Fields and Galois Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Monomorphisms between Fields

The Vector Space $\mathscr{M}$

- Let K be a field and let S be a non-empty set.
- Let $\mathscr{M}$ be the set of mappings from S into K.
- If $\theta, \varphi \in \mathscr{M}$, then $\theta + \varphi$, defined by
$$(\theta + \varphi)(s) = \theta(s) + \varphi(s), \quad s \in S,$$
is a mapping from S into K, and so belongs to $\mathscr{M}$.
- If $\theta \in \mathscr{M}$ and $a \in K$, then $a\theta$, defined by
$$(a\theta)(s) = a\theta(s), \quad s \in S,$$
belongs to $\mathscr{M}$.
- $\mathscr{M}$ is a vector space with respect to these two operations.
- The zero vector in $\mathscr{M}$ is the mapping ζ given by
$$\zeta(s) = 0, \quad s \in S.$$
- We denote the mapping ζ simply by 0, since the context makes it clear whether we mean the zero element of K or the mapping ζ.

Linear Independence in $\mathscr{M}$

- A set $\{\theta_1,\theta_2,\ldots,\theta_n\}$ of elements of $\mathscr{M}$ is **linearly independent** if, for all $a_1,a_2,\ldots,a_n$ in K,

$$a_1\theta_1(s)+a_2\theta_2(s)+\cdots+a_n\theta_n(s)=0,$$

  for all s in S, if and only if $a_1=a_2=\cdots=a_n=0$.
- More compactly, we can write the condition as

$$a_1\theta_1+a_2\theta_2+\cdots+a_n\theta_n=0 \text{ (strictly, } \zeta\text{) iff } a_1=a_2=\cdots=a_n=0.$$

Linear Independence of Field Monomorphisms

Theorem

Let K and L be fields, and let $\theta_1, \theta_2, \ldots, \theta_n$ be distinct monomorphisms from K into L. Then $\{\theta_1, \theta_2, \ldots, \theta_n\}$ is a linearly independent set in the vector space $\mathscr{M}$ of all mappings from K into L.

- We prove the theorem by induction on n.

  For $n = 1$: By hypothesis, θ_1 is a monomorphism. Thus, it maps the identity 1 of K to the identity 1 of L. So it is not the zero mapping.

  Assume that we have established that every set of fewer than n distinct monomorphisms of K into L is linearly independent.

  Suppose, for a contradiction, that there exist $a_1, a_2, \ldots, a_n$ in L, not all zero, such that $a_1\theta_1 + a_2\theta_2 + \cdots + a_n\theta_n = 0$. We may assume that all a_i are non-zero: If, e.g., $a_n = 0$, then $\{\theta_1, \theta_2, \ldots, \theta_{n-1}\}$ is linearly dependent, contradicting the induction hypothesis.

Linear Independence of Field Monomorphisms (Cont'd)

- Dividing by a_n, gives
$$b_1\theta_1+\cdots+b_{n-1}\theta_{n-1}+\theta_n=0,$$
where $b_i=\frac{a_i}{a_n}$ $(i=1,2,\ldots,n-1)$. The monomorphisms θ_1 and θ_n are by assumption distinct. So there exists u in K, with $\theta_1(u)\neq\theta_n(u)$. The element u is certainly non-zero, as are both $\theta_1(u)$ and $\theta_n(u)$.
For every z in K, $b_1\theta_1(uz)+\cdots+b_{n-1}\theta_{n-1}(uz)+\theta_n(uz)=0$.
But $\theta_1,\theta_2,\ldots,\theta_n$ are monomorphisms.
So $b_1\theta_1(u)\theta_1(z)+\cdots+b_{n-1}\theta_{n-1}(u)\theta_{n-1}(z)+\theta_n(u)\theta_n(z)=0$.
Dividing this by $\theta_n(u)$, we get, for all z in K,
$$b_1\frac{\theta_1(u)}{\theta_n(u)}\theta_1(z)+\cdots+b_{n-1}\frac{\theta_{n-1}(u)}{\theta_n(u)}\theta_{n-1}(z)+\theta_n(z)=0.$$
Rewriting as an equation concerning mappings gives
$$b_1\frac{\theta_1(u)}{\theta_n(u)}\theta_1+\cdots+b_{n-1}\frac{\theta_{n-1}(u)}{\theta_n(u)}\theta_{n-1}+\theta_n=0.$$

Linear Independence of Field Monomorphisms (Conclusion)

- Subtracting the bottom from he top equation, we obtain

$$b_1\left(1-\frac{\theta_1(u)}{\theta_n(u)}\right)\theta_1+\cdots+b_{n-1}\left(1-\frac{\theta_{n-1}(u)}{\theta_n(u)}\right)\theta_{n-1}=0.$$

  Our choice of u as an element such that $\theta_1(u)\neq\theta_n(u)$ means that the coefficient of θ_1 is non-zero. Thus, the set $\{\theta_1,\theta_2,\ldots,\theta_{n-1}\}$ is linearly dependent. This contradicts the induction hypothesis.

- The set of monomorphisms from K into L is not a subspace of the vector space $\mathscr{M}$.

  Suppose θ_1 and θ_2 are monomorphisms.

  Let 1_K and 1_L be the identities of K and L.

$$(\theta_1+\theta_2)(1_K)=\theta_1(1_K)+\theta_2(1_K)=1_L+1_L\neq 1_L.$$

  So $\theta_1+\theta_2$ is not a monomorphism.

Subsection 2

Automorphisms, Groups and Subfields

The Group of Automorphisms of a Field

Theorem

Let K be a field. Then the set $\text{Aut}K$ of automorphisms of K forms a group under composition of mappings.

- Composition of mappings is always associative. For all x in K and all α, β and γ in $\text{Aut}K$,

$$[(\alpha\circ\beta)\circ\gamma](x)=(\alpha\circ\beta)[\gamma(x)]=\alpha(\beta(\gamma(x)));$$
$$[\alpha\circ(\beta\circ\gamma)](x)=\alpha([\beta\circ\gamma](x))=\alpha(\beta(\gamma(x))).$$

  There exists an identity automorphism ι in $\text{Aut}K$, defined by the property that $\iota(x)=x$, for all x in K.

  Clearly $\iota\circ\alpha=\alpha\circ\iota=\alpha$, for all α in $\text{Aut}K$.

The Group of Automorphisms of a Field (Cont'd)

- Finally, for every automorphism α in $\mathrm{Aut}K$, there is an inverse mapping α^{-1} defined by the property that

$$\alpha^{-1}(x) \text{ is the unique } z \text{ in } K \text{ such that } \alpha(z) = x.$$

  This map is also an automorphism.

  Let $x, y \in K$, and let $\alpha^{-1}(x) = z$, $\alpha^{-1}(y) = t$. Then $\alpha(z) = x$, $\alpha(t) = y$. So $\alpha(z+t) = x+y$ and $\alpha(zt) = xy$. Hence,

$$\begin{array}{rcl} \alpha^{-1}(x) + \alpha^{-1}(y) & = & z + t = \alpha^{-1}(\alpha(z+t)) = \alpha^{-1}(x+y); \\ \alpha^{-1}(x)\alpha^{-1}(y) & = & zt = \alpha^{-1}(\alpha(zt)) = \alpha^{-1}(xy). \end{array}$$

  Thus, $\alpha^{-1} \in G$. Clearly, $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = \iota$.

  Hence G is a group.
- $\mathrm{Aut}K$ is called the **group of automorphisms** of K.

The Galois Group of an Extension

- Let L be an extension of a field K.
- An automorphism α of L is called a K-**automorphism** if $\alpha(x) = x$, for every x in K.
- The set of all K-automorphisms of L is denoted by $\mathrm{Gal}(L:K)$ and is called the **Galois group of L over K**.
- The **Galois group** $\mathrm{Gal}(f)$ **of a polynomial** f in $K[X]$ is defined as $\mathrm{Gal}(L:K)$, where L is a splitting field of f over K.

The Galois Group in the Automorphisms of the Extension

- Let L be an extension of a field K.
  - We have seen that $\mathrm{Aut}L$ is a group.
  - We show that $\mathrm{Gal}(L:K)$ is a subgroup of $\mathrm{Aut}L$.

Theorem

Let $L:K$ be a field extension. The set $\mathrm{Gal}(L:K)$ of all K-automorphisms of L is a subgroup of $\mathrm{Aut}L$.

- Certainly $\iota \in \mathrm{Gal}(L:K)$.

  Let $\alpha, \beta \in \mathrm{Gal}(L:K)$. Then, for all x in K,

$$\begin{array}{rcl} \beta^{-1}(x) & = & \beta^{-1}(\beta(x)) = x; \\ \alpha(\beta(x)) & = & \alpha(x) = x. \end{array}$$

  Thus, $\mathrm{Gal}(L:K)$ is a subgroup of $\mathrm{Aut}L$.

The Maps Γ and Φ

- We now connect the following objects:
  - The subfields E of L containing K;
  - The subgroups H of the group $\mathrm{Gal}(L:K)$.
- For every subfield E of L containing K, we define

$$\Gamma(E) = \{\alpha \in \mathrm{Aut} L : \alpha(z) = z, \text{ for all } z \text{ in } E\}.$$

- For every subgroup H of $\mathrm{Gal}(L:K)$, we define

$$\Phi(H) = \{x \in L : \alpha(x) = x, \text{ for all } \alpha \text{ in } H\}.$$

- We establish conditions on the extension $L:K$ under which Γ and Φ are mutually inverse.

