$$

where at each stage some power $\alpha_i^{n_i} = \beta_i \in F_{i-1}, i = 2, \ldots, k$, and at the top F_k contains a splitting field for $f(X)$. In this case, as for cubics and quartics, the roots of $f(X)$ may be expressed in terms of the radicals α_i in perhaps a very involved way.

THEOREM (Galois's Solvability Criterion). *Let F be a field of characteristic 0, let $f(X) \in F[X]$, and let K be a splitting field of $f(X)$. $f(X)$ is solvable by radicals if and only if the Galois group $G(K/F)$ is a solvable group.*

PROOF. Suppose that $f(X)$ is solvable by radicals. Then there is a tower

$$F = F_1 \subseteq F_2 = F_1(\alpha_2) \subseteq F_3 = F_2(\alpha_3) \subseteq \cdots \subseteq F_k = F_{k-1}(\alpha_k)$$

where at each stage α_i is a root of a polynomial of the form $X^n - \beta$ with $\beta = \beta_i \in F_{i-1}$ and $n = n_i$ is a positive integer.

Let m be the product of the n_i in this tower and let ζ be a primitive mth root of unity (in some extension of F_k.) First, we reduce to the case $\zeta \in F$. To do this note first that $KF(\zeta)$ is a normal extension of F. (It is not hard to see that in general the compositum of two normal extensions is normal. Use the fact that a finite extension is normal if it is fixed under automorphisms of some extension normal over the base field.) Since $F(\zeta)$ is a normal extension of F, it follows that $K \cap F(\zeta) \supseteq F$ is normal, and $G(K \cap F(\zeta)/F)$ is an epimorphic image of $G(F(\zeta)/F)$ so it is abelian. On the other hand, by natural irrationalities, $G(KF(\zeta)/F(\zeta)) \cong G(K/K \cap F(\zeta))$, so since $G(K \cap F(\zeta)/F) \cong G(K/F)/G(K/K \cap F(\zeta))$ is solvable, it suffices to show that $G(KF(\zeta)/F(\zeta))$ is solvable. By forming the composita $F_iF(\zeta)$, we may form a tower of radical extensions starting with $F(\zeta)$ with the last stage containing $KF(\zeta)$ so the extension $KF(\zeta) \supseteq F(\zeta)$ inherits the relevant hypothesis.

Suppose then that $\zeta \in F$. We shall proceed by induction on the number of terms k in the tower. Since $\zeta \in F$, $F_2 \supseteq F_1 = F$ is a normal extension with cyclic Galois group of order dividing m. Consider the compositum KF_2. By essentially the same argument as in the previous paragraph, it suffices to show that $G(KF_2/F_2)$ is solvable. However, $F_2 \subseteq F_3 \subseteq \cdots \subseteq F_k$ is a tower over F_2 with $k-1$ terms, and the last stage contains KF_2. Co by induction, $G(KF_2/F_2)$ is indeed solvable. This completes the first part of the proof.

Suppose conversely that $G(K/F)$ is solvable. Let $m = |G(K/F)|$ and let ζ be a primitive mth root of unity in some extension of K. The extension $F(\zeta) \supseteq F$ is a radical extension in the trivial sense that $\zeta^m = 1 \in F$. Also, by natural rationalities $G(KF(\zeta)/F(\zeta))$ is isomorphic to a subgroup of $G(K/F)$ so it is also solvable. Let $G(KF(\zeta)/F(\zeta)) = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\}$ be a tower of subgroups each normal in the preceding and with cyclic factors. Let $F(\zeta) = K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r = KF(\zeta)$ be the corresponding tower of subfields. Each is normal over the preceding since the corresponding subgroups are. Since at each stage, the Galois group, G_i/G_{i-1}, is cyclic and the base field contains the relevant roots of unity, each stage is a radical extension as required. □

