Galois Theory

Spring 2018

Paul Balister
University of Memphis

7262 1. Field Extensions Spring 2018

A field **extension** K/F is an (injective) ring homomorphism between two fields $i\colon F \to K$ so, by the isomorphism theorem, identifies F with the subfield $i(F)$ of K. When the map i is clear, we often abuse notation by regarding F as a subset of K. For example, $\mathbb{C}/\mathbb{R}$ is a field extension and we commonly write $\mathbb{R} \subset \mathbb{C}$.

If K/F is an extension then we can regard $K = (K, +)$ as a vector space over F since $(K, +)$ is an abelian group and the map $F \times K \to K$; $(x, y) \mapsto xy = i(x)y$ satisfies the properties of multiplication by a scalar. The dimension of this vector space is called the **degree** of K over F, $[K:F] = \dim_F K$. An extension K/F is called **finite** if $[K:F] < \infty$.

Examples: $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}(X)/\mathbb{Q}$, $\mathbb{C}(X)/\mathbb{Q}$ are all field extensions. $[\mathbb{C}:\mathbb{R}] = 2$, $[\mathbb{R}:\mathbb{Q}] = \infty$ since $\{1, \pi, \pi^2, \dots\}$ is linearly independent over $\mathbb{Q}$, $[\mathbb{Q}(X):\mathbb{Q}] = [\mathbb{C}(X):\mathbb{Q}] = \infty$ since $\{1, X, X^2, \dots\}$ is linearly independent over $\mathbb{Q}$.

Theorem (The Tower Law) *If L/K and K/F are field extensions then L/F is a field extension and $[L:F] = [L:K][K:F]$ (finite or infinite).*

Proof. We can compose the inclusions $F \to K$ and $K \to L$ to get an inclusion $F \to L$. Hence L/F is an extension. Let $\{a_i : i \in I\}$ be a basis for K/F and $\{b_j : j \in J\}$ be a basis for L/K. The result will follow if we can show that $\{a_i b_j : i \in I, j \in J\}$ is a basis for L/F.
Independence: If $\sum_{i,j} \lambda_{ij} a_i b_j = 0$ with $\lambda_{ij} \in F$ then $\mu_j = \sum_i \lambda_{ij} a_i \in K$ and $\sum_j \mu_j b_j = 0$. By K-linear independence of the b_j we have $\mu_j = 0$, and then by F-linear independence of the a_i we have $\lambda_{ij} = 0$.
Spanning: If $\alpha \in L$ we can write $\alpha = \sum_j \mu_j b_j$ for some $\mu_j \in K$. But then we can write $\mu_j = \sum_i \lambda_{ij} a_i$ with $\lambda_{ij} \in F$, so $\alpha = \sum_{ij} \lambda_{ij} a_i b_j$. □

Corollary *L/F is finite iff both L/K and K/F are finite.*

If R is a subring of R' and $S \subseteq R'$ then we denote by $R[S]$ the smallest subring of R' containing R and S. More explicitly, $R[S] = \{f(s_1, \dots, s_n) : f \in R[X_1, \dots, X_n], s_i \in S, n \in \mathbb{N}\}$.

If K/F is an extension and $S \subseteq K$, denote by $F(S)$ the smallest subfield of K containing both F and S. Note that $F(S) = \operatorname{Frac} F[S] = \{f(s_1, \dots, s_n)/g(s_1, \dots, s_n) : f, g \in F[X_1, \dots, X_n], g(s_1, \dots, s_n) \neq 0\}$. We write $F(a)$ for $F(\{a\})$ etc..

The extension K/F is called **simple** if $K = F(a)$ for some $a \in K$. In this case a is called a **primitive element** of K/F.
The extension K/F is called **finitely generated** if $K = F(S)$ for some finite set $S \subseteq K$.

Examples: $\mathbb{C}/\mathbb{R}$ is simple since $\mathbb{C} = \mathbb{R}(i)$. $\mathbb{R}/\mathbb{Q}$ is not simple or even finitely generated since $\mathbb{Q}(a_1, \dots, a_n)$ is always a countable set but $\mathbb{R}$ is uncountable.

Warning: Whenever you write $R[a, b, \dots]$ or $F(a, b, \dots)$ it is important that you work inside some *fixed, specified* ring R' or field F'. For example, do not write $(\mathbb{Z}/p\mathbb{Z})[\sqrt[4]{2}]$.

7262 2. Algebraic and Transcendental Spring 2018

Let K/F be a field extension. Then $\alpha \in K$ is **algebraic over** F if there exists a non-zero polynomial $f \in F[X]$ with $f(\alpha) = 0$. Otherwise α is **transcendental over** F. We call K **algebraic over** F if *every* $\alpha \in K$ is algebraic over F. Otherwise K is **transcendental over** F.

Examples: The real number $\sqrt{2}$ is algebraic over $\mathbb{Q}$ (take $f = X^2 - 2$) and π is transcendental over $\mathbb{Q}$. However π is algebraic over $\mathbb{R}$ (take $f = X - \pi \in \mathbb{R}[X]$). Since $\mathbb{R}$ contains at least one element that is transcendental over $\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$ must be transcendental. The extension $\mathbb{C}/\mathbb{R}$ is algebraic since for any $z \in \mathbb{C}$ we can take $f = X^2 - (z + \bar{z})X + z\bar{z} \in \mathbb{R}[X]$.

Theorem 2.1 *Let K/F be a field extension and let $\alpha \in K$.*
(a) If α is algebraic over F then

- A1 $\exists$ *unique monic irreducible* $m_{\alpha,F} \in F[X]\colon\ \forall f \in F[X]\colon f(\alpha) = 0$ *iff* $m_{\alpha,F} \mid f$,
- A2 $F[\alpha] = F(\alpha)$ *and both are isomorphic to* $F[X]/(m_{\alpha,F})$,
- A3 $[F(\alpha)\colon F] = \deg m_{\alpha,F} = n < \infty$ *and the set* $\{1, \alpha, \dots, \alpha^{n-1}\}$ *is a basis for* $F(\alpha)/F$,

(b) If α is transcendental over F then

- T1 $\forall f \in F[X]\colon\ f(\alpha) = 0$ *iff* $f = 0$,
- T2 $F[\alpha] \neq F(\alpha)$, $F[\alpha] \cong F[X]$, *and* $F(\alpha) \cong F(X) = \operatorname{Frac} F[X]$.
- T3 $[F(\alpha)\colon F] = \infty$.

The polynomial $m_{\alpha,F}$ in (a) is called the **minimal polynomial of** α **over** F.

Proof. The map $\mathrm{ev}_\alpha\colon F[X] \to K; f \mapsto f(\alpha)$ is a ring homomorphism and $f \in \operatorname{Ker} \mathrm{ev}_\alpha$ iff $f(\alpha) = 0$. Since $F[X]$ is a PID, $\operatorname{Ker} \mathrm{ev}_\alpha = (m_{\alpha,F})$ for some $m_{\alpha,F}$. But $\operatorname{Im} \mathrm{ev}_\alpha = F[\alpha]$, so $F[\alpha] \cong F[X]/(m_{\alpha,F})$. Now $F[\alpha]$ is an ID ($\subseteq$ Field), so $(m_{\alpha,F})$ is a prime ideal. If α is algebraic, then $\exists f \in (m_{\alpha,F})$, $f \neq 0$, so $m_{\alpha,F} \neq 0$ is prime and so irreducible. Generators of ideals are unique up to multiplication by units and $(F[X])^\times = F^\times$, so by multiplying $m_{\alpha,F}$ by a constant we may assume it is monic and it is then unique. Since $F[X]$ is a PID, $(m_{\alpha,F})$ is maximal, so $F[\alpha]$ is a field, and thus $F[\alpha] = F(\alpha)$. By the division algorithm any $f = qm_{\alpha,F} + r$ with $\deg r < n$. Thus $f(\alpha) = r(\alpha)$ is a linear combination of $\{1, \alpha, \dots, \alpha^{n-1}\}$. These are linearly independent, since otherwise some $r(\alpha) = 0$, $r \neq 0$, so $m_{\alpha,F} \mid r$ contradicting $\deg r < n$.
If α is transcendental then $\operatorname{Ker} \mathrm{ev}_\alpha = (0)$, so $F[\alpha] \cong F[X]$. Then $F(\alpha) = \operatorname{Frac} F[\alpha] \cong F(X)$. If $1/\alpha = f(\alpha)$ then α would be a root of $Xf(X) - 1$. Thus $1/\alpha \notin F[\alpha]$ and so $F[\alpha] \neq F(\alpha)$. Now $\{1, \alpha, \alpha^2, \dots\}$ is linearly independent (otherwise some $f(\alpha) = 0$) so $[F(\alpha) : F] = \infty$. □

Examples: $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$, $m_{i,\mathbb{R}} = X^2 + 1$, $[\mathbb{C}\colon\mathbb{R}] = \deg m_{i,\mathbb{R}} = 2$, and $\{1, i\}$ is a basis for $\mathbb{C}/\mathbb{R}$. Note that $m_{i,\mathbb{C}} = X - i \neq m_{i,\mathbb{R}}$, so it is important to specify the ground field F.

Theorem 2.2 *If K/F is finite then it is algebraic. (Converse not true in general.)*

Proof. If $\alpha \in K$, $\infty > [K:F] = [K:F(\alpha)][F(\alpha):F] \geq [F(\alpha):F]$, so α is algebraic. □

Theorem 2.3 *If A is the set of all elements of K algebraic over F then A is a subfield of K containing F.*

Proof. Elements of F are algebraic over F, so $F \subseteq A \subseteq K$. If $\alpha, \beta \in A$ then β is algebraic over $F(\alpha)$ (since β is algebraic over F). Hence $[F(\alpha,\beta):F] = [F(\alpha,\beta):F(\alpha)][F(\alpha):F] = (\deg m_{\beta,F(\alpha)})(\deg m_{\alpha,F}) < \infty$. Therefore $F(\alpha,\beta)/F$ is algebraic, so $\alpha \pm \beta, \alpha/\beta, \alpha\beta \in F(\alpha,\beta)$ are algebraic over F. Hence $\alpha \pm \beta, \alpha/\beta, \alpha\beta \in A$ and A is a subfield of K. □

Theorem 2.4 *If $L/K/F$ then L/F is algebraic iff both L/K and K/F are.*

Proof. $\Rightarrow$ is clear. Now assume both L/K and K/F are algebraic and $\alpha \in L$. Then $f(\alpha) = 0$ where $f = \sum_{i=0}^{n} b_i X^i \in K[X]$, $f \neq 0$. Define $F_i = F(b_0, \dots, b_{i-1})$. Then α is algebraic over F_{n+1} (since $f \in F_{n+1}[X]$ and $f(\alpha) = 0$), b_i is algebraic over F_i (since $b_i \in K$ is algebraic over F), and $F_{i+1} = F_i(b_i)$. Hence $[F_{n+1}(\alpha):F] = [F_{n+1}(\alpha):F_{n+1}][F_{n+1}:F_n]\dots[F_1:F_0] < \infty$. Therefore $\alpha \in F_{n+1}(\alpha)$ is algebraic over $F = F_0$. □

Constructive proof of Theorems 2.3 and 2.4.

Theorem (Symmetric Function Theorem) *If $f \in R[X_1, \dots, X_n]$ is symmetric under interchange of any pair X_i, X_j, then $f \in R[\sigma_1, \dots, \sigma_n]$ where σ_i is the ith elementary symmetric function of the X_i, $\sigma_i = \sum_{|S|=i} \prod_{j \in S} X_j$.*

Suppose there exists M/K such that $m_\alpha = m_{\alpha,F}$ and $m_\beta = m_{\beta,F}$ **split** in M, i.e., factor completely into linear factors $m_\alpha = (X - \alpha_1)\dots(X - \alpha_n)$, $m_\beta = (X - \beta_1)\dots(X - \beta_m)$, $\alpha = \alpha_1$, $\beta = \beta_1$, $\alpha_i, \beta_j \in M$. (We shall prove the existence of such an M later, the α_i are called the **conjugates** of α). Consider the polynomial

$$f(X) = \prod_{i=1}^{n} \prod_{j=1}^{m} (X - \alpha_i\beta_j) \in F[\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m, X] \subseteq M[X].$$

We can consider f as a polynomial in indeterminates α_i and coefficients in the ring $R = F[\beta_1, \dots, \beta_m, X]$. By the Symmetric Function Theorem, $f \in R[\sigma_1, \dots, \sigma_m]$, where σ_i are the elementary symmetric functions in the α_i. But then σ_i are just $\pm$ the coefficients of m_α, so lie in F. Thus $f \in F[\beta_1, \dots, \beta_m, X]$. A similar argument using symmetry in the β_j shows that $f \in F[X]$. But f is monic (so non-zero) and $f(\alpha\beta) = f(\alpha_1\beta_1) = 0$. Hence $\alpha\beta$ is algebraic over F. Note that f might not be irreducible so we can only conclude that $m_{\alpha\beta,F}$ is a *factor* of f. A similar argument can be used for $\alpha \pm \beta$. For $1/\alpha$ the proof is easier since we can take the polynomial $f(X) = X^n m_\alpha(1/X)$. Hence Theorem 2.3 can be made constructive.

For Theorem 2.4 a similar trick can be used. Let α be algebraic over K with minimal polynomial, $m_{\alpha,K} = \sum_{i=0}^{m} \beta_i X^i$, where each β_i is algebraic over F. Suppose we can find a M/L such that each minimal polynomial $m_{\beta_i,F}$ splits, $m_{\beta_i,F} = \prod_{j=1}^{n_i}(X - \beta_{i,j})$, $\beta_i = \beta_{i,1}$, $\beta_{i,j} \in M$. Now consider

$$f(X) = \prod_{j_1=1}^{n_1} \cdots \prod_{j_m=1}^{n_m} \sum_{i=0}^{m} \beta_{i,j_i} X^i \in F[\beta_{1,1}, \dots, \beta_{1,n_1}, \beta_{2,1} \dots, \dots \beta_{m,n_m}, X].$$

This polynomial is symmetric in each collection $\{\beta_{i,1}, \dots, \beta_{i,n_i}\}$, so by applying the Symmetric Function Theorem m times we get $f \in F[X]$. But $m_{\alpha,K} \mid f$, so $f(\alpha) = 0$.