Γ and Φ are Well-Defined

Theorem

Let $L:K$ be a field extension.

(i) For every subfield E of L containing K, the set $\Gamma(E)$ is a subgroup of $\mathrm{Gal}(L:K)$.

(ii) For every subgroup H of $\mathrm{Gal}(L:K)$, the set $\Phi(H)$ is a subfield of L, containing K.

(i) Certainly $\Gamma(E)$ is non-empty, since it contains ι, the identity automorphism. Since $K \subseteq E$, every automorphism fixing all elements of E automatically fixes all elements of K. Hence, $\Gamma(E) \subseteq \mathrm{Gal}(L:K)$. Let $\alpha, \beta \in \Gamma(E)$. Then, for all z in E,

$$\alpha(\beta^{-1}(z)) = \alpha(\beta^{-1}(\beta(z))) = \alpha(z) = z.$$

So $\alpha\beta^{-1} \in \Gamma(E)$. Hence, $\Gamma(E)$ is a subgroup.

Γ and Φ are Well-Defined

(ii) Every automorphism in $\mathrm{Gal}(L:K)$ fixes the elements of K.

Hence, $K \subseteq \Phi(H)$.

Let $x, y \in \Phi(H)$. Then, for all α in H,

$$\alpha(x-y) = \alpha(x) - \alpha(y) = x - y.$$

So $x - y \in \Phi(H)$.

If $y \neq 0$, then, for all α in H,

$$\alpha(xy^{-1}) = \alpha(x)\alpha(y^{-1}) = \alpha(x)(\alpha(y))^{-1} = xy^{-1}.$$

So $xy^{-1} \in \Phi(H)$.

Thus, $\Phi(H)$ is a subfield of L.

Γ and Φ are Order-Reversing

Theorem

Let $L:K$ be a field extension.

(i) If E_1 and E_2 are subfields of L containing K, then
$$E_1 \subseteq E_2 \quad \text{implies} \quad \Gamma(E_1) \supseteq \Gamma(E_2).$$

(ii) If H_1 and H_2 are subgroups of $\mathrm{Gal}(L:K)$, then
$$H_1 \subseteq H_2 \quad \text{implies} \quad \Phi(H_1) \supseteq \Phi(H_2).$$

(i) Suppose that $E_1 \subseteq E_2$, and let $\alpha \in \Gamma(E_2)$. Then α fixes every element of E_2. So it fixes every element of E_1. Hence, $\alpha \in \Gamma(E_1)$.

(ii) Suppose that $H_1 \subseteq H_2$, and let $z \in \Phi(H_2)$. Then $\alpha(z) = z$, for every α in H_2. So, $\alpha(z) = z$, for every α in H_1. Hence $z \in \Phi(H_1)$.

Γ and Φ May Not Be Inverse Mappings

- Consider the extension $\mathbb{Q}(u)$ of $\mathbb{Q}$, where $u = \sqrt[3]{2}$.
  Suppose $\alpha \in \mathrm{Gal}(\mathbb{Q}(u) : \mathbb{Q})$.
  Then
  $$(\alpha(u))^3 = \alpha(u^3) = \alpha(2) = 2.$$
  So, being real, $\alpha(u)$ must be equal to u.
  Hence, $\mathrm{Gal}(\mathbb{Q}(u) : \mathbb{Q})$ is the trivial group $\{\iota\}$.
  Two mappings are mutually inverse only if they are both bijections.
  Here, however, we have
  $$\Gamma(\mathbb{Q}(u)) = \Gamma(\mathbb{Q}) = \{\iota\}.$$
  To look at it another way, we have
  $$\Phi(\Gamma(\mathbb{Q})) = \Phi(\{\iota\}) = \mathbb{Q}(u).$$

Γ and Φ May Be Inverse Mappings

- We describe the group $\mathrm{Gal}(\mathbb{C}:\mathbb{R})$.
  If $\alpha \in \mathrm{Gal}(\mathbb{C}:\mathbb{R})$, then $\alpha(x) = x$, for all x in R. Let $\alpha(i) = j$. Then $j^2 = (\alpha(i))^2 = \alpha(i^2) = \alpha(-1) = -1$. So $j = \pm i$.
  - Suppose $j = i$. For all $x + yi$ in $\mathbb{C}$ (with x, y in $\mathbb{R}$), $\alpha(x+yi) = \alpha(x) + \alpha(y)\alpha(i) = x + yi$. So $\alpha = \iota$.
  - Suppose $j = -i$. Then $\alpha(x+yi) = x - yi$. This mapping fixes the elements of $\mathbb{R}$. We check that it is an automorphism.
  $$\begin{aligned} &\alpha((x+yi)+(u+vi)) = \alpha((x+u)+(y+v)i) = (x+u)-(y+v)i \\ &= (x-yi)+(u-vi) = \alpha(x+yi)+\alpha(u+vi); \\ &\alpha((x+yi)(u+vi)) = \alpha((xu-yv)+(xv+yu)i) = (xu-yv)-(xv+yu)i \\ &= (x-yi)(u-vi) = (\alpha(x+yi))(\alpha(u+vi)). \end{aligned}$$

  We deduce that $\mathrm{Gal}(\mathbb{C}:\mathbb{R})$ is the group $\{\iota, \kappa\}$ of order 2, where κ is the complex conjugation mapping sending $x + yi$ to $x - yi$.

  Moreover, $[\mathbb{C}:\mathbb{R}] = 2$, a prime number.

  So there cannot be any subfields of $\mathbb{C}$ lying between $\mathbb{C}$ and $\mathbb{R}$.

  We conclude that $\Phi(\{\iota\}) = \mathbb{C}$ and $\Phi(\{\iota, \kappa\}) = \mathbb{R}$.

Galois Group and Roots of Polynomials

Theorem

Let K be a field, let L be an extension of K, and let $z \in L \backslash K$. If z is a root of a polynomial f with coefficients in K, and if $\alpha \in \mathrm{Gal}(L:K)$, then $\alpha(z)$ is also a root of f.

- Let $f = a_0 + a_1 X + \cdots + a_n X^n$, where $a_0, a_1, \ldots, a_n \in K$.

  Suppose that $f(z) = 0$. Then

$$\begin{array}{rcl} f(\alpha(z)) & = & a_0 + a_1\alpha(z) + \cdots + a_n(\alpha(z))^n \\ & = & \alpha(a_0) + \alpha(a_1)\alpha(z) + \cdots + \alpha(a_n)\alpha(z^n) \\ & = & \alpha(a_0 + a_1 z + \cdots + a_n z^n) \\ & = & \alpha(0) \\ & = & 0. \end{array}$$

Example

- We describe the group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q})$ and, for each of its subgroups H, we determine $\Phi(H)$.

  The elements of $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$ are of the form $a + b\sqrt{2} + ci\sqrt{3} + di\sqrt{6}$. By the theorem, if $\alpha \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q})$, then $\alpha(\sqrt{2}) = \pm\sqrt{2}$, $\alpha(i\sqrt{3}) = \pm i\sqrt{3}$. There are four elements in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q})$, namely, ι, τ, θ and β, where ι is the identity map, and:
  - $\tau(a + b\sqrt{2} + ci\sqrt{3} + di\sqrt{6}) = a - b\sqrt{2} + ci\sqrt{3} - di\sqrt{6}$;
  - $\theta(a + b\sqrt{2} + ci\sqrt{3} + di\sqrt{6}) = a + b\sqrt{2} - ci\sqrt{3} - di\sqrt{6}$;
  - $\beta(a + b\sqrt{2} + ci\sqrt{3} + di\sqrt{6}) = a - b\sqrt{2} - ci\sqrt{3} + di\sqrt{6}$.

  All four are $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$. The multiplication table is on the right.

	ι	τ	θ	β
ι	ι	τ	θ	β
τ	τ	ι	β	θ
θ	θ	β	ι	τ
β	β	θ	τ	ι

  The proper subgroups of this group are $H_1 = \{\iota, \tau\}$, $H_2 = \{\iota, \theta\}$ and $H_3 = \{\iota, \beta\}$.

  We have $\Phi(H_1) = \mathbb{Q}(i\sqrt{3})$, $\Phi(H_2) = \mathbb{Q}(\sqrt{2})$, $\Phi(H_3) = \mathbb{Q}(i\sqrt{6})$.

Inflationarity of $\Phi\Gamma$ and $\Gamma\Phi$

- The pair Φ and Γ, known as the **Galois correspondence**, need not be mutually inverse, but they do have a weaker property.

Theorem

Let L be an extension of a field K, let E be a subfield of L containing K, and let H be a subgroup of $\mathrm{Gal}(L:K)$. Then

$$E \subseteq \Phi(\Gamma(E)), \qquad H \subseteq \Gamma(\Phi(H)).$$

- Let $z \in E$. The group $\Gamma(E)$ is the set of all automorphisms fixing each element of E. So z is fixed by all the automorphisms in $\Gamma(E)$. That is, $z \in \Phi(\Gamma(E))$. Hence, $E \subseteq \Phi(\Gamma(E))$.