Remark. There is one additional twist which may be added to the above description of solvability by radicals. Some people, may not consider it valid to call a root of unity a radical. For example, in $\mathbf{C}$, if $\alpha^n = a$ and ζ is a primitive nth root of unity, the roots of $X^n - a$ are $\alpha, \alpha\zeta, \ldots, \alpha\zeta^{n-1}$. If $a \neq 1$, we may reasonably consider $\alpha = \sqrt[n]{a}$ to be a true algebraic radical. But we have no way to express ζ except by using numbers of the form $e^{i\theta}$ which involve trigonometric functions. We noted in the case $n = 3$ that ω could in fact be expressed in terms of a 'true radical' $\sqrt{-3}$, and the same is true in general. Namely, the cyclotomic extension $F(\zeta)$ has abelian (hence solvable) Galois group of order dividing $\phi(n) < n$. Hence, we can apply the analysis in the above proof by considering 'true radicals' and roots of unity of order less than n. The details require some thought, but ultimately we can express the roots of the original polynomial in terms of elements α_i with each $\alpha_i^{n_i} \in F_{i-1}$, the next lower field in the tower, and $\alpha_i^{n_i} \neq 1$. The roots of unity do leave some trace however, since at each stage, we have multiple choices for these 'true radicals' and we must make one specific choice in some manner.

THEOREM (Galois). *There exist polynomials in* $\mathbf{Q}[X]$ *of degree 5 which are not solvable by radicals.*

PROOF. Take $f(X) = X^5 - 4X + 2$. We shall show that the Galois group of the splitting field of $f(X)$ over $\mathbf{Q}$ is S_5 which we know is not solvable.

First note that $f(X)$ is irreducible. This follows from the following important result.

LEMMA (Eisenstein Irreducibility Criterion). *Let p be a prime and let*

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbf{Z}[X]$$

where $a_n \not\equiv 0 \bmod p$, $a_i \equiv 0 \bmod p$ for $0 < i < p$, $a_0 \equiv 0 \bmod p$, but $a_0 \not\equiv 0 \bmod p^2$. Then $f(X)$ is irreducible.

PROOF OF THE LEMMA. Assume $f(X) = g(X)h(X)$ is a proper factorization in $\mathbf{Q}[X]$. By Gauss's Lemma, we may suppose that $g(X)$, $h(X) \in \mathbf{Z}[X]$. Project this factorization onto $\mathbf{Z}/p\mathbf{Z}[X]$. In that ring, we have

$$\overline{f}(X) = \overline{g}(X)\overline{h}(X)$$

where by hypothesis $\overline{f}(X) = \overline{a}_n X^n$ and $\overline{a}_n \neq 0$ in $\mathbf{Z}/p\mathbf{Z}$. By unique factorization, it follows that $\overline{g}(X) = \overline{c}X^r$ and $\overline{h}(X) = \overline{d}X^s$ where $r+s = n$. It follows that the constant terms of both $g(X)$ and $h(X)$ must be divisible by p. From this it follows that the constant term of $f(X)$ must be divisible by p^2 which is false.

NOTE. The Eisenstein Criterion works in $A[X]$ for A any UFD since Gauss's Lemma applies, and if p is an irreducible element of A then A/pA is a field.

We continue with the calculation of the Galois group of $f(X) = X^5 - 4X + 2$. Let K be the splitting field of $f(X)$ and let α be a root in K. Since $f(X)$ is irreducible, $[\mathbf{Q}[\alpha] : \mathbf{Q}] = 5$.