7262 3. Straight Edge and Compass Spring 2018

If P and Q are two distinct points in the plane, write $L(P,Q)$ for the (infinite) line through P and Q and $C(P,Q)$ for the circle with center P going through the point Q.

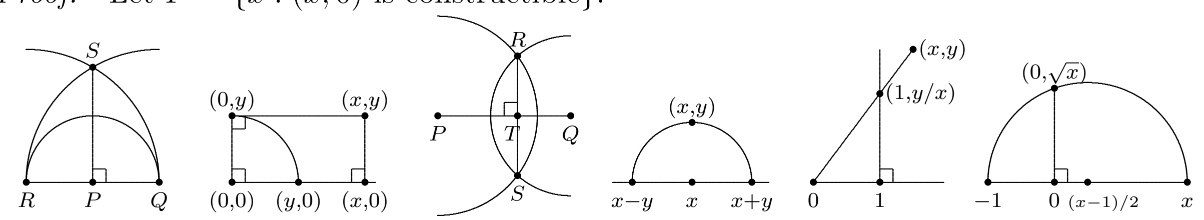
The point $P \in \mathbb{R}^2$ is **constructible by straight edge and compass** from the set of points $\{P_1,\dots,P_n\}$ if there is a sequence of points P_{n+1}, P_{n+2}, $\dots$, $P_m = P$, where each P_i, $i > n$ is constructed from previous points using one of the following constructions:

1. P_i is the point of intersection of two distinct lines of the form $L(P_j,P_k)$, $j,k < i$,
2. P_i is any point of intersection of two distinct circles of the form $C(P_j,P_k)$, $j,k < i$,
3. P_i is any point of intersection of a line $L(P_j,P_k)$ and a circle $C(P_r,P_s)$, $j,k,r,s < i$.

We say a line (resp. circle) is constructible if it is of the form $L(P,Q)$ (resp. $C(P,Q)$) for some pair of constructible points P and Q. If $n = 1$ then the only constructible point is P_1, hence we may assume $n \geq 2$. Define a Cartesian coordinate system so that $P_1 = (0,0)$ and $P_2 = (1,0)$.

Lemma 3.1 *The set of constructible points is of the form $\mathcal{C} = \{(x,y) : x,y \in F\}$ where F is some subfield of $\mathbb{R}$. Moreover, if $a \in F$ and $a > 0$ then $\sqrt{a} \in F$.*

Proof. Let $F = \{x : (x,0) \text{ is constructible}\}$.



Step 1 Steps 2 & 4 Step 3 Step 5 Step 6 Step 7

Step 1. If $P,Q \in \mathcal{C}$ then the line perpendicular to $L(P,Q)$ through P is constructible.
[$R \in L(P,Q) \cap C(P,Q)$, $S \in C(R,Q) \cap C(Q,R)$, $L(P,S)$ is perpendicular to $L(P,Q)$.]
Call this line $L^\perp(P,Q)$.
Step 2. If $(x,0),(y,0) \in \mathcal{C}$ then $(x,y) \in \mathcal{C}$.
[$(0,y) \in C((0,0),(y,0)) \cap L^\perp((0,0),(1,0))$, $(x,y) \in L^\perp((0,y),(0,0)) \cap L^\perp((x,0),(0,0))$.]
Step 3. If $P,Q,R \in \mathcal{C}$ then the projection of R onto $L(P,Q)$ is constructible.
[$S \in C(P,R) \cap C(Q,R)$, $T \in L(R,S) \cap L(P,Q)$.]
Step 4. If $(x,y) \in \mathcal{C}$ then $(x,0),(y,0) \in \mathcal{C}$.
[Project (x,y) onto $L((0,0),(1,0))$ and $L^\perp((0,0),(1,0))$ (the axes) to get $(x,0)$ and $(0,y)$.
$(y,0) \in C((0,0),(0,y)) \cap L((0,0),(1,0))$.]
Steps 2 and 4 imply that $\mathcal{C} = \{(x,y) : x,y \in F\}$.
Step 5. If $x,y \in F$ then $x \pm y \in F$.
[$C((x,0),(x,y)) \cap L((0,0),(1,0)) = \{(x+y,0),(x-y,0)\}$.]
Step 6. If $x,y \in F$ and $x \neq 0$ then $y/x, xy \in F$.
[$(1,y/x) \in L((0,0),(x,y)) \cap L^\perp((1,0),(0,0))$. Also $y/(1/x) = xy$.]
We have now shown that F is a field.
Step 7. If $x \in F$, $x > 0$, then $\sqrt{x} \in F$.
[$C((x-1)/2,0),(x,0) \cap L^\perp((0,0),(1,0)) = \{(0,\pm\sqrt{x})\}$.] □

Lemma 3.2 *If $[K : F] = 2$ and $\operatorname{char} F \neq 2$ then $K = F(\sqrt{\alpha})$ for some $\alpha \in F$.*

Proof. Pick any $\beta \in K$, $\beta \notin F$. Then $[F(\beta) : F] > 1$, so by the Tower Law, $F(\beta) = K$ and $\deg m_{\beta,F} = 2$. Hence β is the solution to $m_{\beta,F} = X^2 + bX + c = 0$ with $b, c \in F$. Hence $\beta = \frac{-b\pm\sqrt{\alpha}}{2}$ can be written in terms of a square root of $\alpha = b^2 - 4c \in F$. Conversely $\sqrt{\alpha} = \pm(2\beta + b)$ can be written in terms of β, so $F(\sqrt{\alpha}) = F(\beta) = K$. □

Theorem 3.3 *A point (x, y) is constructible from $\{P_1, \dots, P_n\}$, $P_0 = (0, 0)$, $P_1 = (1, 0)$, $P_i = (x_i, y_i)$, $i \geq 2$, iff there exists a sequence of fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m \subseteq \mathbb{R}$ with $F_0 = \mathbb{Q}(x_2, y_2, \dots, x_n, y_n)$, $[F_{i+1} : F_i] = 2$, and $x, y \in F_m$.*

Proof. Let F_m be as described above and let F be defined as in Lemma 1. Then $x_i, y_i \in F$, $i = 2, \dots, n$, so $F \supseteq F_0$. Also, $[F_{i+1} : F_i] = 2$, so by Lemma 2, $F_{i+1} = F_i(\sqrt{a})$ for some $a \in F_i$ and $a > 0$ (since $F_{i+1} \subseteq \mathbb{R}$). Hence by induction $F \supseteq F_i$. Thus $x, y \in F_m \subseteq F$ and (x, y) is constructible. Conversely suppose (x, y) is constructible, it is enough to show that if the coordinates of $P_1, \dots, P_{i-1}$ lie in K and $P_i = (x, y)$ is the intersection of lines and/or circles formed from P_j, $j < i$, then $[K(x, y) : K] \leq 2$. If $P, Q \in K^2$, then $L(P, Q)$ is given by an equation of the form $ax + by + c = 0$ where $a, b, c \in K$. Similarly $C(P, Q)$ is a circle of the form $x^2 + y^2 + ax + by + c = 0$, $a, b, c \in K$. It is easy to check that the x and y coordinates of an intersection of such lines and circles can be obtained by solving a linear or quadratic equation. (For the intersection of circles, subtracting the equations reduces to the case of intersecting a circle with a line.) Hence $[K(x, y) : K] \leq 2$. □

From Theorem 3.3 and the Tower Law, if (x, y) is constructible then $[F_0(x, y) : F_0]$ is a power of 2, or equivalently, if $\alpha \in F$ then $[F_0(\alpha) : F_0]$ is a power of 2.

Examples:

1. 'The cube cannot be doubled'.
   The aim is to construct a length $\sqrt[3]{2}$ times longer than a given length P_0P_1. This would imply $\sqrt[3]{2} \in F$ which is impossible since $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ is not a power of 2.

2. 'The circle cannot be squared'.
   The aim is to construct a length $\sqrt{\pi}$ times longer than a given length P_0P_1. This would imply $\pi \in F$ which is impossible since $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ is not a power of 2.

3. In general, 'angles cannot be trisected'.
   An angle is given by three points P_0, P_1, P_2 where $P_0 = (0, 0)$, $P_1 = (1, 0)$, and $P_2 = (x, y)$ where $y/x = \tan\theta$. By intersecting $L(P_0, P_2)$ and $C(P_0, P_1)$ we see $P_2' = (\cos\theta, \sin\theta)$ is constructible. Hence $a = 2\cos\theta \in F$. Conversely we can construct a suitable P_2 from $P_2' = (a, 0)$ by intersecting $L^{\perp}(P_2', P_0)$ with $C(P_0, (2, 0))$. Hence we may assume $F_0 = \mathbb{Q}(a)$. If there are constructible points Q_1, Q_2, Q_3 that make an angle $\theta/3$ then an easy exercise shows that $\alpha = 2\cos(\theta/3) \in F$. Hence $[\mathbb{Q}(a)(\alpha) : \mathbb{Q}(a)]$ is a power of 2. By the triple angle formula for cosines, α is a root of $X^3 - 3X - a = 0$. There are many choices for a that make this polynomial irreducible over $\mathbb{Q}(a)$, for example $a = 1$ ($\theta = 60^\circ$). But then $[\mathbb{Q}(a)(\alpha) : \mathbb{Q}(a)] = 3$, a contradiction.
   Note that *some* angles can be trisected, e.g., $\theta = 90^\circ$ ($a = 0$).

7262 4. Splitting field extensions Spring 2018

We start with a rather technical, but very useful, lemma.

Lemma (Extension Theorem) *Let $\phi\colon F_1 \to F_2$ be an isomorphism of fields. Let K_1/F_1 and K_2/F_2 be two extensions and let $\alpha \in K_1$. Then there is an extension of ϕ to $\tilde{\phi}\colon F_1(\alpha) \to K_2$ with $\tilde{\phi}_{|F_1} = \phi$ and $\tilde{\phi}(\alpha) = \beta \in K_2$ iff β is a zero of $\phi(m_{\alpha,F_1}) \in F_2[X]$. Moreover, for each such β $\tilde{\phi}$ is unique.*

$$\begin{array}{ccc} K_1 & & K_2 \\ \uparrow & & \uparrow \\ F_1(\alpha) & \stackrel{\tilde{\phi}}{\to} & F_2(\beta) \\ \uparrow & & \uparrow \\ F_1 & \stackrel{\phi}{\to} & F_2 \end{array}$$

[If $f \in F_1[X]$ then $\phi(f) \in F_2[X]$ is obtained by applying ϕ to the coefficients of f. In terms of our earlier notation, $\phi(f) = \mathrm{ev}_{\phi,X}(f)$.]

Proof. Write $m_{\alpha,F_1} = \sum b_i X^i$. If $\tilde{\phi}$ exists and $\beta = \tilde{\phi}(\alpha)$ then $\phi(m_{\alpha,F_1})(\beta) = \sum \phi(b_i)\beta^i = \sum \tilde{\phi}(b_i)\tilde{\phi}(\alpha)^i = \tilde{\phi}(\sum b_i\alpha^i) = \tilde{\phi}(0) = 0$. Also, $\tilde{\phi}$ is unique since every element of $F_1(\alpha)$ can be written in the form $f(\alpha)$, $f \in F_1[X]$, and $\tilde{\phi}(f(\alpha)) = \phi(f)(\beta)$ is uniquely determined. Conversely, assume β is a zero of $\phi(m_{\alpha,F_1})$, then $\phi(m_{\alpha,F_1}) = m_{\beta,F_2}$ since it is monic, irreducible, and has β as a root. Now both $\mathrm{ev}_{1,\alpha}\colon F_1[X] \to F_1(\alpha)$ and $\mathrm{ev}_{\phi,\beta}\colon F_1[X] \to F_2(\beta)$ are surjective with kernel (m_{α,F_1}) and we can define $\tilde{\phi}$ as the composition of the two isomorphisms

$$F_1(\alpha) \cong F_1[X]/(m_{\alpha,F_1}) \cong F_2(\beta).$$

Under this isomorphism $\alpha \mapsto X + (m_{\alpha,F_1}) \mapsto \beta$ and $c \mapsto c + (m_{\alpha,F_1}) \mapsto \phi(c)$ for $c \in F_1$. □

We shall often use this lemma with $F_1 = F_2$ and $\phi = 1$. Note that the image of $\tilde{\phi}$ is $F_2(\beta)$, so $\tilde{\phi}$ gives an isomorphism $F_1(\alpha) \to F_2(\beta)$.

Examples:

1. The fields $\mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q}(i\sqrt[4]{2})$ are isomorphic, but distinct, subfields of $\mathbb{C}$.
2. There is an automorphism of $\mathbb{Q}(\sqrt{2})$ sending $\sqrt{2}$ to $-\sqrt{2}$ and fixing $\mathbb{Q}$.

A polynomial $f \in F[X]$ **splits** in K/F if it factors as a product of linear factors in $K[X]$.

Examples:

1. The polynomial $X^2 - 2$ splits in $\mathbb{Q}(\sqrt{2})$.
2. The polynomial $X^3 - 2$ has a zero, but does not split in $\mathbb{Q}(\sqrt[3]{2})$ since $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, but only one of the three roots of $X^3 - 2 = 0$ is real.

A **splitting field extension (sfe)** of $f \in F[X]$ is an extension K/F such that

(a) f splits in K; and

(b) if $F \subseteq L \subseteq K$ and f splits in L then $L = K$.

More generally, a **splitting field extension** of $\mathcal{F} \subseteq F[X]$ is an extension K/F such that

(a) f splits in K for all (non-zero) $f \in \mathcal{F}$; and

(b) if $F \subseteq L \subseteq K$ and f splits in L for all $f \in \mathcal{F}$ then $L = K$.