  Let $\alpha \in H$. The field $\Phi(H)$ is the set of elements of L fixed by every element of H. So α fixes every element of $\Phi(H)$. That is, $\alpha \in \Gamma(\Phi(H))$. Hence, $H \subseteq \Gamma(\Phi(H))$.

Linear Algebraic Deviation: Rank and Nullity

- Let V and W be finite-dimensional vector spaces over a field K, with dimensions m, n, respectively, and let $T : V \to W$ be a linear mapping.
- The **image** $\operatorname{im} T$ of T is the set $\{T(v) : v \in V\}$.

  The image $\operatorname{im} T$ is a subspace of W.

  Its dimension $\dim(\operatorname{im} T)$ is called the **rank** $\rho(T)$ of T.
- The **kernel** $\ker T$ of T is the set $\{v \in V : T(v) = 0\}$.

  The kernel $\ker T$ is a subspace of V.

  Its dimension $\dim(\ker T)$ is called the **nullity** $\nu(T)$ of T.
- A standard result in linear algebra states that

$$\rho(T) + \nu(T) = \dim V = m.$$

Linear Algebraic Deviation: Translation into Matrices

- We know $\rho(T) + \nu(T) = \dim V = m$.

  So, if $n < m$, then certainly $\rho(T) \leq n < m$. So $\nu(T) > 0$.

  Thus, there exists a non-zero vector v in V, such that $T(v) = 0$.

- If we have an $n \times m$ matrix $A = [a_{ij}]_{n \times m}$, with entries in K, and an m-dimensional column vector v, the map $v \mapsto Av$ is a linear mapping from the vector space K^m into the vector space K^n.

  So if $n < m$, then there exists a non-zero vector v such that $Av = 0$.

  That is, there exist $v_1, v_2, \ldots, v_m$ in K, not all zero, such that

$$a_{1j}v_1 + a_{2j}v_2 + \cdots + a_{mj}v_m = 0, \quad j = 1, 2, \ldots, n.$$

Degree of Extension and Order of a Group

Theorem

Let L be a finite extension of a field K, and let G be a finite subgroup of $\mathrm{Gal}(L:K)$. Then $[L:\Phi(G)]=|G|$.

- Let $|G|=m$ and $[L:\Phi(G)]=n$.
  We show $m>n$ leads to a contradiction.
  Write $G=\{\alpha_1=\iota,\alpha_2,\ldots,\alpha_m\}$, where ι is the identity map.
  Suppose that $\{z_1,z_2,\ldots,z_n\}$ is a basis for L over $\Phi(G)$.
  Consider the $n\times m$ matrix $\begin{bmatrix} \alpha_1(z_1) & \alpha_2(z_1) & \cdots & \alpha_m(z_1) \\ \alpha_1(z_2) & \alpha_2(z_2) & \cdots & \alpha_m(z_2) \\ \vdots & \vdots & & \vdots \\ \alpha_1(z_n) & \alpha_2(z_n) & \cdots & \alpha_m(z_n) \end{bmatrix}$.
  Since $m>n$, there exist $v_1,v_2,\ldots,v_m$ in L, not all zero, such that
  $$\alpha_1(z_j)v_1+\alpha_2(z_j)v_2+\cdots+\alpha_m(z_j)v_m=0,\quad j=1,2,\ldots,n.$$

Degree of Extension $\not<$ Order of a Group

- Let $b \in L$. The set $\{z_1, z_2, \ldots, z_n\}$ is a basis for L over $\Phi(G)$. So there exist $b_1, b_2, \ldots, b_n$ in $\Phi(G)$ such that $b = b_1 z_1 + b_2 z_2 + \cdots + b_n z_n$. Multiplying the n preceding equations by $b_1, b_2, \ldots, b_n$, respectively,

$$b_j \alpha_1(z_j) v_1 + b_j \alpha_2(z_j) v_2 + \cdots + b_j \alpha_m(z_j) v_m = 0, \quad j = 1, 2, \ldots, n.$$

The b_j all lie in $\Phi(G)$. The α_i all lie in G. So $b_j = \alpha_i(b_j)$ for all i, j. Thus, we may rewrite the equations as

$$\alpha_1(b_j z_j) v_1 + \alpha_2(b_j z_j) v_2 + \cdots + \alpha_m(b_j z_j) v_m = 0, \; j = 1, 2, \ldots, n.$$

If we add these n equations together, we obtain

$$v_1 \alpha_1(b) + v_2 \alpha_2(b) + \cdots + v_m \alpha_m(b) = 0.$$

This holds for all b in L. So the automorphisms $\alpha_1, \alpha_2, \ldots, \alpha_m$ are linearly dependent. This is impossible.

Degree of Extension $\not>$ Order of a Group

- Suppose that $n = [L : \Phi(G)] > m$. Take a subset $\{z_1, z_2, \ldots, z_{m+1}\}$ of L which is linearly independent over $\Phi(G)$. Consider the $m \times (m+1)$ matrix $\left[\begin{array}{cccc} \alpha_1(z_1) & \alpha_1(z_2) & \cdots & \alpha_1(z_{m+1}) \\ \alpha_2(z_1) & \alpha_2(z_2) & \cdots & \alpha_2(z_{m+1}) \\ \vdots & \vdots & & \vdots \\ \alpha_m(z_1) & \alpha_m(z_2) & \cdots & \alpha_m(z_{m+1}) \end{array}\right]$.

  There exist $u_1, u_2, \ldots, u_{m+1}$ in L, not all zero, such that

  $$\alpha_j(z_1)u_1 + \alpha_j(z_2)u_2 + \cdots + \alpha_j(z_{m+1})u_{m+1} = 0, \quad j = 1, 2, \ldots, m.$$

  Suppose that the elements $u_1, u_2, \ldots, u_{m+1}$ are chosen so that *as few as possible are non-zero*. Relabel the elements so that $u_1, u_2, \ldots, u_r$ are non-zero, and $u_{r+1} = \cdots = u_{m+1} = 0$.

  So now we have

  $$\alpha_j(z_1)u_1 + \alpha_j(z_2)u_2 + \cdots + \alpha_j(z_r)u_r = 0, \; j = 1, 2, \ldots, m.$$

Degree of Extension $\not>$ Order of a Group (Cont'd)

- We have $\alpha_j(z_1)u_1 + \alpha_j(z_2)u_2 + \cdots + \alpha_j(z_r)u_r = 0$, $j = 1, 2, \ldots, m$.
  Dividing by u_r and setting $u'_i = \frac{u_i}{u_r}$, $i = 1, 2, \ldots, r-1$, we get
  $$\alpha_j(z_1)u'_1 + \cdots + \alpha_j(z_{r-1})u'_{r-1} + \alpha_j(z_r) = 0,\ j = 1, 2, \ldots, m.$$
  Since $\alpha_1 = \iota$, the first of these equations is
  $$z_1 u'_1 + \cdots + z_{r-1}u'_{r-1} + z_r = 0.$$
  The set $\{z_1, z_2, \ldots, z_r\}$ is not linearly dependent over $\Phi(G)$.
  So not all of the elements $u'_1, \ldots, u'_{r-1}$ belong to $\Phi(G)$.
  As at least one of $u'_1, \ldots, u'_{r-1}$ is not in $\Phi(G)$, assume $u'_1 \notin \Phi(G)$.
  That is, u'_1 is not fixed by every automorphism in G.
  So there is an automorphism in G, say α_2, such that $\alpha_2(u'_1) \neq u'_1$.
  Applying α_2 to the preceding equations, for $j = 1, 2, \ldots, m$,
  $$(\alpha_2\alpha_j)(z_1)\alpha_2(u'_1) + \cdots + (\alpha_2\alpha_j)(z_{r-1})\alpha_2(u'_{r-1}) + (\alpha_2\alpha_j)(z_r) = 0.$$

Degree of Extension $\ngtr$ Order of a Group (Cont'd)

- We obtained

$$(\alpha_2\alpha_j)(z_1)\alpha_2(u_1') + \cdots + (\alpha_2\alpha_j)(z_{r-1})\alpha_2(u_{r-1}') + (\alpha_2\alpha_j)(z_r) = 0.$$

  G is a group.

  So the set $\{\alpha_2\alpha_1, \alpha_2\alpha_2, \ldots, \alpha_2\alpha_m\}$ is the same as the set $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ except for the order of the elements.

  Hence, we may change the order of the listed equations and obtain

$$\alpha_j(z_1)\alpha_2(u_1') + \cdots + \alpha_j(z_{r-1})\alpha_2(u_{r-1}') + \alpha_j(z_r) = 0, \quad j = 1, 2, \ldots, m.$$

  Subtracting these from the original gives, for $j = 1, 2, ..., m$,

$$\alpha_j(z_1)(u_1' - \alpha_2(u_1')) + \cdots + \alpha_j(z_{r-1})(u_{r-1}' - \alpha_2(u_{r-1}')) = 0.$$

Degree of Extension $\not>$ Order of a Group (Conclusion)

- We obtained

$$\alpha_j(z_1)(u_1' - \alpha_2(u_1')) + \cdots + \alpha_j(z_{r-1})(u_{r-1}' - \alpha_2(u_{r-1}')) = 0.$$

Let $v_i = u_i' - \alpha_2(u_i')$, $i = 1, 2, \ldots, r-1$, and $v_i = 0$, $i = r, r+1, \ldots, m+1$. Then

$$\alpha_j(z_1)v_1 + \alpha_j(z_2)v_2 + \cdots + \alpha_j(z_{m+1})v_{m+1} = 0, \quad j = 1, 2, \ldots, m.$$

We know that the elements v_i are not all zero.