$$K$$

$$\mathbf{Q}[\alpha]$$
$$5$$

$$\mathbf{Q}$$

It follows that $|G(K/\mathbf{Q})|$ is divisible by 5. On the other hand, $G(K/\mathbf{Q})$ is isomorphic to some subgroup of S_5 which is of order $5! = 5 \times 4!$ so the 5-Sylow subgroup of $G = G(K/\mathbf{Q})$ must have order exactly 5 and may be identified with a 5-Sylow subgroup of S_5. Thus, G contains a 5-cycle which by appropriate renumbering of the roots we can identify with $(1 \quad 2 \quad 3 \quad 4 \quad 5)$. On the other hand, $f(X)$ has exactly 3 real roots. (For, $f'(X) = 5X^4 - 4$, and $f''X) = 20X^3$ so $f(X)$ has a local maximum at $x = -\sqrt[4]{4/5}$ and a local minimum at $x = \sqrt[4]{4/5}$. It is positive at the local maximum, negative at the local minimum, negative for x very negative, and positive for x very positive. Hence, it crosses the real x-axis exactly 3 times. There are other more algebraic ways to come to the same conclusion.) The other two roots must be complex conjugates. If we restrict complex conjugation to K, it must interchange the two complex roots and it fixes the 3 real roots, hence it induces a 2-cycle $(i \quad j)$. Thus, G is a subgroup of S_5 which contains a 5-cycle $\sigma = (1 \quad 2 \quad 3 \quad 4 \quad 5)$ and a 2-cycle $\tau = (i \quad j)$. It follows that $G = S_5$. For, conjugating τ by the powers of σ yields the 2-cycles $(i+1 \quad j+1)$, $(i+2 \quad j+2)$, $(i+3 \quad j+3)$, and $(i+4 \quad j+4)$ (where the indices should be read mod 5). Hence, G contains a 2-cycle of the form $(1 \quad k) = (k \quad 1)$. By shifting mod 5 as above, we see that if G contains $(4 \quad 1)$, it contains $(1 \quad 3)$ and if it contains $(5 \quad 1)$, it contains $(1 \quad 2)$. If $(1 \quad 2) \in G$ (and so also $(1 \quad 5)$), then $(2 \quad 3) \in G$ and by conjugation $(1 \quad 3) \in G$ (and so also $(1 \quad 4)$). Hence $(1 \quad k) \in G$ for every k, and by shifting, G contains every transposition so it is S_5. A similar argument works if $(1 \quad 3) \in G$. $\square$

Note that the above argument works as long as the polynomial is irreducible of degree 5 and has exactly 3 real roots. In fact, it will work if the polynomial is irreducible of prime degree p and has exactly $p-2$ real roots.

Exercises.

1. Show by making an appropriate change of variables $Y = X - u$, that we may replace a general cubic polynomial by one in which the coefficient of Y^2 is zero.
2. Let $f(X) = X^3 + pX + q$ be an irreducible cubic with rational coefficients.
   (a) Substitute $X = Y + Z$, and show that

$$f(Y+Z) = Y^3 + Z^3 + (3YZ + p)(Y + Z) + q$$

   (b) Assume Y, Z are restricted to satisfy the relation $3YZ + p = 0$. Solve for Y in terms of Z, and substitute in the above expression to obtain

$$g(Z) = Z^6 + qZ^3 - (p/3)^3.$$

(c) Use the quadratic formula to find the roots γ, γ' of the equation

$$T^2 + qT - (p/3)^3 = 0.$$

Let α be a cube root of γ and α' a cube root of γ' such that $\alpha\alpha' = -p/3$. Tracing the steps backwards, note that setting $Y = \alpha, Z = \alpha'$ and $X = \alpha + \alpha'$ yields a root of the original equation.

(d) Note that subject to the requirement $\alpha\alpha' = -p/3$ (which is consistent with the restraint $YZ+p/3 = 0$), the only other possible choices are replacing α by $\omega\alpha$ and α' by $\omega^2\alpha'$ or replacing α by $\omega^2\alpha$ and α' by $\omega\alpha'$. Conclude that the three roots of the irreducible cubic are given by the expressions in the text.

3. (a) Show that the roots of a real cubic are real if it has three real roots and imaginary otherwise. Hint: A real cubic either has three real roots or one real root and two conjugate complex roots. Use the formula for D in terms of the roots x_1, x_2, x_3.

(b) Let $f(X) = X^3 - 3X + 1$. Apply Cardano's method to find its complex roots.

(c) Show the roots of this polynomial are real by calculating its discriminant in terms of its coefficients. Note that in the formulas you got in part (b), complex numbers enter in an essential way. In other words, Cardano's method uses of non-real complex numbers to describe the roots although all three are real.

(d) What is the Galois group of the splitting field of this polynomial over $\mathbf{Q}$?