Theorem 4.1 *If $f \in F[X]$ then there exists an extension K/F in which f splits. Moreover, if $\deg f = n$ then such a K exists with $[K:F] \le n!$.*

Proof. Induction on n. For $n = 1$, f is linear, so is already split. Assume $n > 1$ and let g be an irreducible factor of f in $F[X]$. Let $F' = F[X]/(g)$. Then (g) is a maximal ideal, F' is a field, and F'/F is a field extension. Let $\alpha = X + (g) \in F'$. Then $g(\alpha) = 0$ in F'. Thus $f(\alpha) = 0$ and using the division algorithm we can write $f(X) = (X - \alpha)h(X)$ in $F'[X]$. Applying induction, there exists an extension K/F' in which $h(X)$ splits and $[K:F'] \le (n-1)!$. But then $f(X)$ splits in K and $[K:F] = [K:F'][F':F] \le n!$. □

We can extend this theorem to any *finite* set $\mathcal{F}$ of polynomials by considering the polynomial $f(X) = \prod_{g \in \mathcal{F} \setminus \{0\}} g(X) \in F[X]$. For infinite $\mathcal{F}$ one needs Zorn's lemma.

Theorem 4.2 *If every $f \in \mathcal{F}$ splits in K then there exists a unique subfield $L \subseteq K$ such that L/F is a sfe for $\mathcal{F}$.*

Proof. Let $A = \{\alpha \in K : \alpha \text{ is a zero of some } f \in \mathcal{F}\}$. Suppose $\mathcal{F}$ splits in $L \subseteq K$. If $f \in \mathcal{F}$, then $f = c\prod(X - \alpha_i)$ in $K[X]$ and $f = c' \prod(X - \beta_i)$ in $L[X] \subseteq K[X]$. By unique factorization in $K[X]$, $\alpha_i = \beta_i$ (up to permutation of factors), so $\alpha_i \in L$. Thus $A \subseteq L$ and hence $F(A) \subseteq L$. Conversely, every $f \in \mathcal{F}$ splits in $F(A)$. Hence $L = F(A)$ is the unique subfield of K that is a sfe for $\mathcal{F}$. □

Theorem 4.3 *Any two sfe's for $f \in F[X]$ are isomorphic.*

Proof. We shall prove a slightly stronger result: If $\phi\colon F \to F'$ is an isomorphism, K is a sfe of $f \in F[X]$, and $\phi(f)$ splits in K'/F', then there is an extension $\tilde{\phi} : K \to K'$ of ϕ.

Let g be a monic irreducible factor of f and let α be a zero of g in K and β a zero of $\phi(g)$ in K'. By the Extension Theorem, ϕ extends to an isomorphism $\phi'\colon F(\alpha) \to F'(\beta)$. Write $f(X) = (X - \alpha)h(X)$ in $F(\alpha)[X]$. Now $K/F(\alpha)$ is a sfe for h and $\phi'(h)$ splits in K' (since $\phi'(h) \mid \phi(f)$). Hence by induction on $\deg f$, ϕ' extends to a map $\tilde{\phi}\colon K \to K'$.

Now assume K' is also a sfe and $F = F'$. Then f splits in $\operatorname{Im}\tilde{\phi} \subseteq K'$. Hence $\operatorname{Im}\tilde{\phi} = K'$ and $\tilde{\phi}$ is an isomorphism. □

Putting Theorems 4.1–4.3 together, we see that a sfe for $f \in F[X]$ exists, is unique up to isomorphism, has degree at most $n!$ over F, and can be written as $K = F(\alpha_1, \dots, \alpha_n)$ where $\alpha_1, \dots, \alpha_n$ are the zeros of f in K.

Examples:

1. The sfe of $X^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}) = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$, where $\zeta_3 = e^{2\pi i/3}$. This extension is of degree $6 = 3!$ over $\mathbb{Q}$. [Prove this!]
2. The sfe of $X^3 - 2$ over $\mathbb{R}$ is $\mathbb{C}$, which is of degree $2 < 3!$ over $\mathbb{R}$.

Exercise: Find the sfe K of $X^4 - 2$ over $\mathbb{Q}$. What is $[K:\mathbb{Q}]$?

The aim is to used Zorn's Lemma to prove, given F, the existence and uniqueness of the splitting field extension of any $\mathcal{F} \subseteq F[X]$. We need to generalize Theorems 4.1 and 4.3 above. (Theorem 4.2 already applies to any $\mathcal{F}$.)

Theorem 5.1 *For any F, there exists an extension K/F in which every $f \in F[X]$ splits.*

The idea of the proof is to use Zorn's Lemma to construct a "maximal" algebraic extension. Unfortunately the collection of algebraic extensions do not form a set, so we have to be a bit more careful. In particular, we need to fix the underlying set of elements we use.

Proof. Let $\mathcal{L} = \{(f, n) : f \in F[X]$ is a monic irreducible polynomial and $n \in \mathbb{N}\}$. An $\mathcal{L}$-extension (not standard notation) will be a field $(K, +, \times)$ where

1. $K \subseteq \mathcal{L}$,
2. the map $i\colon F \to K$ given by $i(a) = (X - a, 1)$ is a ring homomorphism (so K/F is an extension and F can be identified with the set $\{(X - a, 1) : a \in F\} \subseteq K$),
3. if $\alpha = (f, n) \in K$ then $f(\alpha) = 0$ (coefficients c_i of f are identified with $i(c_i) \in K$).

It is clear that any algebraic extension is isomorphic to one of this form. Indeed, if M/F is an algebraic extension we can just rename the roots $\alpha_1, \dots, \alpha_r$ of any irreducible polynomial $f = m_{\alpha_1,F}$ as $(f, 1), \dots, (f, r)$. Since each f has only finitely many roots we never run out of elements of $\mathcal{L}$. [Technically this requires the axiom of choice since there are an infinite number of choices as to how to do the renaming: for each f we must order the roots.]

Let $\mathcal{X}$ be the set of all $\mathcal{L}$-extensions. It is clear that $\mathcal{X}$ is a set. Indeed, it is a subset of $\mathcal{P}(\mathcal{L}) \times \mathcal{P}(\mathcal{L} \times \mathcal{L} \times \mathcal{L}) \times \mathcal{P}(\mathcal{L} \times \mathcal{L} \times \mathcal{L})$ where $\mathcal{P}(A)$ denotes the set of all subsets of A. [We regard $+$ and $\times$ as subsets of $\mathcal{L} \times \mathcal{L} \times \mathcal{L}$, since they can be determined by the set of all triples $(a, b, a + b)$ or (a, b, ab).]

Define a partial order on $\mathcal{L}$-extensions by setting $(K, +, \times) \le (K', +', \times')$ iff K is a subfield of K'., i.e., $K \subseteq K'$ and $+$ and $\times$ are the restrictions of $+'$ and $\times'$ to K. It is clear that $\le$ is a partial order.

The field $\{(X - a, 1) : a \in F\}$ with $(X - a, 1) + (X - b, 1) = (X - (a + b), 1)$ and $(X - a, 1)(X - b, 1) = (X - ab, 1)$ is an $\mathcal{L}$-extension, so $\mathcal{X} \neq \emptyset$. Let $\mathcal{T}$ be a chain in $\mathcal{X}$. We claim that $\bigcup_{K \in \mathcal{T}} K \in \mathcal{X}$. If $\alpha, \beta \in \bigcup_{K \in \mathcal{T}} K$ then $\alpha \in K_1$, $\beta \in K_2$ for some $K_1, K_2 \in \mathcal{T}$. Since $\mathcal{T}$ is totally ordered, we can assume $K_1 \le K_2$, so $\alpha, \beta \in K_2$. Define $\alpha + \beta$ and $\alpha\beta$ by their values in K_2. Then by the definition of $\le$, these values agree with their values in any $K \in \mathcal{T}$ with $K_2 \le K$. The field axioms follow immediately, since to check an axiom, we just take any $K \in \mathcal{T}$ big enough to contain all the relevant elements and use the corresponding axioms in K. The fact that $a \mapsto (X - a, 1)$ is a ring homomorphism and $f(\alpha) = 0$ when $\alpha = (f, n)$ follow from the corresponding properties in each $K \in \mathcal{T}$. It is now clear that $\bigcup_{K \in \mathcal{T}} K$ is an upper bound for $\mathcal{T}$. Zorn's Lemma now provides us with the existence of a maximal $\mathcal{L}$-extension, $(M, +, \times)$ say.

We now prove that every $f \in F[X]$ splits in M. If not, then there exists a sfe for f over M, say M'/M with $M' \neq M$. But M'/M and M/F are algebraic, so M'/F is algebraic.

By renaming the elements of M' we can assume $M \subseteq M'$. By renaming the elements $\alpha \in M' \setminus M$ as $(m_{\alpha,F}, i)$ as above, we can assume that M' is an $\mathcal{L}$-extension containing M. Note that we never run out of choices for i since every $m_{\alpha,F}$ has only finitely many roots. Clearly $M \leq M'$ and $M \neq M'$ contradicting the choice of M. Hence every polynomial in $F[X]$ splits in M. □

Theorem 5.3 *If K/F and M/F are extensions with K/F an sfe for $\mathcal{F} \subseteq F[X]$ and assume $\mathcal{F}$ splits in M. There exists an homomorphism $\phi\colon K \to M$ that fixes F. In particular, if M/F is also an sfe for $\mathcal{F}$ then ϕ is an isomorphism.*

Proof. Let $\mathcal{X}$ be the set of homomorphisms $\phi\colon L_\phi \to M$ where L_ϕ is some subfield of K containing F and ϕ fixes F. The inclusion $F \to M$ lies in $\mathcal{X}$, so $\mathcal{X} \neq \emptyset$. Define a partial ordering on $\mathcal{X}$ by $\phi \leq \psi$ if $L_\phi \subseteq L_\psi$ and $\phi = \psi$ on L_ϕ. This is clearly a partial order. Let $\mathcal{T}$ be a chain in $\mathcal{X}$. Define $\tilde{L}$ to be $\bigcup_{\phi\in\mathcal{T}} L_\phi$. Since the L_ϕ are totally ordered by inclusion, $\tilde{L}$ is a subfield of K containing F. [If $\alpha, \beta \in \tilde{L}$ then $\alpha \in L_\phi$, $\beta \in L_\psi$ for some $\phi, \psi \in \mathcal{T}$. Since $\mathcal{T}$ is totally ordered, we may assume $\phi \leq \psi$, so $\alpha, \beta \in L_\psi$. Then $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in L_\psi \subseteq \tilde{L}$.] Define $\tilde{\phi}(a)$ to be $\phi(a)$ for any $\phi \in \mathcal{T}$ for which $a \in L_\phi$. Since $\mathcal{T}$ is totally ordered, if $a \in L_\phi, L_\psi$ we can assume $\phi \leq \psi$ and so $\phi(a) = \psi(a)$. Hence $\tilde{\phi}$ is well defined. It is obvious that $\tilde{\phi}$ is a ring homomorphism from $\tilde{L}$ to M, so $\tilde{\phi} \in \mathcal{X}$ and it is clearly an upper bound for $\mathcal{T}$. Now using Zorn's Lemma we have a maximal $\phi \in \mathcal{T}$.

If $L_\phi \neq K$ then some $f \in \mathcal{F}$ does not split in L_ϕ. Hence there exists a root α of f with $\alpha \in K$ and $\alpha \notin L_\phi$. Let m_α be the minimal polynomial of α over L_ϕ. Note that $m_\alpha \mid f$. Let $L' = \mathrm{Im}(\phi)$ be the image of L_ϕ in M. Then L' is a subfield of M, isomorphic (via ϕ) to L_ϕ. The image $\phi(m_\alpha)$ is therefore irreducible in $L'[X]$. Since $m_\alpha \mid f$, $\phi(m_\alpha) \mid \phi(f) = f$, so $\phi(m_\alpha)$ must split in M (since f does). Therefore there exists a $\beta \in M$ which is a root of $\phi(m_\alpha)$. The minimal polynomial of β over L' is clearly $\phi(m_\alpha)$, so by the Extension Theorem, there exists a $\tilde{\phi}\colon L_\phi(\alpha) \to M$ which agrees with ϕ on L_ϕ. Hence $\tilde{\phi} \in \mathcal{X}$ and $\phi < \tilde{\phi}$ contradicting the choice of ϕ. Therefore $L_\phi = K$.

Finally, since K is isomorphic to the image $\mathrm{Im}\,\phi$, $\mathcal{F}$ splits in $\mathrm{Im}\,\phi/F$ and $\mathrm{Im}\,\phi \subseteq M$. If M/F is a sfe, $\mathrm{Im}\,\phi = M$ and ϕ gives an isomorphism from K to M fixing F. □

Lemma 5.4 *If K/F is an extension, then K is a sfe for $\mathcal{F} = F[X]$ iff*
(a) K/F is algebraic; and
(b) K is **algebraically closed**: *every non-constant $f \in K[X]$ has a root in K.*

Proof. Assuming (a) and (b) and using induction on $\deg f$ we see that every $f \in F[X]$ splits in K. But every element of K is a root of some $f \in F[X]$ so K must be a sfe for $F[X]$. Conversely, if K is the sfe for $F[X]$ then K/F is algebraic and if $f \in K[X]$ is irreducible, $M = K[X]/(f)$ is an algebraic extension of K. But then M/F is algebraic, so every $\alpha \in M$ is a root of some $g \in F[X]$. But then $\alpha \in K$, so $M = K$ and f is linear. In particular every non-constant polynomial in $K[X]$ factors into linear factors, so has a root in K. □

The extension K of Lemma 5.4 is called the **algebraic closure** of F and is denoted $\overline{F}$. The above theorems show that the algebraic closure exists and is unique up to isomorphism.

7262 6. Normal Extensions Spring 2018

An extension K/F is **normal** iff K/F is algebraic and if any *irreducible* $f \in F[X]$ has a root in K then it splits in K.