In this arrangement, no more than $r-1$ of the v_i are non-zero.

This contradicts the minimality of r in the choice of the elements $u_1, u_2, \ldots, u_{m+1}$.

We conclude that it is not possible to have $[L : \Phi(G)] > m$.

Subsection 3

Normal Extensions

Normal Extensions

- We considered the two extensions of $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$.
  - In the first case X^2-2, the minimum polynomial of $\sqrt{2}$, splits completely over $\mathbb{Q}(\sqrt{2})$.
  - In the second case we see that X^3-2, the minimum polynomial of $\sqrt[3]{2}$, does not split completely over $\mathbb{Q}(\sqrt[3]{2})$.

  This is an important difference.
- Although it is convenient to consider arbitrary extensions $L:K$, our primary interest is with Galois groups of polynomials, when L is a splitting field over K for some polynomial.
- We call $L:K$ a **normal extension** if every irreducible polynomial in $K[X]$ having at least one root in L splits completely over L.

Characterization of Normality

Theorem

A finite extension L of a field K is normal if and only if it is a splitting field for some polynomial in $K[X]$.

- Suppose that L is a finite normal extension.

  Let $\{z_1, z_2, \ldots, z_n\}$ be a basis for L over K.

  For $i = 1, 2, \ldots, n$, let m_i be the minimum polynomial of z_i, and let $m = m_1 m_2 \cdots m_n$.

  - Each m_i has at least one root z_i in L. So, by hypothesis, it splits completely over L. Hence, m splits completely over L.
  - But L is generated by $z_1, z_2, \ldots, z_n$. So it is not possible for m to split completely over any proper subfield of L.

  Thus, L is a splitting field for m over K.

Characterization of Normality (Converse)

- Suppose that E is a splitting field for some polynomial g over K.

  Let f, with degree at least 2, be an irreducible polynomial in $K[X]$, having a root α in E. We must show that f splits completely over E.

  The polynomial fg certainly lies in $E[X]$. It has a splitting field L containing E. Suppose that β is another root of f in L. We have subfields of L as indicated in the diagram, in which the arrows denote inclusion. We have

$$\begin{tikzcd}
& L & \\
E(\alpha) \arrow[ur] & & E(\beta) \arrow[ul] \\
& E \arrow[uu] \arrow[ul] \arrow[ur] & \\
K(\alpha) \arrow[uu] & & K(\beta) \arrow[uu] \\
& K \arrow[uu] \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

$$[E(\alpha):E][E:K]=[E(\alpha):K]=[E(\alpha):K(\alpha)][K(\alpha):K];$$
$$[E(\beta):E][E:K]=[E(\beta):K]=[E(\beta):K(\beta)][K(\beta):K].$$

  But α and β are roots of the same irreducible polynomial f.

  So there is a K-isomorphism φ from $K(\alpha)$ onto $K(\beta)$.

  Certainly $[K(\alpha):K]=[K(\beta):K]$.

Characterization of Normality (Converse Cont'd)

- E is a splitting field for g over K.

  So $E(\alpha)$ is a splitting field for g over $K(\alpha)$

  and $E(\beta)$ is a splitting field for g over $K(\beta)$.

  Hence, there is an isomorphism φ^* from $E(\alpha)$ onto $E(\beta)$, extending the K-isomorphism φ from $K(\alpha)$ onto $K(\beta)$. It follows in particular that $[E(\alpha):K(\alpha)]=[E(\beta):K(\beta)]$.

$$\begin{tikzcd}
 & L & \\
E(\alpha) \arrow[ur] & & E(\beta) \arrow[ul] \\
 & E \arrow[uu] \arrow[ul] \arrow[ur] & \\
K(\alpha) \arrow[uu] & & K(\beta) \arrow[uu] \\
 & K \arrow[uu] \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

  Now $[E(\alpha):E]=1$, since $\alpha \in E$ by assumption. Hence,

$$\begin{aligned}
[E(\beta):E][E:K] &= [E(\beta):K(\beta)][K(\beta):K] \\
&= [E(\alpha):K(\alpha)][K(\alpha):K] \\
&= [E(\alpha):E][E:K] \\
&= [E:K].
\end{aligned}$$

  Thus $[E(\beta):E]=1$. So $\beta \in E$, as required.

Extension of K-Monomorphisms

Corollary

Let L be a normal extension of finite degree over a field K, and let E be a subfield of L containing K. Then every K-monomorphism from E into L can be extended to a K-automorphism of L.

- Let φ be a K-monomorphism from E into L.

  By the theorem, there exists a polynomial f such that L is a splitting field for f over K.

  L is also a splitting field for f over each of the fields E and $\varphi(E)$.

  By a preceding theorem, we deduce that there is a K-automorphism φ^* of L extending φ.

Example

- Let $K = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.
  Let $\varphi : E \to L$ be defined by
  $$\varphi(a + b\sqrt{2}) = a - b\sqrt{2}.$$
  Then φ is a K-monomorphism.
  So φ extends to a $\mathbb{Q}$-automorphism φ^* of L.
  φ^* is defined by
  $$\varphi^*(a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}) = a - b\sqrt{2} + c\sqrt{5} - d\sqrt{10}.$$

K-Automorphisms Mapping Roots

Corollary

Let L be a normal extension of finite degree over a field K. If z_1 and z_2 are roots in L of an irreducible polynomial in $K[X]$, then there exists a K-automorphism θ of L, such that $\theta(z_1) = z_2$.

- By a preceding theorem, there is a K-isomorphism from $K(z_1)$ onto $K(z_2)$. By the corollary, this extends to a K-automorphism θ of L.

Example

- Let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(u, i\sqrt{3})$, where $u = \sqrt[3]{2}$.

  L is the splitting field over $\mathbb{Q}$ of $X^3 - 2$ (has complex roots $\sqrt[3]{2}$, $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$).

  So it is a normal extension of $\mathbb{Q}$.

  The set $\{1, u, u^2, i\sqrt{3}, ui\sqrt{3}, u^2 i\sqrt{3}\}$ is a basis for L over $\mathbb{Q}$.

  The polynomial $X^3 - 2$ is irreducible over $\mathbb{Q}$

  Consider the two roots u and $ue^{2\pi i/3} = -\frac{1}{2}u + ui\frac{\sqrt{3}}{2}$.

  There is a $\mathbb{Q}$-isomorphism $\theta : \mathbb{Q}(u) \to \mathbb{Q}(ue^{2\pi i/3})$.

  By the corollary, this extends to a $\mathbb{Q}$-automorphism θ^* of L.

Example (Cont'd)

- Any $\mathbb{Q}$-automorphism of L maps $i\sqrt{3}$ to $\pm i\sqrt{3}$.
  Let us choose $\theta^*(i\sqrt{3}) = i\sqrt{3}$.
  Then, recalling that $e^{2\pi i/3} = \frac{1}{2}(-1+i\sqrt{3})$, we deduce that:

  $$\begin{array}{rcl}\theta^*(u^2) & = & u^2 e^{4\pi i/3} = \frac{1}{2}(-u^2 - u^2 i\sqrt{3});\\ \theta^*(ui\sqrt{3}) & = & (-\frac{1}{2}u + ui\frac{\sqrt{2}}{3})i\sqrt{3} = \frac{1}{2}(-ui\sqrt{3} - 3u);\\ \theta^*(u^2 i\sqrt{3}) & = & (-\frac{1}{2}u^2 - u^2 i\frac{\sqrt{2}}{3})i\sqrt{3} = \frac{1}{2}(-u^2 i\sqrt{3} + 3u^2).\end{array}$$

  So the required extension is defined by

  $$\begin{aligned}&\theta^*(a_1 + a_2 u + a_3 u^2 + a_4 i\sqrt{3} + a_5 ui\sqrt{3} + a_6 u^2 i\sqrt{3})\\ &\quad = a_1 + a_2\tfrac{1}{2}(-u + ui\sqrt{3}) + a_3\tfrac{1}{2}(-u^2 - u^2 i\sqrt{3})\\ &\qquad\qquad + a_4 i\sqrt{3} + a_5\tfrac{1}{2}(-ui\sqrt{3} - 3u) + a_6\tfrac{1}{2}(-u^2 i\sqrt{3} + 3u^2)\\ &\quad = a_1 + (-\tfrac{1}{2}a_2 - \tfrac{3}{2}a_5)u + (-\tfrac{1}{2}a_3 + \tfrac{3}{2}a_6)u^2 + a_4 i\sqrt{3}\\ &\qquad\qquad + (\tfrac{1}{2}a_2 - \tfrac{1}{2}a_5)ui\sqrt{3} + (-\tfrac{1}{2}a_3 - \tfrac{1}{2}a_6)u^2 i\sqrt{3}.\end{aligned}$$

Normal Closure

- If L is a finite extension of a field K, a field N containing L is said to be a **normal closure of L over K** if:
  (i) It is a normal extension of K;
  (ii) If E is a proper subfield of N containing L, then E is not a normal extension of K.