4. (a) Let $K = F(\alpha)$ where $\alpha^n \in F$ for some $n > 1$. Show that there is a tower of subfields F_i, $i = 0, 1, \ldots, k$, between F and K with $F_0 = F$ and $F_k = K$ and such that

$$F_i = F_{i-1}(\beta_i) \text{ where } \beta_i^{p_i} \in F_{i-1} \text{ and } p_i \text{ is } \textit{prime}.$$

(b) Let $f(X) = X^3 + pX + q \in \mathbf{Q}[X]$ be irreducible. Let F be an extension of $\mathbf{Q}$ contained in $\mathbf{C}$, and let $N = F(x_1)$ where x_1 is one of the roots of $f(X)$. Show that if $\sqrt{D} \in F$ (where D is the discriminant of $f(X)$) then N is normal over F. (c) Show that if $f(X) = X^3 + p^X + q \in \mathbf{Q}[X]$ has 3 real roots then $\sqrt{D} \in \mathbf{R}$.

(d) Assume $f(X)$ as above is irreducible and has 3 real distinct roots. Show that there is no tower of *real* fields starting with $\mathbf{Q}$ and ending with a field in which $f(X)$ splits completely and such that each stage is a radical extension. In short, an irreducible real cubic with 3 real roots cannot be solved by real radicals. **Hint:** By part (a), you can assume the stages are all of prime degree. By forming the composita with $\mathbf{Q}[\sqrt{D}]$, you may assume the tower starts with that field. Somewhere along the way one of the fields would be a normal extension of degree 3 over the previous stage. (Why?) It would also be obtained by adjoining a cube root of some element since it would be a radical extension of degree 3. By normality, it would have to contain a primitive cube root of unity. (Why?)

6. Symmetric polynomials

Before Galois showed that it is not generally true that every equation of degree 5 or higher is solvable by radicals, Abel derived a related result. He showed that, in a certain sense we shall make clear below, there are no "radical formulas" for the roots of a polynomial $f(X)$ of degree n derived from its coefficients.

Let k be a field and let $K = k(X_1, \ldots, X_n)$ be the field of rational functions in the indeterminates $X_1, \ldots, X_n$ i.e. the field of fractions of $k[X_1, \ldots, X_n]$. The symmetric group S_n may be viewed as a finite group of automorphisms of K since each permutation of the indeterminates induces an automorphism of $k[X_1, \ldots, X_n]$ and hence also of K. Let F be the fixed field of S_5. Then by our previous theory, $K = F(X_1, \ldots, X_n)$ is the splitting field of

$$\begin{aligned} f(X) &= \prod (X - X_i) \\ &= X^n - \phi_1 X^{n-1} + \phi_2 X^{n-2} + \cdots + (-1)^n \phi_n \in F[X] \end{aligned}$$

where

$$\begin{aligned}\phi_1 &= \sum_i X_i \\ \phi_2 &= \sum_{i<j} X_i X_j \\ &\vdots \\ \phi_n &= X_1 X_2 \dots X_n.\end{aligned}$$

(The polynomials are called the elementary symmetric functions of the indeterminates. Any polynomial left fixed by S_n is called symmetric.) By Galois Theory, $K \supseteq F$ is a finite, normal separable extension with Galois group S_n which of course is not solvable for $n > 4$. Hence, the above polynomial in $F[X]$ is not solvable by radicals. This would not be very interesting were it not for the following additional facts. First, K is also a splitting field for the separable polynomial $f(X)$ over the field $F' = k(\phi_1, \dots, \phi_n)$, and since $[K : F'] \leq n! = [K : F]$, it follows that $F = k(\phi_1, \dots, \phi_n)$. Moreover, we shall show below that if we choose indeterminates $T_1, \dots, T_n$ then $T_i \to X_i$ defines an *isomorphism* $k[T_1, \dots, T_n] \to k[\phi_1, \dots, \phi_n]$ and the field of fractions of the latter is the field F. Thus, we may identify F with the rational function field $k(T_1, \dots, T_n)$. If we think of $T_1, \dots, T_n$ as the coefficients of a general polynomial of degree n, then Abel's Theorem asserts that this general equation is not solvable by radicals in the sense discussed previously. That means there are no general radical formulas for the roots as functions of *indeterminate* coefficients.