Theorem 6.1 *Assume K/F is an extension. The following are equivalent.*

(a) K/F is normal,

(b) K/F is a sfe for some $\mathcal{F} \subseteq F[X]$,

(c) K/F is algebraic and for any field M and any two homomorphisms $\phi, \psi \colon K \to M$ with $\phi_{|F} = \psi_{|F}$, we have $\operatorname{Im}\phi = \operatorname{Im}\psi$.

Proof.
(a)⇒(b): Assume K/F is normal and let $\mathcal{F} = \{m_{\alpha,F} : \alpha \in K\}$. Then every $f \in \mathcal{F}$ splits in K, so $\mathcal{F}$ splits in K. Conversely, if $L \subseteq K$ and $\mathcal{F}$ splits in L then L contains all the roots of each $m_{\alpha,F}$. Hence L contains each $\alpha \in K$. Therefore $L = K$ and K is a sfe.
(b)⇒(c): Both $\operatorname{Im}\phi$ and $\operatorname{Im}\psi$ are subfields of M and are sfe's for $\phi(\mathcal{F}) = \psi(\mathcal{F})$ over F. Hence by Theorem 4.2, $\operatorname{Im}\phi = \operatorname{Im}\psi$.
(c)⇒(a): Assume K/F is not normal. Then there exists an irreducible $f \in F[X]$ such that f has a root $\alpha \in K$ but does not split over K, without loss of generality $f = m_{\alpha,F}$. Let M be a sfe over K for the set $\mathcal{F} = \{m_{\gamma,F} : \gamma \in K\}$, so in particular $f = m_{\alpha,F}$ splits in M. Let β be another root of f in M that does not lie in K. By the Extension Theorem, there exists an isomorphism $\phi \colon F(\alpha) \to F(\beta)$ fixing F. Now $M/F(\alpha)$ and $M/F(\beta)$ are sfe's for $\mathcal{F}$ and $\phi(\mathcal{F}) = \mathcal{F}$ respectively. Hence ϕ extends to an isomorphism $\tilde{\phi} \colon M \to M$ with $\tilde{\phi}(\alpha) = \beta$. Now $\tilde{\phi}_{|K}$ and the inclusion $i \colon K \to M$ are two maps $K \to M$ with distinct images since $\beta \in \operatorname{Im}\tilde{\phi}_{|K}$ but $\beta \notin \operatorname{Im} i$. This contradicts (c), so K/F is normal. □

Corollary 6.2 *An extension K/F is finite and normal iff it is the sfe over F of some polynomial $f \in F[X]$.*

Proof. If K/F is a sfe for f, then by Theorem 4.1+4.2 it is finite ($[K:F] \le (\deg f)!$), and by Theorem 6.1 it is normal.
If K/F is normal and $K = F(A)$ for some set A, then the proof of (a)⇒(b) above in fact shows that K is a sfe for $\mathcal{F} = \{m_{\alpha,F} : \alpha \in A\}$: clearly $\mathcal{F}$ splits in K, but if $\mathcal{F}$ splits in L, $K/L/F$, then L must contain A, and so contains $F(A) = K$. But if $[K:F] < \infty$ we can take A to be finite (e.g., a basis for K/F), and then a sfe for $\mathcal{F}$ is just a sfe for the single polynomial $f = \prod_{g \in \mathcal{F} \setminus \{0\}} g$. □

Let K/F be algebraic. Then M is a **normal closure** of K/F iff M is an extension of K such that

(a) M/F is normal; and

(b) if $K \subseteq L \subseteq M$ and L/F is normal then $L = M$.

In other words, M is a smallest extension of K such that M/F is normal. Clearly, if K/F is already normal then $M = K$, otherwise M will be larger (assuming it exists).

Lemma 6.3 *Let K/F be algebraic and $K = F(A)$ for some subset $A \subseteq K$. Then M/K is a normal closure of K/F iff M is a sfe for $\mathcal{F} = \{m_{\alpha,F} \mid \alpha \in A\}$ over K (or over F).*

Proof. Let M be a normal closure of K/F. Then every $m_{\alpha,F} \in \mathcal{F}$ has a root $\alpha \in K \subseteq M$. Hence every $m_{\alpha,F}$ splits in M. Let $L \subseteq M$ be a sfe for $\mathcal{F}$ over F. Then L contains all the roots of every $m_{\alpha,F} \in \mathcal{F}$. In particular $A \subseteq L$, so $F(A) = K \subseteq L$. This implies L is a sfe for $\mathcal{F}$ over K as well. Also L/F is a sfe, so is normal. Thus by the definition of normal closure $L = M$. Now let M/K be a sfe for $\mathcal{F}$. Let $L \subseteq M$ be a sfe for $\mathcal{F}$ over F. Then $A \subseteq L$, $F(A) = K \subseteq L$ and L is a sfe for $\mathcal{F}$ over K. Hence $L = M$ and M/F is normal. Now Let $K \subseteq L' \subseteq M$ with L'/F normal. Since every $m_{\alpha,F} \in \mathcal{F}$ has a root $\alpha \in K \subseteq L'$, it must split in L'. Therefore $\mathcal{F}$ splits in L' and $L' = M$ by definition of sfe. □

Corollary 6.4 *Normal closures exist and are unique up to isomorphism. Also, if $[K:F] < \infty$ and M/K is a normal closure of K/F then $[M:F] < \infty$.*

Proof. Existence and uniqueness up to isomorphism follow since M/K is a sfe for some $\mathcal{F}$. If $[K:F] < \infty$ then $K = F(A)$ for some finite set A. Hence M/F is a sfe for a finite set of polynomials and so $[M:F] < \infty$. □

Examples:

1. The normal closure of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is equal to the sfe of $m_{\sqrt[4]{2},\mathbb{Q}} = X^4 - 2$ over $\mathbb{Q}(\sqrt[4]{2})$ (or $\mathbb{Q}$), which is $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}, i^2\sqrt[4]{2}, i^3\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$.
2. Any quadratic extension is normal: Any quadratic extension K/F is of the form $K = F(\alpha)$ for some (any) $\alpha \in K$, $\alpha \notin F$. If $K = F(\alpha)$ then K/F is normal iff $m_{\alpha,F}$ splits, which it will definitely do if it is quadratic.
3. A normal extension of a normal extension need not be normal. For example, the extensions $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are both quadratic, so normal, but $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal ($X^4 - 2$ does not split in $\mathbb{Q}(\sqrt[4]{2})$).
4. If $M/K/F$ and M/F is normal, then M/K is normal, but K/F may not be: If M is a sfe of $\mathcal{F}$ over F then it is also a sfe of $\mathcal{F}$ over K. But, for example, $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ is normal while $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not.

7. Separability

Lemma 7.1 *Let K_1/F_1 and K_2/F_2 be extensions with $[K_1 : F_1] < \infty$. Let $\phi\colon F_1 \to F_2$ be an isomorphism. Then*

$$|\{\tilde{\phi}\colon K_1 \to K_2 : \tilde{\phi}_{|F_1} = \phi\}| \leq [K_1 : F_1].$$

Moreover if $K_1 = F_1(A)$ then equality holds iff $\phi(m_{\alpha,F_1})$ splits in $K_2[X]$ into distinct linear factors for all $\alpha \in A$.

Proof. Proof is by induction on $[K_1 : F_1]$. When $[K_1 : F_1] = 1$ the result is clear. Now assume $[K_1 : F_1] > 1$ and pick some $\alpha \in A$, $\alpha \notin F_1$. Now let $\beta_1, \dots, \beta_r \in K_2$ be the (distinct) roots of $\phi(m_{\alpha,F_1})$ in K_2. By the Extension theorem, for each $i = 1, \dots, r$ there exists an isomorphism $\phi_i\colon F_1(\alpha) \to F_2(\beta_i)$ given by $\phi_i(\alpha) = \beta_i$. By induction each ϕ_i can be extended to at most $[K_1 : F_1(\alpha)]$ maps $\tilde{\phi}\colon K_1 \to K_2$. Conversely any map $\tilde{\phi}\colon K_1 \to K_2$ gives by restriction to $F_1(\alpha)$ one of the maps ϕ_i. Therefore the number of $\tilde{\phi}$s is at most $[K_1 : F_1(\alpha)]r$. But $r \leq \deg m_{\alpha,F_1} = [F_1(\alpha) : F_1]$, so there are at most $[K_1 : F_1(\alpha)][F_1(\alpha) : F_1] = [K_1 : F_1]$ such maps.

Moreover, if m_{α,F_1} does not split into distinct linear factors in $K_2[X]$ then $r < \deg m_{\alpha,F_1}$ and we have a strict inequality. Conversely if every m_{α,F_1} does split into distinct linear factors then $r = \deg m_{\alpha,F_1}$. Also every $\phi_i(m_{\alpha',F_1(\alpha)})$ with $\alpha' \in A$ splits into distinct linear factors in $K_2[X]$ since they are factors of $\phi(m_{\alpha',F_1})$. Hence by induction the number of extensions of each ϕ_i is exactly $[K_1 : F_1(\alpha)]$ and we have equality. □

There are therefore two ways in which we may have fewer that $[K_1 : F_1]$ maps in Lemma 1. The first is if K_2 is not "big enough". In this case some of the m_{α,F_1} may not split. The other is that the m_{α,F_1} may split, but some of the roots may be multiple roots. This motivates the following definitions.

An *irreducible* polynomial $f \in F[X]$ is **separable** if it has no multiple roots in a sfe of f over F. An element $\alpha \in K$ is **separable over** F if it is algebraic over F and $m_{\alpha,F}$ is separable. An extension K/F is **separable** if every $\alpha \in K$ is separable over F. Polynomials, elements, and field extensions are **inseparable** iff they are not separable.

The **separable degree** $[K : F]_s$ of an algebraic extension K/F is the number of maps $\phi\colon K \to M$ which fix F, where M/F is (or contains) the normal closure of K/F.

Containing the normal closure means that all the $m_{\alpha,F}$'s in Lemma 7.1 split in $K_2 = M$. Enlarging M further does not affect the number of maps since the image of any map $K \to M$ will always lie in the normal closure. Thus, for example, one can also choose $M = \overline{F}$, the algebraic closure of F.

Corollary 7.2 *If K/F is finite then $[K : F]_s \leq [K : F]$ with equality iff K/F is separable.*

Proof. Immediate from Lemma 7.1 by taking $A = K$, $\phi = 1_F$. □

Example: Let $K = \mathbb{F}_p(t)$ and $F = \mathbb{F}_p(t^p) \subseteq K$ where t is a transcendental element over $\mathbb{F}_p$. Then K is obtained from F by adjoining a root of $f(X) = X^p - t^p$. In $K[X]$, $f(X)$ splits as $f(X) = (X - t)^p$. The only non-trivial monic factors of f in $K[X]$ are therefore of the form $(X-t)^r$, $0<r<p$, and it is clear that these do not lie in $F[X]$ (consider the constant term). Hence f is irreducible in $F[X]$ and so f, t, and K are inseparable over F.

In fact the above example is typical as the following lemma shows.

Lemma 7.3 *If $f \in F[X]$ is irreducible then the following are equivalent:*

(a) f is inseparable,

(b) $f'=0$ where f' is the formal derivative of f. (If $f=\sum a_n X^n$ then $f'=\sum n a_n X^{n-1}$.)

(c) $\operatorname{char} F = p > 0$ *and $f(X)=g(X^p)$ for some irreducible $g \in F[X]$.*

Proof. Write $f=(X-\alpha)h(X)$ in some sfe. Then $f'=(X-\alpha)h'+1.h$. In particular $f'(\alpha)=h(\alpha)$. If α is a multiple root of f then $f'(\alpha)=h(\alpha)=0$, so $m_\alpha \mid f'$. But $m_\alpha \mid f$ and f is irreducible, so $\deg m_\alpha = \deg f > \deg f'$. Hence $f'=0$. Conversely, if α is not a multiple root then $f'(\alpha)=h(\alpha)\neq 0$, so $f'\neq 0$. This proves (a)⇔(b).
If $f=\sum a_n X^n$ then $f'=\sum n a_n X^{n-1}$. Hence $f'=0$ iff $na_n=0$ for all n. If $\operatorname{char} F=0$ then f is a constant, contradicting the irreducibility of f. If $\operatorname{char} F=p$ then $a_n=0$ for all $p \nmid n$. Hence $f(X)=g(X^p)$. Any factorization of g would give a factorization of f, so g is irreducible. Conversely if $f(X)=g(X^p)$ and $\operatorname{char} F=p$ then $f'=0$. Hence (b)⇔(c). □

A field F is called **perfect** if every algebraic extension K/F is separable.

Lemma 7.4 *F is perfect iff either (a)* $\operatorname{char} F = 0$*, or (b)* $\operatorname{char} F = p > 0$ *and every element of F has a pth root in F.*

Proof. If F is perfect and $\operatorname{char} F = p > 0$, consider the polynomial $X^p - a$ for $a \in F$. In a sfe K/F this polynomial factors as $(X-b)^p$ where $b^p=a$. Thus $m_{b,F} \mid (X-b)^p$. If K/F is separable then $m_{b,F}$ has no multiple roots. Thus $m_{b,F}=X-b$ and $b\in F$.

If $\operatorname{char} F=0$ then K/F is separable. Assume $\operatorname{char} F = p>0$ and every element in F has a pth root. If α is not separable over F then the minimal polynomial of α is $f(X)=g(X^p)$ for some $g=\sum g_i X^i \in F[X]$. Let $h(X)=\sum g_i^{1/p} X^i$, where $g_i^{1/p}$ is any pth root of g_i in F. Then $h(X)^p=(\sum g_i^{1/p}X^i)^p=\sum g_i X^{pi}=g(X^p)=f(X)$. Hence f is not irreducible and cannot be the minimal polynomial of α. Hence every algebraic K/F is separable. □

Note: If K/F is an algebraic extension and $\operatorname{char} F = 0$ then K/F is automatically separable. Hence separability is only an issue in characteristic $p>0$.

Exercises

1. Show that if $\operatorname{char} F = p$ then the map $\phi\colon F \to F$ given by $\phi(a)=a^p$ is a homomorphism. Deduce that F is perfect iff either $\operatorname{char} F=0$ or ϕ is an isomorphism. [ϕ is called the **Frobenius map**.]
2. Show that if F is finite then ϕ is an isomorphism. Deduce that all finite fields are perfect.