Theorem

Let L be a finite extension of a field K. Then:

(i) There exists a normal closure N of L over K;

(ii) If L' is a finite extension over K, such that there is a K-isomorphism $\varphi : L \to L'$, and if N' is a normal closure of L' over K, then there is a K-isomorphism $\psi : N \to N'$, such that the diagram (in which ι is the identity map and unmarked maps are inclusions) commutes.

$$\begin{tikzcd} K \arrow[r] \arrow[d, "\iota"'] & L \arrow[r] \arrow[d, "\varphi"'] & N \arrow[d, "\psi"] \\ K \arrow[r] & L' \arrow[r] & N' \end{tikzcd}$$

Proof of Existence of Normal Closure

(i) Let $\{z_1, z_2, \ldots, z_n\}$ be a basis for L over K.

Each z_i is algebraic over K.

Let m_i be the minimum polynomial of z_i.

Set $m = m_1 m_2 \cdots m_n$, and let N be a splitting field for m over K.

- By the proof of the previous theorem, N is a normal extension of K.
- N contains all the roots of each of the polynomials m_i.
  So it certainly contains $z_1, z_2, \ldots, z_n$.
  Hence, N contains L.
- Let E be a subfield of N containing L. Suppose that E is normal.
  For each $i = 1, \ldots, n$, the field E contains one root of m_i, namely z_i.
  By normality, E contains all the roots of all the m_i.
  So $E = N$.

Thus, N is a normal closure.

Proof of Uniqueness of Normal Closure

(ii) Let N' be a normal closure of L' over K. Every element of L has a unique expression $a_1z_1 + a_2z_2 + \cdots + a_nz_n$, where $a_1, a_2, \ldots, a_n \in K$.
Let $u' = \varphi(u)$ be an arbitrary element of L'.
There is a unique n-tuple $(a_1, a_2, \ldots, a_n)$ of elements of K, such that

$$u' = \varphi(u) = \varphi(a_1z_1 + a_2z_2 + \cdots + a_nz_n) = a_1\varphi(z_1) + a_2\varphi(z_2) + \cdots + a_n\varphi(z_n).$$

It is easy to see that $\{\varphi(z_1), \varphi(z_2), \ldots, \varphi(z_n)\}$ is a basis for L' over K.
The isomorphism φ also ensures that, for $i = 1, 2, \ldots, n$, the minimum polynomial of $\varphi(z_i)$ is $\widehat{\varphi}(m_i)$ (where $\widehat{\varphi}$ is the canonical extension of φ to the polynomial ring $L[X]$).
Now N' is, by assumption, a normal extension of L'.
So it must contain all the roots of all of the $\widehat{\varphi}(m_i)$.
So it must be a splitting field of $\widehat{\varphi}(m) = \widehat{\varphi}(m_1)\widehat{\varphi}(m_2)\cdots\widehat{\varphi}(m_n)$.
The existence of the isomorphism ψ now follows from a previous theorem.

Alternative Expression for Normal Closure

Corollary

Let L be a finite extension of K and let N be a normal closure of L. Then $N = L_1 \vee L_2 \vee \cdots \vee L_k$, where $L_1, L_2, \ldots, L_k$ are subfields containing K, each of them isomorphic to L.

- By the theorem just proved, we may suppose that:
  - $L = K(z_1, z_2, \ldots, z_n)$;
  - $m_1, m_2, \ldots, m_n$ are the minimum polynomials of $z_1, z_2, \ldots, z_n$;
  - N is a splitting field over K for the polynomial $m_1 m_2 \cdots m_n$.

  Let $i \in \{1, 2, \ldots, n\}$ and let z_i' be a root of m_i.

  Then, for all i and z_i', the field $K(z_1, \ldots, z_i', \ldots, z_n)$ is isomorphic to L.

  The field N is generated over K by the set $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ of all the roots of all the polynomials $m_1, m_2, \ldots, m_n$.

  So N is generated by the fields of type $K(z_1, \ldots, z_i', \ldots, z_n)$.

Example

- We determine the normal closure of $K = \mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$.
  A basis for K over $\mathbb{Q}$ is $\{1, u, u^2\}$, where $u = \sqrt[3]{2}$.
  - 1 has a minimum polynomial $X - 1$;
  - u has minimum polynomial $X^3 - 2$;
  - u^2 has minimum polynomial $X^3 - 4$.

  We must find the splitting field of $(X-1)(X^3-2)(X^3-4)$.
  Obviously the factor $X - 1$ is irrelevant, since it already splits over $\mathbb{Q}$.
  We know that, over the field $\mathbb{Q}(u, i\sqrt{3})$,
  $$X^3 - 2 = (X-u)(X-ue^{2\pi i/3})(X-ue^{-2\pi i/3}).$$
  Over the same field,
  $$\begin{aligned} (X-u^2)(X-u^2e^{2\pi i/3})(X-u^2e^{-2\pi i/3}) \\ &= (X-u^2)(X^2+u^2X+u^4) \\ &= X^3+u^2X^2+2uX-u^2X^2-2uX-4 \\ &= X^3-4. \end{aligned}$$
  The conclusion is that the normal closure is $\mathbb{Q}(u, i\sqrt{3})$.

Normal Extensions and K-Automorphisms

Theorem

Let L be a finite normal extension of a field K, and let E be a subfield of L containing K. Then E is a normal extension of K if and only if every K-monomorphism of E into L is a K-automorphism of E.

- Suppose E is a normal extension. So E is its own normal closure.
  Let φ be a K-monomorphism from E into L, and let $z \in E$.
  Let $m = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ be the minimum polynomial of z over K. Then $z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 = 0$.
  Applying φ, $(\varphi(z))^n + a_{n-1}(\varphi(z))^{n-1} + \cdots + a_1\varphi(z) + a_0 = 0$.
  Thus, $\varphi(z)$ is also a root of m in L.
  But z, an element of E, is a root of the irreducible polynomial m.
  Since E is normal, m splits completely over E. So $\varphi(z) \in E$.
  Thus, $\varphi(E)$ is a field contained in E.

Normal Extensions and K-Automorphisms (Converse)

- We showed that $\phi(E) \subseteq E$. Now,

$$[\varphi(E):K] = [\varphi(E):\varphi(K)] = [E:K] = [E:\varphi(E)][\varphi(E):K].$$

  So $\varphi(E) = E$. Thus, φ is a K-automorphism of E.
- Conversely, suppose that every K-monomorphism from E into L is a K-automorphism of E.

  Let f be an irreducible polynomial in $K[X]$ having a root z in E.

  To establish that E is normal, we must show that f splits over E.

  Certainly, since L is normal, f splits completely over L.

  Let z' be another root of f in L. By a previous corollary, there is a K-automorphism ψ of L, such that $\psi(z) = z'$. Let ψ^* be the restriction of ψ to E. Then ψ^* is a K-monomorphism from E into L. By hypothesis, ψ^* is a K-automorphism of E. Thus, we get $z' = \psi(z) = \psi^*(z) \in E$. Thus, E is normal.

Extensions Over Intermediate Fields

Theorem

Let L be a normal extension of a field K, and let E be a subfield of L containing K. Then L is a normal extension of E.

- Let $f(X)$ be an irreducible polynomial in $E[X]$.

  Suppose $f(X)$ has a root α in L.

  Let $m_K(X)$ be the minimal polynomial of α over K.

  $m_K(X)$ in $K[X]$ has root α in L and $L:K$ is normal.

  Therefore, $m_K(X)$ splits over L.

  Since $m_K(X)$ is in $E[X]$ and $m_K(\alpha)=0$, $f(X) \mid m_K(X)$.

  Since $m_K(X)$ splits over L and $f(X) \mid m_K(X)$, $f(X)$ also splits over L.

  Hence, $L:E$ is a normal extension.

Subsection 4

Separable Extensions

Separable Polynomials and Separable Extensions

- An irreducible polynomial f with coefficients in a field K is said to be **separable over** K if it has no repeated roots in a splitting field.
  That is, in a splitting field L of f,
  $$f = k(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n),$$
  where the roots $\alpha_1,\alpha_2,\ldots,\alpha_n$ are all distinct.
- An arbitrary polynomial g in $K[X]$ is called **separable over** K if all its irreducible factors are separable over K.
- An algebraic element in an extension L of K is called **separable over** K if its minimum polynomial is separable over K.
- An algebraic extension L of K is called **separable** if every α in L is separable over K.
- A field K is called **perfect** if every polynomial in $K[X]$ is separable over K.
- Separability is the second property (after normality) that will ensure that the maps Φ and Γ are mutually inverse.

Separability of Polynomials

- We know that the irreducible polynomial f has repeated roots in its splitting field if and only if f and Df have a non-trivial common factor.

Theorem

Let f be an irreducible polynomial with coefficients in a field K.

(i) If K has characteristic 0, then f is separable over K.

(ii) If K has finite characteristic p, then f is separable unless it is of the form
$$b_0 + b_1 X^p + b_2 X^{2p} + \cdots + b_m X^{mp}.$$

- Suppose $f = a_0 + a_1 X + \cdots + a_n X^n$, with $\partial f = n \geq 1$, is not separable.
  Then f and Df have a common factor d of degree at least 1.
  Since f is irreducible, d must be a constant multiple (associate) of f.
  This divides Df only if $Df = a_1 + 2a_2 X + \cdots + na_n X^{n-1}$ is the zero polynomial. Hence, $a_1 = 2a_2 = \cdots = na_n = 0$.