To complete the discussion we now prove the following important result.

THEOREM. *Let A be any commutative ring and let $X_1, \dots, X_n$ be indeterminates. Every symmetric polynomial in $A[X_1, \dots, X_n]$ is uniquely expressible as a polynomial in the elementary symmetric polynomials.*

PROOF. We shall use the abbreviated notation $X = (X_1, \dots, X_n)$ and $X' = (X_1, \dots, X_{n-1})$.

We proceed by a double induction on n the number of indeterminates and d the degree of the polynomial $f(X)$. For $n = 1$ there is nothing to prove so suppose $n > 1$. Assume $f(X)$ is symmetric of degree $d > 0$.

If $X_n | f(X)$ then by symmetry, $X_i | f(X)$ for every i, and in this case it is easy to see that $X_1 \dots X_n = \phi_n$ divides $f(X)$, i.e.

$$f(X) = f'(X)\phi_n.$$

Since $f(X)$ and ϕ_n are fixed by S_n it follows that $f'(X)$ is also symmetric. (For this, you only need to be able to cancel factors like X_i; A need not be a domain.) Now apply induction on d to conclude that $f'(X)$ and hence $f(X)$ are expressible as polynomials in $\phi_1, \dots, \phi_n$. If on the other hand X_n does not divide $f(X)$, then we may write $f(X) = g(X') + h(X)$ where $g(X')$ is a polynomial in the first $n-1$ indeterminates and X_n divides $h(X)$. Since $f(X)$ is fixed by S_{n-1}, it is easy to see that $g(X')$ (and also $h(X)$) is fixed by S_{n-1}. By induction, we may suppose that $g(X') = k(\phi'_1, \dots, \phi'_{n-1})$ where $\phi'_1, \dots, \phi'_{n-1}$ are the elementary symmetric functions in the first $n-1$ indeterminates. Consider $f_1(X) = f(X) - k(\phi_1, \dots, \phi_{n-1})$. (Note that the primes have been dropped from the ϕ's.) Put $X_n = 0$ in that equation and note that $h(X_1, \dots, X_{n-1}, 0) = 0$ since $X_n | h(X)$ and that $\phi_i(X_1, \dots, X_{n-1}, 0) = \phi'_i$ for $i = 1, 2, \dots, n-1$. We get that $f_1(X_1, \dots, X_{n-1}, 0) = 0$ so that $X_n | f_1(X)$. We can now apply the first part of the argument to conclude that $f_1(X)$ is expressible as a polynomial in $\phi_1, \dots, \phi_n$. Hence, the same is true of $f(X) = f_1(X) + k(\phi)$.

We now show that the representation of a symmetric polynomial as a polynomial in the ϕ_i is unique. To this end, map the polynomial ring $A[T_1, \dots, T_n]$ in indeterminates $T_1, \dots, T_n$ to $A[X_1, \dots, X_n]$ by $T_i \to \phi_i$. Suppose $f(T) \in A[T]$ satisfies $f(\phi) = 0$. If $T_n | f(T)$ then $f(T) = f'(T)T_n$ and $f'(\phi)\phi_n = 0$. Hence, $f'(\phi) = 0$ and by induction we may conclude that $f'(T)$—and hence $f(T)$—is the zero polynomial. Otherwise, $f(T) = g(T_1, \dots, T_{n-1}) + h(T)$ where $T_n | h(T)$. If we put $X_n = 0$ in the relation $f(\phi_1, \dots, \phi_n) = 0$ and use the fact that $\phi_n(X_1, \dots, X_{n-1}, 0) = 0$, $f(\phi) = g(\phi_1, \dots, \phi_{n-1}) + h(\phi_1, \dots, \phi_{n-1}, \phi_n) = 0$ tells us that $g(\phi'_1, \dots, \phi'_{n-1}) = 0$. (Note the primes on the ϕ's.) By induction, we may conclude that $g(T_1, \dots, T_{n-1}) = 0$. Hence, $h(\phi) = 0$ with $T_n | h(T)$. Applying the first part of the argument, we conclude that $h(T) = 0$. □

Exercises.