Let K/F be an arbitrary field extension, then the **Galois group** of K/F is the group

$$\mathrm{Gal}(K/F) = \{\phi\colon K \to K : \phi_{|F} = 1_F,\ \phi \text{ is isomorphism}\},$$

with the group operation given by composition.

Let K be a field and G a group of automorphisms of K. The **fixed field** of G is

$$K^G = \{\alpha \in K : \forall g \in G\colon g(\alpha) = \alpha\}.$$

Note that K^G is indeed a subfield of K. [Proof: $g(1) = 1$, so $1 \in K^G$. If $\alpha, \beta \in K^G$ then $g(\alpha - \beta) = g(\alpha) - g(\beta) = \alpha - \beta$, so $\alpha - \beta \in K^G$, similarly for $\alpha\beta$, $1/\alpha$.]

K/F is a **Galois extension** if it is algebraic and $F = K^G$ for some G.

Note 1: For any K/F and G we have $F \subseteq K^{\mathrm{Gal}(K/F)}$ and $G \subseteq \mathrm{Gal}(K/K^G)$.

Note 2: If K/F is Galois then $F \subseteq K^{\mathrm{Gal}(K/F)} \subseteq K^G = F$. Thus without loss of generality we can assume $G = \mathrm{Gal}(K/F)$ in the definition of Galois extension.

Examples:

1. $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, c\}$, where c = complex conjugation. Now $\mathbb{C}^{\{1,c\}} = \{\alpha \in \mathbb{C} : \bar{\alpha} = \alpha\} = \mathbb{R}$. Hence $\mathbb{C}/\mathbb{R}$ is Galois.
2. If $g \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ then $g(\sqrt[3]{2})$ is a root of $X^3 - 2 = 0$ in $\mathbb{Q}(\sqrt[3]{2})$. But there is only one root $\sqrt[3]{2}$, so $g(\sqrt[3]{2}) = \sqrt[3]{2}$. Since $\sqrt[3]{2}$ generates $\mathbb{Q}(\sqrt[3]{2})$, $g = 1$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$. Now $\mathbb{Q}(\sqrt[3]{2})^{\{1\}} = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$, so $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois.
3. If $g \in \mathrm{Gal}(\mathbb{F}_p(t)/\mathbb{F}_p(t^p))$ then $g(t)^p = g(t^p) = t^p$. Thus $g(t)$ is a root of $X^p - t^p = (X - t)^p = 0$, so $g(t) = t$. Since t generates $\mathbb{F}_p(t)$, $g = 1$ and $\mathrm{Gal}(\mathbb{F}_p(t)/\mathbb{F}_p(t^p)) = \{1\}$. Now $\mathbb{F}_p(t)^{\{1\}} = \mathbb{F}_p(t) \neq \mathbb{F}_p(t^p)$, so $F_p(t)/\mathbb{F}_p(t^p)$ is not Galois.

Theorem 8.1 *K/F is Galois if and only if it is both normal and separable.*

Proof. The definitions of Galois, normal, and separable all require K/F to be algebraic, so we may assume this. Assume first that K/F is normal and separable. We know that $F \subseteq K^{\mathrm{Gal}(K/F)}$, so it enough to show that for every $\alpha \in K$, $\alpha \notin F$, there exists a $\phi \in \mathrm{Gal}(K/F)$ with $\phi(\alpha) \neq \alpha$. Since K/F is normal, $m_{\alpha,F}$ splits in $K[X]$. Since K/F is separable, $m_{\alpha,F}$ has distinct roots in K. Since $\alpha \notin F$, $\deg m_{\alpha,F} > 1$. Hence there is a $\beta \in K$ with $m_{\alpha,F}(\beta) = 0$, $\beta \neq \alpha$. By the Extension theorem, there exists $\phi\colon F(\alpha) \to F(\beta)$ fixing F with $\phi(\alpha) = \beta$. Since K/F is normal, K is the sfe of some $\mathcal{F} \subseteq F[X]$ over F. Hence K is a sfe of $\mathcal{F}$ over either $F(\alpha)$ or $F(\beta)$. By the proof of the uniqueness of the sfe, there exists an isomorphism $\tilde{\phi}\colon K \to K$ that agrees with ϕ on $F(\alpha)$. This $\tilde{\phi}$ is an element of $\mathrm{Gal}(K/F)$ which does not fix α.

Now assume K/F is Galois with $F = K^G$. For any $\alpha \in K$ let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_r$ be the *distinct* values of $g(\alpha)$ as g runs over $\mathrm{Gal}(K/F)$. Note that there are only finitely many such values (even if $\mathrm{Gal}(K/F)$ is infinite) since each α_i is a root of $m_{\alpha,F}$. Indeed, $r \leq \deg m_{\alpha,F}$. Consider the polynomial $f(X) = \prod_{i=1}^r (X - \alpha_i)$. Each $g \in G$ is injective on K and if $\alpha_i = h(\alpha)$ then $g(\alpha_i) = (gh)(\alpha) = \alpha_j$ for some j. Hence g permutes the α_is and so $g(f(X)) = f(X)$. Thus $f \in K^G[X] = F[X]$. But $f(\alpha) = 0$, so $m_{\alpha,F} \mid f$. Therefore $m_{\alpha,F}$ splits into distinct linear factors in $K[X]$. Since this holds for any $\alpha \in K$, K/F is both normal and separable. □

Note: The first part of the proof of Theorem 8.1 shows that if K/F is Galois and $\alpha \in K$ then $\mathrm{Gal}(K/F)$ permutes the roots of $m_{\alpha,F}$ **transitively**, i.e., for any other root β there exists $g \in \mathrm{Gal}(K/F)$ with $g(\alpha) = \beta$.

Theorem 8.2 *If G is a finite group of automorphisms of K then $[K : K^G] = |G|$ and $G = \mathrm{Gal}(K/K^G)$.*

Proof. Assume first that $[K : K^G] > |G| = n$. Let $\alpha_1, \dots, \alpha_m$, $m > n$, be a subset of K, linearly independent over K^G and let $G = \{g_1, \dots, g_n\}$. Consider the system of linear equations

$$g_j(\alpha_1)x_1 + \dots + g_j(\alpha_m)x_m = 0, \qquad j = 1, \dots, n. \tag{1}$$

There are n equations in $m > n$ unknowns x_i. Hence there is a non-trivial solution with $x_i \in K$. Pick a non-trivial solution with the least number of non-zero x_i. Without loss of generality assume $x_1, \dots, x_r \neq 0$ and $x_{r+1}, \dots, x_m = 0$. Let $g \in G$ and apply g to each of the equations above. Then

$$gg_j(\alpha_1)g(x_1) + \dots + gg_j(\alpha_r)g(x_r) = 0, \qquad j = 1, \dots, n. \tag{2}$$

As j varies, gg_j runs over all the elements of G. Hence

$$g_j(\alpha_1)g(x_1) + \dots + g_j(\alpha_r)g(x_r) = 0, \qquad j = 1, \dots, n. \tag{3}$$

Multiplying (2) by $g(x_r)$ and (3) by x_r and subtracting gives

$$\textstyle\sum_{i=1}^{r} g_j(\alpha_i)(x_i g(x_r) - x_r g(x_i)) = 0.$$

However the $i = r$ term vanishes, so we get a solution to (1) with fewer non-zero x_is. The only way in which this is possible is if all the coefficients $x_i g(x_r) - x_r g(x_i)$ are zero. But then $x_i/x_r = g(x_i/x_r)$ for all $g \in G$. Hence $y_i = x_i/x_r \in K^G$. Dividing through by x_r and setting $g_j = 1$ in (1) gives

$$\alpha_1 y_1 + \dots \alpha_r y_r = 0$$

with $y_i \in K^G$ non-zero, contradicting linear independence of the α_is. Thus $[K : K^G] \leq |G|$.

For any extension K/F, every element of $\mathrm{Gal}(K/F)$ is a map $K \to K$ which fixes F, hence gives a map $K \to M$ fixing F for any M/K. Thus

$$|\,\mathrm{Gal}(K/K^G)| \leq [K : K^G]_s \leq [K : K^G] \leq |G|.$$

But $G \subseteq \mathrm{Gal}(K/K^G)$, so $G = \mathrm{Gal}(K/K^G)$ and $|G| = [K : K^G]$. □

Exercises

1. Show that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ is Galois and $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong S_3$. [Hint: consider the action of an automorphism on the roots of $X^3 - 2 = 0$].
2. For each subgroup $H \leq \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$ identify the fixed field $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)^H$.
3. Show that if K/F is finite and separable then the normal closure M/F of K/F is finite and Galois.

Theorem (Fundamental Theorem of Galois Theory)
Assume K/F is a finite Galois extension, then there exists a bijection

$$\{\textit{subgroups } H \le \mathrm{Gal}(K/F)\} \leftrightarrow \{\textit{subfields } L \subseteq K : K/L/F\}$$
$$H \to K^H$$
$$\mathrm{Gal}(K/L) \leftarrow L$$

Proof. Since $|\mathrm{Gal}(K/F)| \le [K:F]$, $\mathrm{Gal}(K/F)$ is finite. We shall show the two maps given are inverse to each over. Starting with $H \le \mathrm{Gal}(K/F)$ we get $H \mapsto K^H \mapsto \mathrm{Gal}(K/K^H)$. Now H is finite so by Theorem 8.2, $H = \mathrm{Gal}(K/K^H)$. Starting with $L \subseteq K$, we get $L \mapsto \mathrm{Gal}(K/L) \mapsto K^{\mathrm{Gal}(K/L)}$. However, K/L is both normal and separable (since K/F is), so K/L is Galois and $L = K^{\mathrm{Gal}(K/L)}$. Thus these maps are inverse to one another and we have a bijection. □

The **join** or **compositum** L_1L_2 of two subfields L_1 and L_2 of a field K is the smallest field containing them both. I.e., $L_1L_2 = L_1(L_2) = L_2(L_1)$.

Warning: It is possible that $L_2 \cong L_3$ but $L_1L_2 \not\cong L_1L_3$. Hence you should always specify L_1 and L_2 as subfields of a specific field K. It is not enough just to define L_1 and L_2 up to isomorphism.

Corollary 9.1 *Let K/F be a finite Galois extension with* $\mathrm{Gal}(K/F) = G$. *Let $H_i \le G$ and let $L_i \subseteq K$ be the subfields corresponding to H_i. Then*

(a) $H_1 \le H_2$ iff $L_1 \supseteq L_2$ and in this case $[H_2 : H_1] = [L_1 : L_2]$,

(b) $H_1 \cap H_2$ corresponds to L_1L_2,

(c) $\langle H_1 \cup H_2\rangle$ corresponds to $L_1 \cap L_2$,

(d) if $g \in G$ then gHg^{-1} corresponds to $g(L)$,

(e) $H_1 \trianglelefteq H_2 \iff L_2/L_1$ is Galois $\iff L_2/L_1$ is normal, and in this case $\mathrm{Gal}(L_1/L_2) \cong H_2/H_1$.

Proof.
(a) If $H_1 \le H_2$, then $L_1 = K^{H_1} \supseteq K^{H_2} = L_2$.
If $L_1 \supseteq L_2$, then $H_1 = \mathrm{Gal}(K/L_1) \le \mathrm{Gal}(K/L_2) = H_2$.
$|H_i| = [K : K^{H_i}] = [K : L_i]$, so $[L_1 : L_2] = [K : L_2]/[K : L_1] = |H_2|/|H_1| = [H_2 : H_1]$.
(b) $H_1 \cap H_2$ is the largest subgroup of G that is contained in both H_1 and H_2. This corresponds to the smallest subfield of K that contains both L_1 and L_2, but this is just L_1L_2.
(c) $\langle H_1 \cup H_2\rangle$ is the smallest subgroup of G that contains both H_1 and H_2. This corresponds to the largest subfield of K that is contained in both L_1 and L_2, but this is just $L_1 \cap L_2$.
(d) Any element of $g(L)$ is of the form $g(\alpha)$ with $\alpha \in L$. But if $ghg^{-1} \in gHg^{-1}$ then h fixes α and so $ghg^{-1}(g(\alpha)) = g(h(\alpha)) = g(\alpha)$. Thus $g(\alpha)$ is fixed by gHg^{-1}, $g(L) \subseteq K^{gHg^{-1}}$. But g is an automorphism of K, so $[K : g(L)] = [g(K) : g(L)] = [K : L]$. Also $[K : L] = |H| = |gHg^{-1}| = [K : K^{gHg^{-1}}]$. Hence $g(L) = K^{gHg^{-1}}$.