Separability of Polynomials (Cont'd)

- Suppose K has characteristic 0.

  The preceding equations give $a_1 = a_2 = \cdots = a_n = 0$.

  Thus, f is the constant polynomial a_0.

  This contradicts the hypothesis.

  So f must be separable.

- Suppose $\mathrm{char} K = p$.

  Then $ra_r = 0$ implies that $a_r = 0$ if and only if $p \nmid r$.

  So the only non-zero terms in f are of the form $a_{kp}X^{kp}$, $k = 0, 1, \ldots$.

  Writing a_{kp} as b_k gives the required conclusion.

Corollary

Every field of characteristic 0 is perfect.

Irreducibility in Characteristic p

Theorem

Let K be a field with finite characteristic p, and let

$$f(X) = g(X^p) = b_0 + b_1X^p + b_2X^{2p} + \cdots + b_mX^{mp}.$$

Then the following statements are equivalent:

(i) f is irreducible in $K[X]$;

(ii) g is irreducible in $K[X]$, and not all of the coefficients b_i are p-th powers of elements of K.

(i)⇒(ii): Suppose g has a non-trivial factorization $g(X) = u(X)v(X)$. Then f factors $f(X) = g(X^p) = u(X^p)v(X^p)$. This is a contradiction. Hence g is irreducible.

Suppose $b_i = c_i^p$, for $i = 1, 2, \ldots, m$. Then, by a previous theorem,

$$\begin{array}{rcl} f(X) & = & g(X^p) = c_0^p + (c_1X)^p + \cdots + (c_mX^m)^p \\ & = & (c_0 + c_1X + \cdots + c_mX^m)^p. \end{array}$$

Again a contradiction. Hence, not all of the b_i's are p-th powers.

Irreducibility in Characteristic p (Converse Case 1)

(ii)$\Rightarrow$(i): Suppose that f is reducible. We must prove either that g is reducible, or that all the coefficients of f are p-th powers. We have two cases:

1. $f = u^r$, where $r > 1$ and u is irreducible;
2. $f = vw$, where $\partial v, \partial w > 0$, and v and w are coprime.

Case 1:

- Suppose first that $p \mid r$. Then $f = (u^{r/p})^p = h^p$ (say).
  Let $h = d_0 + d_1 X + \cdots + d_s X^s$. Then, using the same theorem,
  $$f = h^p = (d_0 + d_1 X + \cdots + d_s X^s)^p = d_0^p + d_1^p X^p + \cdots + d_s^p X^{sp}.$$
  So all the coefficients of f are p-th powers.
- Suppose that $p \nmid r$. By the definition of f, $Df = 0$.
  Thus, $0 = Df = r(Du)u^{r-1}$. So $Du = 0$. Thus, we may write
  $$u(X) = e_0 + e_1 X^p + \cdots + e_t X^{tp} = v(X^p).$$
  Now we get $g(X^p) = f(X) = (u(X))^r = (v(X^p))^r$.
  Thus, $g(X) = (v(X))^r$. So g is not irreducible.

Irreducibility in Characteristic p (Converse Case 2)

Case 2: $f = vw$, $\partial v, \partial w > 0$, v, w are coprime. $K[X]$ is a Euclidean domain. So there exist s, t in $K[X]$, such that $sv + tw = 1$.
By hypothesis, $Df = 0$. So $(Dv)w + v(Dw) = 0$. We now get

$$0 = (Dv)tw + tv(Dw) = (Dv)(1 - sv) + tv(Dw).$$

So $Dv = sv(Dv) - tv(Dw)$. Hence $v \mid Dv$.
But $\partial(Dv) < \partial v$. Hence, $Dv = 0$. Similarly, $Dw = 0$. We may write

$$\begin{array}{rcl} v(X) & = & d_0 + d_1 X^p + \cdots + d_s X^{sp}, \\ w(X) & = & e_0 + e_1 X^p + \cdots + e_t X^{tp}. \end{array}$$

Define $\overline{v}(X) = d_0 + d_1 X + \cdots + d_s X^s$ and $\overline{w}(X) = e_0 + e_1 X + \cdots + e_t X^t$. Then

$$g(X^p) = f(X) = v(X)w(X) = \overline{v}(X^p)\overline{w}(X^p).$$

So $g(X) = \overline{v}(X)\overline{w}(X)$. Thus g is not irreducible.

Finite Fields are Perfect

Theorem

Every finite field is perfect.

- Let K be a finite field of characteristic p.

  The Frobenius mapping $a \mapsto a^p$ is an automorphism of K.

  So every element of K is a p-th power.

  By a previous theorem, the only candidate for an inseparable irreducible polynomial is something of the form

$$f = b_0 + b_1 X^p + \cdots + b_m X^{mp}.$$

  But all the coefficients are p-th powers.

  By the last theorem, even polynomials of this form are reducible.

  Hence K is perfect.

An Example of an Imperfect Field

- An "imperfect" field has to be infinite and of finite characteristic.
- The most obvious example is $K = \mathbb{Z}_p(X)$, the field of all rational forms with coefficients in $\mathbb{Z}_p$.
- For polynomials with coefficients in K we must use a different letter, such as Y, for the indeterminate.
- We look at the polynomial $f(Y) = Y^p - X$ in $K[Y]$.
- We show $f(Y)$ is irreducible in K and inseparable.
  - Suppose f is reducible. By the theorem, $-X$ is a p-th power in K. So there exists $\frac{u(X)}{v(X)}$ in K, such that $\left[\frac{u(X)}{v(X)}\right]^p = -X$. Thus, $-X[v(X)]^p = [u(X)]^p$. But $p \mid \partial([u(X)]^p)$ and $p \nmid \partial(X[v(X)]^p)$. This is a contradiction.
  - Let L be a splitting field for f over K. Let α be a root of f in L. Thus, $\alpha^p = X$. The factorization of f in L is
  $$f(Y) = Y^p - X = Y^p - \alpha^p = (Y - \alpha)^p.$$
  The polynomial f is as inseparable as it is possible to be!

Separability of Intermediate Fields

Theorem

Let L be a finite separable extension of a field K, and let E be a subfield of L containing K. Then L is a separable extension of E.

- Let $\alpha \in L$, and let m_K, m_E be the minimum polynomials of α over K and E, respectively. Suppose that m_K is separable. Within $E[X]$ we can use the division algorithm $m_K = qm_E + r$, $\partial r < \partial m_E$. We get $r(\alpha) = m_K(\alpha) - q(\alpha)m_E(\alpha) = 0 - 0 = 0$. This contradicts the minimality of m_E unless $r = 0$. Hence $m_K = qm_E$ in the ring $E[X]$.

  Suppose m_E is not separable. Then there is a non-constant polynomial g dividing m_E and Dm_E. But $Dm_K = qDm_E + m_E Dq$.

  So g divides m_K and Dm_K. This can happen only if m_K has at least one repeated root in a splitting field. So we have a contradiction.

  Hence, m_E is separable.

Subsection 5

The Galois Correspondence

The Galois Extension

- A finite extension of a field K that is both normal and separable is called a **Galois extension**.
- We look again at $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$ and $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$.
  - $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$ is normal, since it is the splitting field of $(X^2-2)(X^2+3)$.
    $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$ is separable, since $\mathbb{Q}$ is perfect.
    The order of the Galois group is equal to the degree over $\mathbb{Q}$ of the extension.
  - $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ is normal, since it is the splitting field of X^3-2.
    $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ is separable, since $\mathbb{Q}$ is perfect.
    The order of the Galois group is equal to the degree over $\mathbb{Q}$ of the extension.
- We will prove that, if $L:K$ is a normal, separable extension of degree n, and G is the Galois group of L over K, then $|G| = [L:K]$.

Monomorphisms into a Normal Closure

Theorem

Let $L:K$ be a separable extension of finite degree n. Then there are precisely n distinct K-monomorphisms of L into a normal closure N of L over K.

- By induction on the degree $[L:K]$.
- Suppose $[L:K]=1$. Then $L=K=N$. Hence, the only K-monomorphism of K into N is the identity mapping ι.
- Assume now that the result is established for all $n \leq k-1$. Suppose that $[L:K]=k>1$. Let $z_1 \in L \backslash K$. Let m (with $\partial m = r \geq 2$) be the minimum polynomial of z_1 over K. Thus, $K \subset K(z_1) \subseteq L$, and $[K(z_1):K]=r$. But m is irreducible and has one root z_1 in the normal extension N. So m splits completely over N. Since L is separable, the roots of m are all distinct. Suppose the roots are $z_1, z_2, \ldots, z_r$. Let $[L:K(z_1)]=s$. Then $1 \leq s < k$, and $rs=k$.

Monomorphisms into a Normal Closure (Cont'd)

- The field N is a normal closure of L over $K(z_1)$.

  So, by the induction hypothesis, the number of $K(z_1)$-monomorphisms from L into N is precisely s. Denote them by $\mu_1, \mu_2, \ldots, \mu_s$.

  Let $\lambda_1, \lambda_2, \ldots, \lambda_r$ be r distinct K-automorphisms of N, with $\lambda_i(z_1) = z_i$.