1. For $n = 2$, express the symmetric polynomial $(X_1 - X_2)^2$ in terms of the elementary symmetric polynomials.

2. (a) For $n = 3$, express the symmetric polynomial $[(X_1 - X_2)(X_1 - X_3)(X_2 - X_3)]^2$ in terms of the elementary symmetric polynomials.

(b) Assuming the relation $X_1 + X_2 + X_3 = 0$ for the first elementary symmetric function, show that the expression in part (a) gives the discriminant previously calculated for a cubic of the form $X^3 + pX + q$.

3. The power sum $P_k = X_1^k + X_2^k + \cdots + X_n^k$ is certainly a symmetric polynomial. There are formulas due to Newton for inductively expressing each power sum in terms of elementary symmetric functions and power sums of lower degree. These may be used either to express the power sums as polynomials in the elementary symmetric polynomials with integral coefficients of the elementary symmetric polynomials in terms of the power sums with rational coefficients. Look these formulas up in an appropriate source, and use them to for $n = 4$ to express $P_k, k = 1, 2, 3, 4, 5$ in terms of the elementary symmetric functions. (You might also study the proof that the formulas are valid while you are at it.)

7. Division rings

There is a famous theorem of Wedderburn which asserts that there are no finite non-commutative divisions rings.

THEOREM. *Every finite division ring is a field.*

PROOF. Let $x \in D$ and consider the *centralizer* of x in D

$$C_D(x) = \{y \in D | xy = yx\}.$$

It is not hard to see that $C_D(x)$ is a subring of D, and it is even a sub-division ring since if $y \neq 0$ commutes with x, then multiplying on left and right by y^{-1} shows that y^{-1} also commutes with x. Clearly, $C_D(x)$ contains the *center* $Z(D)$ of D (i.e. the set of all elements which commute with every element of D.) $Z(D)$ is also a sub-division ring and because it is commutative, it is a field.

Let $|Z(D)| = q$. Then, because everything in sight is a vector space over $Z(D)$, we have $|C_D(x)| = q^{d(x)}$ and $|D| = q^n$. Again, because D is a free module over $C_D(x)$, it follows that q^n is a power of $q^{d(x)}$ so $d(x)|n$.

Let $G = D^*$ be the multiplicative group of non-zero elements of D. $|G| = q^n - 1$. The center $Z(G)$ is clearly just $Z(D)^*$ so $|Z(G)| = q - 1$. Finally, the centralizer $C_G(x)$ (in G of x) is clearly $C_D(x)^*$ so $|C_G(x)| = q^{d(x)} - 1$. Now consider the class equation for G

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} (G : C_G(x))$$

which comes down to

$$q^n - 1 = q - 1 + \sum (q^n - 1)/(q^{d(x)} - 1).$$

Consider the nth cyclotomic polynomial $\Phi_n(X)$—the minimal polynomial over $\mathbf{Q}$ of a primitive nth root of unity ζ_n. We know that $\Phi_n(X)|X^n - 1$ but of course $\Phi_n(X)$ does not divide $X^d - 1$ for any $d < n$. If $d|n$, then

$$X^n - 1 = H(X)(X^d - 1)$$

(where $H(X)$ is just a sum of ascending powers of X^d.) It follows that $\Phi_n(X)|H(X)$. By Gauss's Lemma and associated arguments, we know that $\Phi_n(X)$ has integral coefficients and in fact the above divisibility relations take place in $\mathbf{Z}[X]$. It follows that we may put $X = q$ in the above relation to obtain $\Phi_n(q)|H(q) = (q^n - 1)/(q^d - 1)$ for each $d|n$. It follows that $\Phi_n(q)|q - 1$.

To complete the proof, we show that $|q - 1| < |\Phi_n(q)|$ if $n > 1$. This follows by noting that

$$\Phi_n(q) = \prod (q - \zeta^i)$$

where the product is taken over all primitive nth roots of unity. However, it is easy to see that for any $z \neq 1$ on the unit circle in the complex plane we have $|q - 1| < |q - z|$. (Draw the picture!) $\square$