(e) If $H_1 \trianglelefteq H_2$ then $gH_1g^{-1} = H_1$, so $g(L_1) = L_1$ for all $g \in H_2 = \operatorname{Gal}(K/L_2)$. Hence $g_{|L_1} \in \operatorname{Gal}(L_1/L_2)$. Thus we have a map $\phi\colon \operatorname{Gal}(K/L_2) \to \operatorname{Gal}(L_1/L_2)$ which maps $g \mapsto g_{|L_1}$. This is clearly a group homomorphism with kernel equal to $\operatorname{Gal}(K/L_1)$. But $L_2 \subseteq L_1^{\operatorname{Gal}(L_1/L_2)} \subseteq L_1^{\operatorname{Im}\phi} \subseteq K^{\operatorname{Gal}(K/L_2)} = L_2$, so L_1/L_2 is Galois. If L_1/L_2 Galois then L_1/L_2 normal, so we now prove L_1/L_2 normal implies $H_1 \trianglelefteq H_2$. If L_1/L_2 is normal and $g \in H_2$, then $g(L_1)$ must have the same image in K as $1(L_1) = L_1$. Hence $g(L_1) = L_1$ and $gH_1g^{-1} = H_1$. Thus $H_1 \trianglelefteq H_2$. Finally $H_2/H_1 = H_2/\operatorname{Ker}\phi \cong \operatorname{Im}\phi$ is a subgroup of $\operatorname{Gal}(L_1/L_2)$, but $[H_2 : H_1] = [L_1 : L_2] = |\operatorname{Gal}(L_1/L_2)|$, so the image of ϕ is $\operatorname{Gal}(L_1/L_2)$ and $\operatorname{Gal}(L_1/L_2) \cong H_2/H_1$. □

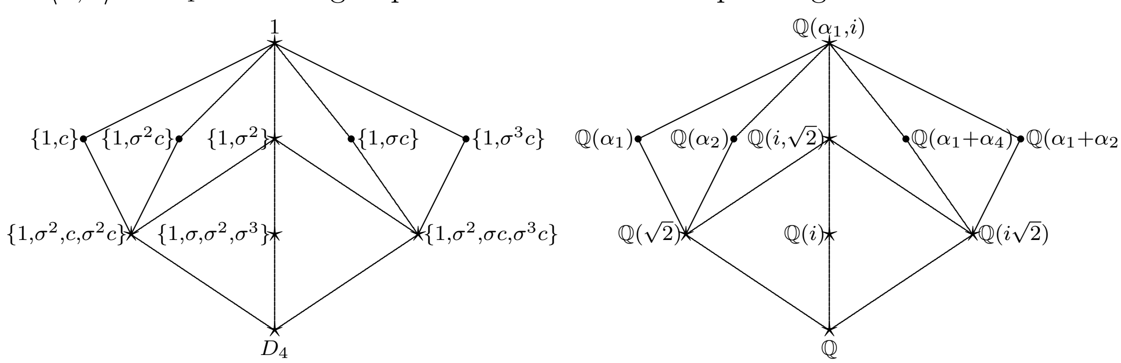
Lemma 9.2 *If K/F is the sfe for $f \in F[X]$ then* $\operatorname{Gal}(K/F)$ *is isomorphic to a subgroup of the symmetric group S_R where R is the set of roots of f in K.*

Proof. Map $\operatorname{Gal}(K/F) \to S_R$ by restricting $\phi \in \operatorname{Gal}(K/F)$ to $R \subseteq K$. The image is a permutation since ϕ is injective and maps the finite set R to R. The map is a group homomorphism since the group operation on each side is the same — composition of functions. If the image in S_R is the identity then ϕ fixes R and F, so fixes $F(R) = K$ and so $\phi = 1$. Hence the map $\operatorname{Gal}(K/F) \to S_R$ is injective and $\operatorname{Gal}(K/F)$ is isomorphic to the image of this map in S_R. □

Example: Consider $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ which is the sfe of $X^4 - 2$. Let $G = \operatorname{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$. By the Extension Theorem there exists a $\sigma \in G$ with $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$. There is also $c \in G$ with $c =$ complex conjugation. We do not know what $\sigma(i)$ is, but if $\sigma(i) = -i$ then $\sigma c(i) = i$ and $\sigma c(\sqrt[4]{2}) = \sqrt[4]{2}$. Hence by replacing σ with σc if necessary we may assume $\sigma(i) = i$. Let the four roots of $X^4 - 2$ be

$$\alpha_1 = \sqrt[4]{2}, \qquad \alpha_2 = i\sqrt[4]{2}, \qquad \alpha_3 = -\sqrt[4]{2}, \qquad \alpha_4 = -i\sqrt[4]{2}.$$

Then σ acts as the permutation (1234) and c acts as the permutation (24) on the roots. The subgroup of S_4 generated by these is D_4 which is of order 8. But $|G| = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$, so $G = \langle \sigma, c\rangle \cong D_4$. The subgroups of G and their corresponding subfields are:



In order to apply Galois theory we need a finite Galois extension. The following Lemma is therefore extremely useful.

Lemma 9.3 *If K/F is finite and separable and if M is the normal closure of K/F then M/F is finite and Galois.*

Proof. Exercise. □

7262 10. Finite Fields Spring 2018

If F is a field of characteristic p, then the map $\phi\colon F \to F$ given by $\phi(a) = a^p$ is called the **Frobenius map**.

Lemma 10.1 *The Frobenius map is a ring homomorphism from F to F.*

Proof. If $a, b \in F$ then $\phi(a+b) = (a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$. However, for $0 < i < p$ the binomial coefficient $\binom{p}{i} = p!/i!(p-i)!$ is divisible by p since $p \mid p!$ but $p \nmid i!(p-i)!$. Hence $\phi(a+b) = a^p + b^p = \phi(a) + \phi(b)$. Also $\phi(1) = 1$ and $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$. Thus ϕ is a ring homomorphism. $\square$

Note: The Frobenius map is always injective, but it need not be surjective. For example, take $F = \mathbb{F}_p(t)$ where t is transcendental over $\mathbb{F}_p$. Then $t \notin \operatorname{Im}\phi$.

Theorem 10.2 *For all primes p and all $n \geq 1$ there exists a field $\mathbb{F}_{p^n}$ with p^n elements. It is the sfe of $X^{p^n} - X$ over $\mathbb{F}_p$. Conversely every finite field is isomorphic to some $\mathbb{F}_{p^n}$.*

Proof. Let K be the sfe of $f(X) = X^{p^n} - X$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then K is finite and the Frobenius map ϕ is therefore an automorphism of K. Let G be the cyclic group of automorphisms of K generated by ϕ^n. Then $K^G = \{\alpha : \phi^n(\alpha) = \alpha\} = \{\alpha : \alpha^{p^n} = \alpha\}$ is just the set of roots of f in K. But K^G is a subfield of K containing $\mathbb{F}_p$ and all the roots of f. Hence $K = K^G = \{\alpha : f(\alpha) = 0\}$. For any root α, $f'(\alpha) = -1 \neq 0$, so f has no multiple roots. Since f splits in K, there are exactly p^n roots of f in K, and $|K| = p^n$.

Now assume K is some finite field. The characteristic of K cannot be zero, since otherwise K would contain $\mathbb{Q}$ which is infinite. Assume $\operatorname{char} K = p$. Then $\mathbb{F}_p \subseteq K$ and so $K/\mathbb{F}_p$ is a field extension. The extension is clearly finite since one cannot have a basis for K/F with more than $|K|$ elements. If $[K : \mathbb{F}_p] = n$ then $K \cong \mathbb{F}_p^n$ as a vector space, so $|K| = p^n$. Any $\alpha \in K$ is either zero, or in $K^\times$ which is a group of order $p^n - 1$. Hence either $\alpha = 0$ or $\alpha^{p^n-1} = 1$. Thus every $\alpha \in K$ is a root of $f(X) = X^{p^n} - X$. Since there are at most p^n roots of f in K and $|K| = p^n$, f splits in K. Thus K contains a sfe of f over $\mathbb{F}_p$. But since K consists of the roots of f, K must be equal to a sfe of f over $\mathbb{F}_p$. Since any two sfe's are isomorphic, $K \cong \mathbb{F}_{p^n}$. $\square$

Theorem 10.3 *Any finite extension K/F of a finite field F is Galois. The Galois group is cyclic and is generated by a power of the Frobenius map.*

Proof. Since $|F| < \infty$ and $[K : F] < \infty$, we have $|K| = |F|^{[K:F]} < \infty$. Assume $K = \mathbb{F}_{p^n}$ and let G be the cyclic group of automorphisms generated by the Frobenius map ϕ. The fixed field $K^G = \{\alpha : \phi(\alpha) = \alpha\}$ is just the set of roots of the polynomial $X^p - X = 0$. But there are at most p roots, and ϕ fixes $\mathbb{F}_p$. Therefore $K^G = \mathbb{F}_p$. Hence $K/\mathbb{F}_p$ is Galois and $\operatorname{Gal}(K/\mathbb{F}_p) = G$ is a cyclic group, generated by the Frobenius map ϕ.

If K/F then $\mathbb{F}_p \subseteq F \subseteq K$, so by the Fundamental theorem of Galois theory, $F = K^H$ for some $H \leq G$. Thus K/F is Galois with Galois group $\operatorname{Gal}(K/F) = H$. Now H is a subgroup of a cyclic group G, so is cyclic. It is generated by some element of G, which is a power of ϕ. $\square$

Note: If $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n. The subgroups are cyclic of order m for some $m \mid n$ and are generated by $\phi^{n/m}$. The fixed field of $\phi^{n/m}$ is just $\mathbb{F}_{p^{n/m}}$. Hence the subfields of $\mathbb{F}_{p^n}$ are precisely the $\mathbb{F}_{p^d}$ for all $d \mid n$.

Lemma 10.4 *Any finite subgroup G of the multiplicative group $F^\times$ of a field is cyclic.*

Proof. G is finite and abelian, so $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$ where $d_{i+1} \mid d_i$. Every element of G has order dividing d_1, so $X^{d_1} - 1 = 0$ has at least $|G| = d_1 d_2 \ldots d_r$ roots. But then $|G| \leq d_1$, so $d_2 = \cdots = d_r = 1$ and G is cyclic. □

Corollary 10.5 *For each n there exists some irreducible polynomial of degree n in $\mathbb{F}_p[X]$. Furthermore $X^{p^n} - X$ is the product of all monic irreducible polynomials of degree $d \mid n$.*

Proof. The group $\mathbb{F}_{p^n}^\times$ is cyclic, generated by α say. Then $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ and the minimal polynomial $m_{\alpha,\mathbb{F}_p}$ is irreducible of degree $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

Write $X^{p^n} - X = \prod f_i$ where f_i are irreducible monic polynomials in $\mathbb{F}_p[X]$. If α is a root of f_i in the sfe $\mathbb{F}_{p^n}$, then $\mathbb{F}_p(\alpha)$ is a subfield of $\mathbb{F}_{p^n}$. Hence $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$ for some $d \mid n$ and $f_i = m_{\alpha,\mathbb{F}_p}$ has degree $[\mathbb{F}_{p^d} : \mathbb{F}_p] = d$. Conversely if f is an irreducible polynomial of degree $d \mid n$, and α is a root of f in some extension, then $\mathbb{F}_p(\alpha)$ is isomorphic to $\mathbb{F}_{p^d}$. But every element of $\mathbb{F}_{p^d}$ is a root of $X^{p^d} - X \mid X^{p^n} - X$. Hence α is a root of $X^{p^n} - X$. Thus $f \mid X^{p^n} - X$. Since $X^{p^n} - X$ has no multiple roots, it cannot be divisible by f^2. Hence $X^{p^n} - X$ is precisely the product of monic irreducible polynomials of degree $d \mid n$. □

Lemma 10.6 *If $f \in \mathbb{F}_p[X]$ and $f = f_1 f_2 \ldots f_r$ where $f_i \in F_p[X]$ are distinct irreducibles, then the sfe for f over $\mathbb{F}_p$ is $\mathbb{F}_{p^d}$ where $d = \mathrm{lcm}\{\deg f_i\}$. The Frobenius map ϕ acts on the roots of f as a permutation of cycle type $(\deg f_1)(\deg f_2) \ldots (\deg f_r)$ in $S_{\deg f}$ permuting the roots of each f_i cyclically.*

Proof. Let K be the sfe for f. The Galois group $G = \mathrm{Gal}(K/\mathbb{F}_p)$ permutes the roots of each f_i transitively and is also cyclic, generated by the Frobenius map ϕ. The only way this can happen is if ϕ permutes the roots of f_i cyclically, and so has cycle type $(\deg f_1)(\deg f_2) \ldots (\deg f_r)$. Finally, if $K = \mathbb{F}_{p^d}$ then $d = [K : \mathbb{F}_p] = |G| =$ the order of ϕ, which is $\mathrm{lcm}\{\deg f_i\}$. □

Notation If $f \in F[X]$, then $\mathrm{Gal}(f/F)$ denotes $\mathrm{Gal}(K/F)$, where K/F is a sfe for f.

Theorem (Comparison Theorem) *If $f = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$, p is a prime with $p \nmid a_n$, and the reduction $\bar{f}$ of f mod p is a product of* **distinct** *irreducible polynomials in $\mathbb{F}_p[X]$, $\bar{f} = f_1 \ldots f_r$, then $\mathrm{Gal}(f/\mathbb{Q})$ contains an automorphism which acts on the roots of f as a permutation with cycle type $(\deg f_1)(\deg f_2) \ldots (\deg f_r)$.*

The proof of this result is rather technical, so I will not include it here.

Example: Let $f(X) = X^3 + 7X + 3$. Then mod 2, $\bar{f} = X^3 + X + 1$ is irreducible, so $\mathrm{Gal}(f/\mathbb{Q})$ contains a 3-cycle. But mod 3, $\bar{f} = X^3 + X = X(X^2 + 1)$, and $X^2 + 1$ is irreducible. Therefore $\mathrm{Gal}(f/\mathbb{Q})$ contains an element of cycle type (1)(2), i.e., a transposition. Since $\mathrm{Gal}(f/\mathbb{Q})$ is a subgroup of S_3, $\mathrm{Gal}(f/\mathbb{Q}) \cong S_3$.

A **primitive** nth root of 1 is an element $\zeta_n \in K$ with order n in $K^\times$, i.e., $\zeta_n^n = 1$ but $\zeta_n^r \neq 1$ for $0 < r < n$.