  Define maps $\varphi_{ij} : L \to N$, by

$$\varphi_{ij}(x) = \lambda_i(\mu_j(x)), \quad x \in L,\ i = 1, 2, \ldots, r,\ j = 1, 2, \ldots, s.$$

  The maps are all K-monomorphisms.

  Claim: The maps φ_{ij} are all distinct.

  First, $\varphi_{ij}(z_1) = \lambda_i(\mu_j(z_1)) = \lambda_i(z_1) = z_i$. So $\varphi_{ij} = \varphi_{pq}$ implies $i = p$.

  Let $\varphi_{ij} = \varphi_{iq}$. Then, for all x in L, $\lambda_i(\mu_j(x)) = \lambda_i(\mu_q(x))$. But λ_i is one-one. So $\mu_j(x) = \mu_q(x)$, for all x in L. That is, $j = q$.

  Thus, there are at least k distinct K-monomorphisms from L into N.

Monomorphisms into a Normal Closure (Conclusion)

Claim: There are no more than k distinct K-monomorphisms from L into N.

We show that every K-monomorphism ψ from L into N coincides with one of the maps φ_{ij}.

The map ψ must map z_1 to another root z_i of m in N.

Let $\chi : L \to N$ be defined by $\chi(x) = \lambda_i^{-1}(\psi(x))$.

This is certainly a K-monomorphism.

Moreover, $\chi(z_1) = \lambda_i^{-1}(\psi(z_1)) = \lambda_i^{-1}(z_i) = z_1$.

So ψ is a $K(z_1)$-monomorphism.

So it must coincide with one of $\mu_1, \mu_2, \ldots, \mu_s$, say μ_j.

Thus, for all x in L, $\mu_j(x) = \lambda_i^{-1}(\psi(x))$.

So $\psi(x) = \lambda_i(\mu_j(x)) = \varphi_{ij}(x)$. Thus, $\psi = \varphi_{ij}$.

Cardinality of the Galois Group of a Galois Extension

Corollary

Let L be a Galois extension of K, and let G be the Galois group of L over K. Then $|G| = [L : K]$.

- Let L be a Galois extension of K.

  Then L is both normal as well as separable.

  Thus, L is its own normal closure.

  By the theorem, $|G| = [L : K]$.

Galois Automorphisms and Roots

Lemma

Let L be a finite extension of K. Suppose $\text{Gal}(L:K) = \{\varphi_1 = \iota, \varphi_2, \ldots, \varphi_n\}$. Let f be an irreducible polynomial in $K[X]$, having a root z in L and set $\varphi_i(z) = z_i$, with the $z_1, \ldots, z_r$ distinct. Then, for all $\varphi_j \in \text{Gal}(L:K)$,

$$\{z_1, z_2, \ldots, z_r\} = \{\varphi_j(z_1), \varphi_j(z_2), \ldots, \varphi_j(z_r)\}.$$

- We note that $\varphi_j(z_i)$ is equal to $(\varphi_j \varphi_i)(z)$.

  This is equal to $\varphi_k(z) = z_k$, for some k, since $\varphi_j \varphi_i \in \text{Gal}(L:K)$.

  But φ_j is one-one.

  So it merely permutes the elements $z_1, z_2, \ldots, z_r$.

Form of the Minimum Polynomial

Lemma

Let L be a finite extension of K. Suppose $\mathrm{Gal}(L:K) = \{\varphi_1 = \iota, \varphi_2, \ldots, \varphi_n\}$. Let f be an irreducible polynomial in $K[X]$, having a root z in L and set $\varphi_i(z) = z_i$, with the $z_1, \ldots, z_r$ distinct. The polynomial

$$g(X) = (X - z_1)(X - z_2) \cdots (X - z_r)$$

is the minimum polynomial of z over K.

- We must show that every polynomial in $K[X]$ having z as a root is divisible by g. Suppose that

  $$h = a_0 + a_1 X + \cdots + a_m X^m,$$

  with coefficients in K, is such that $a_0 + a_1 z + \cdots + a_m z^m = 0$. Apply φ_j (which fixes all the a_i's) to obtain

  $$a_0 + a_1 z_j + \cdots + a_m z_j^m = 0, \quad j = 1, 2, \ldots, r.$$

  So h is divisible by $X - z_1, X - z_2, \ldots, X - z_r$. Thus, it is divisible by g.

Separability and Normality and the Map Φ

Theorem

Let L be a finite extension of K. Then $\Phi(\mathrm{Gal}(L:K)) = K$ if and only if L is a separable normal extension of K.

- Let L be a separable and normal extension of K, with $[L:K] = n$.

  By the preceding corollary, $|\mathrm{Gal}(L:K)| = n$.

  Denote $\Phi(\mathrm{Gal}(L:K))$ by K'.
  - We know that $K \subseteq K'$.
  - By a preceding theorem, we have that

$$[L:K'] = [L:\Phi(\mathrm{Gal}(L:K))] = |\mathrm{Gal}(L:K)| = n.$$

  Now $K \subseteq K'$ and $[L:K] = [L:K']$.

  It follows that $K = K'$.

Separability and Normality and the Map Φ (Converse)

- Suppose $K = K' = \Phi(\mathrm{Gal}(L:K))$.

  Let $\mathrm{Gal}(L:K) = \{\varphi_1 = \iota, \varphi_2, \ldots, \varphi_n\}$.

  Let f be an irreducible polynomial in $K[X]$ having a root z in L.

  We must show that:
    - f splits completely over L;
    - f has distinct roots in L.

  The images of z under the K-automorphisms $\varphi_1, \varphi_2, \ldots, \varphi_n$ need not all be distinct.

  We have $\varphi_1(z) = \iota(z) = z$, and re-label the elements of $\mathrm{Gal}(L:K)$ so that $\varphi_2(z), \ldots, \varphi_r(z)$ are the remaining distinct images of z under the automorphisms in $\mathrm{Gal}(L:K)$. Write $\varphi_i(z) = z_i$.

Separability and Normality and the Map Φ (Converse)

- Let g be the polynomial

$$(X-z_1)(X-z_2)\cdots(X-z_r)=X^r-e_1X^{r-1}+\cdots+(-1)^re_r,$$

where the coefficients $e_1,e_2,\ldots,e_r$ are the elementary symmetric functions $e_1=\sum_{i=1}^r z_i, e_2=\sum_{i\neq j} z_iz_j,\ldots,e_r=z_1z_2\cdots z_r$.
These coefficients are unchanged by any permutation of $z_1,z_2,\ldots,z_r$.
By a previous lemma, they are unchanged by each φ_j in $\mathrm{Gal}(L:K)$.
Thus, g is a polynomial with coefficients in $\Phi(\mathrm{Gal}(L:K))=K$.
z is assumed to be a root in L of the irreducible polynomial f in $K[X]$.
By the preceding lemma, f is divisible by g.
By the irreducibility of f, f is a constant multiple of g.
Since g splits completely over L, so does f.
Moreover, all its roots are distinct.
So L is a separable normal extension of K.

Galois Automorphisms and Intermediate Fields

Theorem

Let L be a Galois extension of a field K, and let E be a subfield of L containing K. If $\delta \in \mathrm{Gal}(L:K)$, then $\Gamma(\delta(E)) = \delta\Gamma(E)\delta^{-1}$.

- Write $\delta(E) = E'$, $\Gamma(E) = H$ and $\Gamma(E') = H'$. We show $H' = \delta H \delta^{-1}$.
  Let $\theta \in H$. We shall show that $\delta\theta\delta^{-1} \in H'$.
  Let $z' \in E'$ and z be the unique element of E, such that $\delta(z) = z'$.
  Since $\theta \in \Gamma(E)$, θ fixes all the elements of E. Thus, we get
  $$(\delta\theta\delta^{-1})(z') = (\delta\theta\delta^{-1}\delta)(z) = \delta(\theta(z)) = \delta(z) = z'.$$
  So $\delta\theta\delta^{-1} \in H'$. Therefore, $\delta H \delta^{-1} \subseteq H'$.
  Let $\theta' \in H'$, and let $z \in E$. Then $\delta(z) \in E'$. So $\theta'(\delta(z)) = \delta(z)$.
  Hence, $(\delta^{-1}\theta'\delta)(z) = (\delta^{-1}\delta)(z) = z$. So $\delta^{-1}\theta'\delta \in \Gamma(E) = H$.
  We have shown that $\delta^{-1}H'\delta \subseteq H$.
  It follows immediately that $H' \subseteq \delta H \delta^{-1}$.

Subsection 6

The Fundamental Theorem

Fundamental Theorem of Galois Theory

Theorem (The Fundamental Theorem of Galois Theory)

Let L be a separable normal extension of a field K, with finite degree n.

(i) For all subfields E of L containing K, and for all subgroups H of the Galois group $\mathrm{Gal}(L:K)$, $\Phi(\Gamma(E)) = E$, $\Gamma(\Phi(H)) = H$.

We also have $|\Gamma(E)| = [L:E]$ and $\frac{|\mathrm{Gal}(L:K)|}{|\Gamma(E)|} = [E:K]$.

(ii) A subfield E is a normal extension of K if and only if $\Gamma(E)$ is a normal subgroup of $\mathrm{Gal}(L:K)$. If E is a normal extension, then $\mathrm{Gal}(E:K)$ is isomorphic to the quotient group $\mathrm{Gal}(L:K)/\Gamma(E)$.