Lemma 11.1 *If K/F is a sfe for $X^n - 1$ and $\operatorname{char} F \nmid n$ then the roots of $X^n - 1$ in K are $\{1, \zeta_n, \dots, \zeta_n^{n-1}\}$ where $\zeta_n \in K$ is a primitive nth root of 1. Also $K = F(\zeta_n)$ and K/F is Galois with $\operatorname{Gal}(K/F) \leq (\mathbb{Z}/n\mathbb{Z})^\times$ where $(\mathbb{Z}/n\mathbb{Z})^\times = \{r \bmod n : \gcd(r, n) = 1\}$ is the group of units of $\mathbb{Z}/n\mathbb{Z}$ under multiplication.*

Proof. Let $A = \{\alpha \in K : \alpha^n = 1\}$. Then A is a subgroup of $K^\times$. If α is a multiple root of $f(X) = X^n - 1$ then $f'(\alpha) = n\alpha^{n-1} = 0$. But $\alpha \neq 0$ and $\operatorname{char} F \nmid n$, so this is impossible. Hence $|A| = n$. Since any finite subgroup of $K^\times$ is cyclic, $A = \{1, \zeta_n, \dots, \zeta_n^{n-1}\}$ for some ζ_n which is then a primitive nth root of 1. Now $K = F(A) = F(\zeta_n)$ is normal and separable over F, so K/F is Galois. If $\sigma \in \operatorname{Gal}(K/F)$ then $\sigma(\zeta_n) = \zeta_n^r$ for some r which is uniquely determined mod n. But ζ_n^r must also have order n in $K^\times$ since σ is an automorphism. Hence $\gcd(r, n) = 1$. Thus we have a map $\phi\colon \operatorname{Gal}(K/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ sending $\sigma \mapsto r \bmod n$. If $\sigma(\zeta_n) = \zeta_n^r$ and $\tau(\zeta_n) = \zeta_n^s$ then $\sigma\tau(\zeta_n) = \sigma(\zeta_n^s) = \sigma(\zeta_n)^s = \zeta_n^{rs}$, so $\phi(\sigma\tau) = rs = \phi(\sigma)\phi(\tau)$. Thus ϕ is a group homomorphism. It is injective since $K = F(\zeta_n)$, so if $\sigma(\zeta_n) = \zeta_n^1$ then $\sigma = 1$. Hence $\operatorname{Gal}(K/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Note that it is not always the case that $\operatorname{Gal}(K/F) = (\mathbb{Z}/n\mathbb{Z})^\times$. For example, F may already contain ζ_n in which case $K = F$ and $\operatorname{Gal}(K/F) = \{1\}$.

Assume $\operatorname{char} K = 0$ (so that $\mathbb{Q} \subseteq K$) and let $\zeta_n \in K$ be a primitive nth root of 1. Define $\Phi_n(X) = \prod_{r \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^r) \in K[X]$.

Lemma 11.2 *For $n > 0$, $X^n - 1 = \prod_{d|n} \Phi_d(X)$, where $\Phi_n(X)$ is irreducible in $\mathbb{Z}[X]$.*

Proof. Note that $\Phi_n(X) = \prod_\zeta (X - \zeta)$ where the product runs over all primitive nth roots of 1. Also $\Phi_n \in \mathbb{Q}(\zeta_n)[X]$ and for any $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $\sigma(\Phi_n) = \Phi_n$ since σ permutes the set of primitive nth roots of 1. Thus $\Phi_n \in \mathbb{Q}(\zeta_n)^{\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})}[X] = \mathbb{Q}[X]$.

For any r, ζ_n^r has order $d = n/\gcd(r, n)$, so is a primitive dth root of 1 for some $d \mid n$. Conversely any primitive dth root of 1 is of the form ζ_n^r for some r since it is a power of a fixed primitive dth root of 1, namely $\zeta_n^{n/d}$. Hence $X^n - 1 = \prod_r (X - \zeta_n^r) = \prod_{d|n} \prod_\zeta (X - \zeta)$ where the second product is over all primitive dth roots of 1. Therefore $X^n - 1 = \prod_{d|n} \Phi_d(X)$. Now by induction we can assume $\Phi_d \in \mathbb{Z}[X]$ for all $d < n$. Hence both $X^n - 1$ and $\prod_{d|n,\ d<n} \Phi_d$ are monic (and hence primitive) elements of $\mathbb{Z}[X]$, while $\Phi_n \in \mathbb{Q}[X]$. Thus by Gauss' Lemma $\Phi_n \in \mathbb{Z}[X]$.

Write $\Phi_n = fg$ where $f = m_{\zeta_n, \mathbb{Q}}$. Then by Gauss $f, g \in \mathbb{Z}[X]$. If Φ_n is not irreducible then $\deg g > 0$ and $g(\zeta_n^r) = 0$ for some $r > 1$, $\gcd(r, n) = 1$. Write r as a product of (not necessarily distinct) primes $r = p_1 \dots p_s$. By considering $\zeta_n^{p_1 \cdots p_i}$ for each $i = 0, \dots, s$ there must be some α and prime $p \nmid n$ such that $f(\alpha) = 0$ and $g(\alpha^p) = 0$. Hence $f = m_{\alpha, \mathbb{Q}}$ and $f(X) \mid g(X^p)$ in $\mathbb{Z}[X]$. Consider the reductions $\bar{f}$ and $\bar{g}$ of f and g mod p. Then $\bar{f}(X) \mid \bar{g}(X^p) = (\bar{g}(X))^p$. Then any root β of $\bar{f}$ is also a root of $\bar{g}$, so is a multiple root of

$\bar{\Phi}_n = \bar{f}\bar{g}$. Hence β is a multiple root of $X^n - 1 = \bar{\Phi}_n \dots \bar{\Phi}_1$. But then β is a root of the derivative nX^{n-1} and since $p \nmid n$ this implies $\beta = 0$ which is not a root of $X^n - 1$. Hence Φ_n is irreducible in $\mathbb{Z}[X]$. □

Corollary 11.3 *If ζ_n is a primitive nth root of 1 then* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg m_{\zeta_n,\mathbb{Q}} = \deg \Phi_n = |\{r \bmod n : \gcd(r,n) = 1\}| = |(\mathbb{Z}/n\mathbb{Z})^\times|$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \leq (\mathbb{Z}/n\mathbb{Z})^\times$, the groups must be equal. □

We now consider the equation $X^n - a = 0$ with $a \neq 1$.

Lemma 11.4 *Assume F contains a primitive nth root of 1. If K is the sfe of $X^n - a$ then* $\mathrm{Gal}(K/F)$ *is isomorphic to a subgroup of the cyclic group $\mathbb{Z}/n\mathbb{Z}$. Conversely, if K/F is a Galois extension with* $\mathrm{Gal}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$, *then $K = F(\alpha)$ for some α with $\alpha^n \in F$.*

Proof. The roots of $X^n - a$ are of the form $\{\zeta_n^i \alpha : 0 \leq i < n\}$ for some $\alpha \in K$ with $\alpha^n = a$. If $\sigma \in \mathrm{Gal}(K/F)$ then $\sigma(\alpha) = \zeta_n^i \alpha$ for some $i \in \mathbb{Z}/n\mathbb{Z}$. Since $\zeta_n \in F$, $\sigma(\zeta_n) = \zeta_n$. Thus if $\tau(\alpha) = \zeta_n^j \alpha$ then $\sigma\tau(\alpha) = \zeta_n^{i+j}\alpha$, so the map $\mathrm{Gal}(K/F) \to (\mathbb{Z}/n\mathbb{Z}, +)$ sending σ to $i \bmod n$ is a homomorphism. This map is injective since if $\sigma(\alpha) = \zeta_n^0 \alpha = \alpha$ then σ fixes F and α, so fixes $F(\alpha) = K$. Hence $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$. Conversely, assume K/F is a Galois extension with $\mathrm{Gal}(K/F) = \langle \sigma \rangle$, and σ of order n. For $\alpha \in K$ define

$$\beta = \alpha + \sigma(\alpha)\zeta_n^{-1} + \cdots + \sigma^{n-1}(\alpha)\zeta_n^{-(n-1)}$$

Then $\sigma(\beta) = \zeta_n \beta$. Hence $\sigma(\beta^n) = \beta^n$ and so $\beta^n \in K^{\mathrm{Gal}(K/F)} = F$. It remains to prove that we can choose α so that $F(\beta) = K$. If $\beta \neq 0$ then $\sigma^i(\beta) = \zeta_n^i \beta$ gives n distinct values as i varies from 0 to $n-1$. Hence $m_{\beta,F}$ has n distinct roots and $[F(\beta) : F] = \deg m_{\beta,F} \geq n = |\mathrm{Gal}(K/F)| = [K : F]$ so $F(\beta) = K$. The result now follows from the following Theorem (with $\sigma_i = \sigma^{i-1}$ and $\lambda_i = \zeta_n^{-(i-1)}$). □

Theorem (Dedekind Independence Theorem) *Suppose $\sigma_1, \dots, \sigma_n$ are distinct automorphisms of a field K. Then for any $\lambda_1, \dots, \lambda_n \in K$, not all zero, there is an $\alpha \in K$ such that $\sum_{i=1}^n \lambda_i \sigma_i(\alpha) \neq 0$.*

Proof. We shall prove the result by induction on n. For $n = 1$ the result is clear. Assume $n > 1$ and suppose $\sum \lambda_i \sigma_i(\alpha) = 0$ for all $\alpha \in K$. Since $\sigma_1 \neq \sigma_2$ there is an $\beta \in K$ with $\sigma_1(\beta) \neq \sigma_2(\beta)$. Then for all $\alpha \in K$

$$\sum \lambda_i \sigma_i(\beta)\sigma_i(\alpha) = \sum \lambda_i \sigma_i(\alpha\beta) = 0$$
$$\sum \lambda_i \sigma_1(\beta)\sigma_i(\alpha) = \sigma_1(\beta) \sum \lambda_i \sigma_i(\alpha) = 0$$

Subtracting we get $\sum_{i=2}^n \lambda_i(\sigma_i(\beta) - \sigma_1(\beta))\sigma_i(\alpha) = 0$ since the terms for $i = 1$ cancel. Hence by induction $\lambda_i(\sigma_i(\beta) - \sigma_1(\beta)) = 0$ for all i, in particular $\lambda_2(\sigma_2(\beta) - \sigma_1(\beta)) = 0$. But then $\lambda_2 = 0$. Repeating this argument for any pair (i, j) in place of $(1, 2)$ gives $\lambda_j = 0$ for all j. □

We shall assume throughout that char $F = 0$, $f \in F[X]$, and K/F is a sfe for f. Write the roots of f in K as $\alpha_1, \dots, \alpha_n$.

Quadratics

Let $f(X) = aX^2 + bX + c$. In general $\mathrm{Gal}(K/F) \cong S_2 = C_2$, and $\zeta_2 = -1 \in F$, so $K = F(\sqrt{d})$ for some $d \in F$. To find d we use the trick in Lemma 11.4. $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ where σ acts as the permutation (12) on the roots. Let $\beta = \alpha_1 + \zeta_2^{-1}\sigma(\alpha_1) = \alpha_1 - \alpha_2$. Then β^2 is fixed by S_2. Thus β^2 can be written in terms of elementary symmetric functions of the roots, and hence in terms of the coefficients of f. Indeed $\beta^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = (-b/a)^2 - 4(c/a) = (b^2 - 4ac)/a^2$. Using $\alpha_1 + \alpha_2 = -b/a$ and $\alpha_1 - \alpha_2 = \beta = \sqrt{b^2 - 4ac}/a$ we can now solve for α_1, α_2 to give the well known formula $\alpha_i = (-b \pm \sqrt{b^2 - 4ac})/2a$. It can be checked that this formula also works when $\mathrm{Gal}(K/F) < S_2$ (in which case $\sqrt{d} \in F$).

Cubics

Assume $\zeta_3 \in F$ and $\mathrm{Gal}(K/F) \cong S_3$. Then there is an intermediate field L with $\mathrm{Gal}(K/L) \cong A_3 = C_3$ and $\zeta_3 \in L$. Write

$$
\begin{aligned}
z_0 &= \alpha_1 + \alpha_2 + \alpha_3 \\
z_1 &= \alpha_1 + \zeta_3\alpha_2 + \zeta_3^2\alpha_3 \\
z_2 &= \alpha_1 + \zeta_3^2\alpha_2 + \zeta_3\alpha_3
\end{aligned}
$$

Then A_3 fixes z_1^3 and z_2^3 so $z_1^3, z_2^3 \in L$. But the transposition (23) swaps z_1^3 and z_2^3 so in general we do not expect z_1^3 or z_2^3 to lie in F. Construct a new polynomial

$$g(X) = (X - z_1^3)(X - z_2^3) = X^2 - (z_1^3 + z_2^3)X + z_1^3 z_2^3$$

This polynomial is fixed by S_3 and so we can write its coefficients in terms of the coefficients of f. Indeed, by "completing the cube" we can assume $f(X) = X^3 + pX + q$, in which case $g(X) = X^2 + 27qX - 27p^3$ and $z_0 = 0$. Solving $g(X) = 0$ then gives z_1^3, z_2^3 as roots. Since we know z_0 we can now reconstruct the roots as

$$\alpha_1 = (z_0 + z_1 + z_2)/3, \quad \alpha_2 = (z_0 + \zeta_3^2 z_1 + \zeta_3 z_2)/2, \quad \alpha_3 = (z_0 + \zeta_3 z_1 + \zeta_3^2 z_2)/2.$$

As for the quadratics, these formula work even if $\mathrm{Gal}(K/F) < S_3$.

Quartics

Assume $\zeta_3 \in F$ and $\mathrm{Gal}(K/F) \cong S_4$. By "completing the quartic" we can write f in the form $f(X) = X^4 + pX^2 + qX + r$ so that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$. There is an intermediate field L with $\mathrm{Gal}(K/L) = V$, the Klein group. Now $V \trianglelefteq S_4$ and $\mathrm{Gal}(L/F) \cong S_4/V \cong S_3$, so with some luck we can get L by splitting a cubic. Write

$$
\begin{aligned}
y_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = -(\alpha_1 + \alpha_2)^2 \\
y_2 &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) = -(\alpha_1 + \alpha_3)^2 \\
y_3 &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) = -(\alpha_1 + \alpha_4)^2
\end{aligned}
$$

Then y_i is fixed by V so $y_i \in L$. The cubic

$$g(X) = (X - y_1)(X - y_2)(X - y_3)$$

is now fixed by S_4, so the coefficients of g are polynomials in the coefficients of f. Indeed $g(X) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2$. Finding the roots y_1, y_2, y_3 as above we can recover $\alpha_i = (\pm\sqrt{-y_1} \pm \sqrt{-y_2} \pm \sqrt{-y_3})/2$ for suitable choice of signs (chosen so that the product of the square root terms is $-q$). Once again, this works even when $\mathrm{Gal}(K/F) < S_4$.

An extension K/F is a **radical** extension if $K = F(\alpha_1, \dots, \alpha_n)$ and there exists integers $n_i > 0$ such that $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ for each i.

Lemma 12.1 *If $F \subseteq L_1, L_2 \subseteq K$ and L_1/F and L_2/F are radical, then so is L_1L_2/F.*

Proof. Clear. □

Lemma 12.2 *The normal closure of a radical extension is radical.*

Proof. Let M/F be the normal closure of K/F. If K/F is radical, then $g(K)/g(F) = g(K)/F$ is radical for each $g \in \mathrm{Gal}(M/F)$. Hence the join L of all the $g(K)$ is radical over F. But if $H = \mathrm{Gal}(M/K)$ then $\mathrm{Gal}(M/L) = \bigcap gHg^{-1}$. However, this is a normal subgroup of $\mathrm{Gal}(M/F)$, so L/F is normal and $L \supseteq K$. Thus $L = M$ is radical over F. □

Theorem 12.3 *If K/F is radical and normal then* $\mathrm{Gal}(K/F)$ *is a solvable group.*

Proof. Write $K = F(\alpha_1, \dots, \alpha_r)$ with $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ and let $n = \mathrm{lcm}\{n_i\}$. Then $K(\zeta_n)/F$ is also normal (if K/F is the sfe of $\mathcal{F}$ then $K(\zeta_n)/F$ is the sfe of $\mathcal{F} \cup \{X^n - 1\}$). Also $K(\zeta_n) = F(\zeta_n, \alpha_1, \dots, \alpha_r)$ and $F(\zeta_n, \alpha_1, \dots, \alpha_i)$ is the sfe of $X^{n_i} - \alpha_i^{n_i}$ over $F(\zeta_n, \alpha_1, \dots, \alpha_{i-1})$. Hence if $H_i = \mathrm{Gal}(K(\zeta_n)/F(\zeta_n, \alpha_1, \dots, \alpha_i))$ then $H_i \trianglelefteq H_{i-1}$ and H_{i-1}/H_i is cyclic. Also $H_0 = \mathrm{Gal}(K(\zeta_n)/F(\zeta_n)) \trianglelefteq G = \mathrm{Gal}(K(\zeta_n)/F)$ and $G/H_0 \cong \mathrm{Gal}(F(\zeta_n)/F) \leq (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian. But $H_r = \{1\}$, so G is solvable. Now $\mathrm{Gal}(K/F)$ is a quotient of G, so is also solvable. □

Corollary 12.4 *There exist quintics that do not have roots in any radical extension.*

Proof. There exist quintics f over $\mathbb{Q}$ with Galois group S_5. If $K/\mathbb{Q}$ were a radical extension containing a root of f then its normal closure $M/\mathbb{Q}$ would be a radical extension containing all roots of f. But then M would contain a sfe L for f and $\mathrm{Gal}(L/\mathbb{Q})$ would be a quotient group of $\mathrm{Gal}(M/\mathbb{Q})$ which is solvable. Hence $\mathrm{Gal}(L/\mathbb{Q}) \cong S_5$ would be solvable, a contradiction. □

Theorem 12.5 *If K/F is Galois with solvable Galois group then K is contained in a radical extension of F.*

Proof. Let $n = [K : F]$. Then $\mathrm{Gal}(K(\zeta_n)/F)$ is solvable [$\mathrm{Gal}(K(\zeta_n)/K)$ is an abelian normal subgroup with solvable quotient $\mathrm{Gal}(K/F)$]. Hence $G = \mathrm{Gal}(K(\zeta_n)/F(\zeta_n))$ is solvable [$\leq \mathrm{Gal}(K(\zeta_n)/F)$]. The map $G \to \mathrm{Gal}(K/F)$ obtained by restricting $g \in G$ to K is an injective homomorphism [if g fixes K and $F(\zeta_n)$ then it clearly fixes $K(\zeta_n)$], so $|G| \mid n$. Thus there is a sequence $1 = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_r = G$ with H_i/H_{i-1} cyclic and if $L_i = K(\zeta_n)^{H_i}$ then L_{i-1}/L_i is a Galois extension with cyclic Galois group of order $n_i \mid |H_i/H_{i-1}| \mid n$, so $\zeta_{n_i} \in L_i$. Thus $L_{i-1} = L_i(\alpha_i)$ for some α_i with $\alpha_i^{n_i} \in L_i$ and $L_r = F(\zeta_n)$. Thus $L_0 = K(\zeta_n)$ is radical over F and contains K. □

Any finite Galois extension has a finite number of intermediate fields since these just correspond to subgroups of a finite group. The following lemma gives a criterion for when this happens in general.

Lemma 13.1 *Let K/F be a finite extension. Then K/F has finitely many intermediate fields L, $F \subseteq L \subseteq K$, if and only if K/F is simple, i.e., $K = F(\alpha)$ for some $\alpha \in K$.*

Proof. Assume first that $K = F(\alpha)$ is simple. Let L be an intermediate field and consider $m_{\alpha,L}$. Now $m_{\alpha,L} \mid m_{\alpha,F}$ in $L[X]$ since $m_{\alpha,F}(\alpha) = 0$. Thus $m_{\alpha,L}$ is a factor of $m_{\alpha,F}$ in $K[X]$. But if $m_{\alpha,F} = f_1 f_2 \dots f_r$ in $K[X]$ with f_i irreducible, then by unique factorization in $K[X]$, $m_{\alpha,L}$ must be some product of some of the f_i. Hence there are at most 2^r possible values for $m_{\alpha,L}$. If $m_{\alpha,L} = \sum_{i=0}^m b_i X^i$, let $M = F(b_0, \dots, b_m)$. Clearly $M \subseteq L$ so $m_{\alpha,L} \mid m_{\alpha,M}$ since $m_{\alpha,M} \in L[X]$ and $m_{\alpha,M}(\alpha) = 0$. However $m_{\alpha,L} \in M[X]$ so $m_{\alpha,M} \mid m_{\alpha,L}$. Thus $m_{\alpha,L} = m_{\alpha,M}$. Now $K = F(\alpha) \subseteq M(\alpha) \subseteq L(\alpha) \subseteq K$, and $[L(\alpha) : L] = [M(\alpha) : M] = \deg m_{\alpha,L}$, so $[K : L] = [K : M]$ and $M = L$. Since $m_{\alpha,L}$ determines $M = L$ and there are only finitely many possible $m_{\alpha,L}$s, there can be only finitely many Ls.

Now assume there are only finitely many intermediate fields. We shall first consider the case when F is infinite. Since K/F is finite, $K = F(\alpha_1, \dots, \alpha_r)$ for some $\alpha_i \in K$ (e.g., take the α_i to be a basis for K/F). We shall show that for any $\alpha, \beta \in K$, $F(\alpha, \beta) = F(\gamma)$ for some $\gamma \in K$. The result will then follow by taking r above to be minimal and noting that if $r \geq 2$ then $F(\alpha_1, \dots, \alpha_r) = F(\alpha_1, \alpha_2)(\alpha_3, \dots, \alpha_r) = F(\gamma, \alpha_3, \dots, \alpha_r)$ for some γ.

Let $\gamma = \alpha + c\beta$ for some $c \in F$. Then $F(\gamma)$ is some intermediate field. Since there are only finitely many intermediate fields and F is infinite, there exists $c_1, c_2 \in F$ $c_1 \neq c_2$ with $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$. Call this field L. Then $(c_1 - c_2)\beta = (\alpha + c_1\beta) - (\alpha + c_2\beta) \in L$. Also $c_1 - c_2 \in F \subseteq L$, so $\beta \in L$. Now $\alpha = (\alpha + c_1\beta) - c_1(\beta) \in L$, so $F(\alpha, \beta) \subseteq L$. Clearly $L \subseteq F(\alpha, \beta)$, so $F(\alpha, \beta) = F(\alpha + c_1\beta)$ as required.

If F is finite then $|K| = |F|^{[K : F]} < \infty$, so K is finite. Then $K^\times$ is cyclic, generated by α say, so $K = \{0, 1, \alpha, \alpha^2, \dots, \alpha^r\}$ and $K = F(\alpha)$. □

Theorem (The Theorem of the Primitive Element) *If K/F is finite and separable then $K = F(\alpha)$ for some $\alpha \in K$.*

Proof. Let M be the normal closure of K/F, so M/F is finite and Galois. By the fundamental theorem of Galois theory, there are only finitely many fields L with $F \subseteq L \subseteq M$. Hence there are only finitely many fields with $F \subseteq L \subseteq K$. Hence K/F is simple by Lemma 1. □

Example: Let $K = \mathbb{F}_p(x, y)$ where x, y are algebraically independent (in particular y is transcendental over $\mathbb{F}_p(x)$ and x is transcendental over $\mathbb{F}_p$). Let $F = \mathbb{F}_p(x^p, y^p) \subseteq K$. Then $\{x^i y^j : 0 \leq i, j < p\}$ is a basis of K/F so any $\gamma \in K$ is of the form $\sum a_{ij} x^i y^j$ with $a_{ij} \in F$. Now $\gamma^p = \sum a_{ij}^p x^{pi} y^{pj} \in F$, so $[F(\gamma) : F] \leq p$. But $[K : F] = p^2$, so K/F is not simple and has an infinite number of intermediate fields.

7262 14. Norm and Trace Spring 2018

Assume K/F is a finite extension with $[K:F] = n$. Then K can be regarded as an n-dimensional F-vector space. If $\alpha \in K$ then the map $t_\alpha : K \to K$ which sends β to $\alpha\beta$ is an F-linear map from the F-vector space K to itself, and as such can be represented by an $n \times n$ matrix with coefficients in F.

The **norm** of an element $\alpha \in K$ is the determinant $\mathrm{N}_{K/F}(\alpha) = \det t_\alpha$ and the **trace** of α is the trace $\mathrm{Tr}_{K/F}(\alpha) = \mathrm{tr}\, t_\alpha$ of the matrix representing t_α. Note that both these quantities are independent of the basis for K/F.

Theorem 14.1

(a) $\mathrm{N}_{K/F}(\alpha\beta) = \mathrm{N}_{K/F}(\alpha)\,\mathrm{N}_{K/F}(\beta)$ *and* $\mathrm{Tr}_{K/F}(\alpha+\beta) = \mathrm{Tr}_{K/F}(\alpha) + \mathrm{Tr}_{K/F}(\beta)$.

(b) If $K/L/F$ *and* $\alpha \in L$ *then* $\mathrm{N}_{K/F}(\alpha) = \mathrm{N}_{L/F}(\alpha)^{[K:L]}$ *and* $\mathrm{Tr}_{K/F}(\alpha) = [K:L]\,\mathrm{Tr}_{L/F}(\alpha)$.

(c) If $m_{\alpha,F} = X^n + a_{n-1}X^{n-1} + \dots + a_0$ *then* $\mathrm{N}_{F(\alpha)/F}(\alpha) = (-1)^n a_0$ *and* $\mathrm{Tr}_{F(\alpha)/F}(\alpha) = -a_{n-1}$.

(d) If K/F *is Galois,* $\mathrm{N}_{K/F}(\alpha) = \prod_{g\in\mathrm{Gal}(K/F)} g(\alpha)$ *and* $\mathrm{Tr}_{K/F}(\alpha) = \sum_{g\in\mathrm{Gal}(K/F)} g(\alpha)$.

Proof.
(a) Follows from standard properties of det and tr using $t_{\alpha\beta} = t_\alpha \circ t_\beta$ and $t_{\alpha+\beta} = t_\alpha + t_\beta$.
(b) Let $\{\alpha_i\}$ be a basis for L/F and $\{\beta_j\}$ be a basis for K/L. Then by the tower law $\{\alpha_i\beta_j\}$ is a basis for K/F. In this basis, $t_\alpha(K/F)$ is represented as a matrix with blocks corresponding to $t_\alpha(L/F)$ down the diagonal and zeros elsewhere. Thus $\det t_\alpha(K/F) = (\det t_\alpha(L/F))^r$ and $\mathrm{tr}\, t_\alpha(K/F) = r\,\mathrm{tr}\, t_\alpha(L/F)$ where $r = [K:L]$ is the number of blocks.
(c) Use a basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ for $F(\alpha)/F$. Then the matrix t_α will be of the form

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$$

(d) $\mathrm{N}_{K/F}(\alpha) = \mathrm{N}_{F(\alpha)/F}(\alpha)^r = (\pm a_0)^r = \prod \alpha_i^r$ where $r = [K:F(\alpha)]$, and $\alpha = \alpha_1, \alpha_2, \dots$ are the roots of $m_{\alpha,F}$. Let $G = \mathrm{Gal}(K/F)$ and let $H = \mathrm{Gal}(K/F(\alpha))$. For each i there exists a $g \in G$ with $g(\alpha) = \alpha_i$. Moreover if $g'(\alpha) = \alpha_i$ then $g^{-1}g'$ fixes α, so $g^{-1}g' \in H$ and $g' \in gH$. Conversely if $g' \in gH$ then $g'(\alpha) = g(\alpha) = \alpha_i$. Hence

$$\prod_{g\in G} g(\alpha) = \prod_{gH\in G/H}\prod_{g'\in gH} g'(\alpha) = \prod_{gH\in G/H} \alpha_i^{|H|} = \prod \alpha_i^r = \mathrm{N}_{K/F}(\alpha).$$

A similar argument works for Tr. □

Exercises

1. Show that if $K/L/F$ and both K/F and L/F are Galois then $\mathrm{N}_{K/F}(\alpha) = \mathrm{N}_{L/F}\,\mathrm{N}_{K/L}(\alpha)$ and $\mathrm{Tr}_{K/F}(\alpha) = \mathrm{Tr}_{L/F}\,\mathrm{Tr}_{K/L}(\alpha)$. [In fact this is true for any finite $K/L/F$.]
2. Describe the functions $\mathrm{N}_{\mathbb{C}/\mathbb{R}}$ and $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}$ explicitly.