(i) Let E be a subfield of L containing K. By previous theorems, L is both normal and separable over E. Hence, $|\Gamma(E)| = [L:E]$. So $[E:K] = \frac{[L:K]}{[L:E]} = \frac{|\mathrm{Gal}(L:K)|}{|\Gamma(E)|}$. But $\Gamma(E) = \mathrm{Gal}(L:E)$.

So we get $\Phi(\Gamma(E)) = \Phi(\mathrm{Gal}(L:E)) = E$.

Fundamental Theorem of Galois Theory (Cont'd)

- Now let H be any subgroup of the finite group $\mathrm{Gal}(L:K)$.
  We know that $H \subseteq \Gamma(\Phi(H))$. Denote $\Gamma(\Phi(H))$ by H'.
  We have $\Phi(H) = \Phi(\Gamma(\Phi(H))) = \Phi(H')$.
  We now obtain $|H| = [L:\Phi(H)] = [L:\Phi(H')] = |H'|$.
  This, and the finiteness of $\mathrm{Gal}(L,K)$, imply that $H' = H$.

(ii) Suppose now that E is a normal extension.
  Let $\delta \in \mathrm{Gal}(L:K)$ and δ' the restriction of δ to E.
  Then δ' is a monomorphism from E into L.
  So, by a previous theorem, δ' is a K-automorphism of E.
  By the last theorem, $\Gamma(E) = \Gamma(\delta(E)) = \delta\Gamma(E)\delta^{-1}$.
  Thus, $\Gamma(E)$ is a normal subgroup of $\mathrm{Gal}(L:K)$.

Fundamental Theorem of Galois Theory (Cont'd)

- Suppose that $\Gamma(E)$ is a normal subgroup of $\mathrm{Gal}(L:K)$.

  Let δ_1 be a K-monomorphism from E into L.

  By a previous corollary, this extends to a K-automorphism δ of L.

  The normality of $\Gamma(E)$ within $\mathrm{Gal}(L:K)$ means that $\delta\Gamma(E)\delta^{-1}=\Gamma(E)$.

  Hence, by the preceding theorem, $\Gamma(\delta(E))=\Gamma(E)$.

  Since Γ is one-one, it follows that $\delta(E)=\delta_1(E)=E$.

  Thus, δ_1 is a K-automorphism of E.

  We have shown that every K-monomorphism of E into L is a K-automorphism of E.

  By a preceding theorem, E is a normal extension of K.

Fundamental Theorem of Galois Theory (Conclusion)

- It remains to show that, if E is a normal extension, then $\mathrm{Gal}(E:K) \cong \mathrm{Gal}(L:K)/\Gamma(E)$.

  So suppose that E is normal. As above, let δ' be the restriction to E of the K-automorphism δ of L. We have seen that $\delta' \in \mathrm{Gal}(E:K)$.

  Let $\Theta : \mathrm{Gal}(L:K) \to \mathrm{Gal}(E:K)$ be defined by $\Theta(\delta) = \delta'$.

  Then Θ is a group homomorphism. For all δ_1, δ_2 in $\mathrm{Gal}(L:K)$, with $\Theta(\delta_1) = \delta'_1$ and $\Theta(\delta_2) = \delta'_2$, and all z in E,

$$\begin{array}{rcl}([\Theta(\delta_1)][\Theta(\delta_2)])(z) & = & (\delta'_1\delta'_2)(z) = \delta'_1(\delta_2(z)) \\ & = & \delta_1(\delta_2(z)) = (\delta_1\delta_2)(z) \\ & = & (\Theta(\delta_1\delta_2))(z).\end{array}$$

  Hence $[\Theta(\delta_1)][\Theta(\delta_2)] = \Theta(\delta_1\delta_2)$. The kernel of Θ is the set of all δ in $\mathrm{Gal}(L:K)$, such that δ' is the identity map on E, i.e., $\Gamma(E)$.

  The Homomorphism Theorem yields $\mathrm{Gal}(E:K) \cong \mathrm{Gal}(L:K)/\Gamma(E)$.

The Join of Two Subfields

- Let U and V be subgroups of a group G.
  - Then $U \cap V$ is a subgroup of G.
  - In general, $U \cup V$ is not a subgroup, but there is always a smallest subgroup containing U and V, consisting of all products $u_1 v_1 u_2 v_2 \cdots u_n v_n$ (for all n) with $u_1, u_2, \ldots \in U$, $v_1, v_2, \ldots \in V$.
    We denote this by $U \vee V$, and call it the **join** of U and V.
- Similarly, if E and F are subfields of a field K, then:
  - $E \cap F$ is also a subfield;
  - There is a subfield $E \vee F = E(F) = F(E)$.
    It is called the **join** of E and F.

Γ, Meets and Joins

Theorem

Let L be a Galois extension of finite degree over K, with Galois group G, and let E_1, E_2 be subfields of L containing K. If $\Gamma(E_1) = H_1$ and $\Gamma(E_2) = H_2$, then $\Gamma(E_1 \cap E_2) = H_1 \vee H_2$, $\Gamma(E_1 \vee E_2) = H_1 \cap H_2$.

- $E_1 \subseteq E_1 \vee E_2$. Since the Galois correspondence is order-reversing, $\Gamma(E_1 \vee E_2) \subseteq \Gamma(E_1) = H_1$. Similarly, $\Gamma(E_1 \vee E_2) \subseteq \Gamma(E_2) = H_2$. Hence, $\Gamma(E_1 \vee E_2) \subseteq H_1 \cap H_2$.

  Let α in $H_1 \cap H_2$. Since $\alpha \in H_1 = \Gamma(E_1)$, $\alpha(x) = x$, for all x in E_1. Similarly, $\alpha(y) = y$, for all y in E_2. By a previous theorem, the elements of $E_1 \vee E_2 = E_1(E_2)$ are quotients of finite linear combinations (with coefficients in E_1) of finite products of elements of E_2.

  So $\alpha(z) = z$, for all z in $E_1 \vee E_2$. Thus, $\alpha \in \Gamma(E_1 \vee E_2)$.

  So the first assertion of the theorem is proved.

Γ, Meets and Joins

- From $E_1 \cap E_2 \subseteq E_1$ it follows that $H_1 = \Gamma(E_1) \subseteq \Gamma(E_1 \cap E_2)$. Similarly, $H_2 \subseteq \Gamma(E_1 \cap E_2)$. So $H_1 \vee H_2 \subseteq \Gamma(E_1 \cap E_2)$.

  Let x be an element of L not in $E_1 \cap E_2$. Say $x \notin E_1$.

  We know $E_1 = \Phi(H_1)$.

  So there exists γ in $H_1 \subseteq H_1 \vee H_2$, such that $\gamma(x) \neq x$.

  Thus, $x \notin E_1 \cap E_2$ implies $x \notin \Phi(H_1 \vee H_2)$.

  This shows that $\Phi(H_1 \vee H_2) \subseteq E_1 \cap E_2$.

  Now, the Galois correspondence gives $\Gamma(E_1 \cap E_2) \subseteq H_1 \vee H_2$.

Splitting Fields of Extensions

Theorem

Let K be a field of characteristic zero, and let $f \in K[X]$. Let $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a splitting field for f over K. Let M be a field containing K, and let N be a splitting field of f over M. Then, up to isomorphism, L is a subfield of N, and $\mathrm{Gal}(N:M) \cong \mathrm{Gal}(L:M \cap L)$.

$$\begin{tikzcd}[column sep=small] & N \arrow[dl, dash] \arrow[dr, dash] & \\ M \arrow[dr, dash] & & L \arrow[dl, dash] \\ & M \cap L \arrow[d, dash] & \\ & K & \end{tikzcd}$$

- The field N is an extension of M, and hence of K, such that f splits completely in $N[X]$. Hence, by the definition of a splitting field, L is, up to isomorphism, a subfield of N. Write N as $M(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Let $H = \mathrm{Gal}(N:M)$, and let $\gamma \in H$. Then the restriction γ' of γ to L is a monomorphism from L into N. Since γ fixes the elements of M, it certainly fixes the elements of K. Hence, so does γ'. Also, γ maps each root α_i of f to another root of f. Thus, so does γ'.
  So γ' is a monomorphism of L into itself.

Splitting Fields of Extensions (Cont'd)

- γ is an automorphism of $N = M(\alpha_1, \alpha_2, \ldots, \alpha_n)$. So every root α_i of f is the image of some root of f under γ. Hence, also under γ'.

  Thus γ' maps onto $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. So it is a K-automorphism.

  We have a mapping θ from H into $G = \mathrm{Gal}(L:K)$, given by $\theta(\gamma) = \gamma'$.
  - θ is one-one. Let $\delta \in H$ such that $\gamma' = \delta'$. Then γ' and δ' act identically on the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. So $\gamma = \delta$.
  - θ is a group homomorphism. The restriction of $\gamma\delta$ to L is $\gamma'\delta'$.

  Thus, $H \cong \theta(H)$. We show $\theta(H)$ is the subgroup $\mathrm{Gal}(L : M \cap L)$ of G.

  Each γ in H fixes the elements of M. So each γ' fixes those of $M \cap L$.

  Thus $M \cap L \subseteq \Phi(\theta(H))$. By the Galois Theorem, $\theta(H) \subseteq \mathrm{Gal}(L : M \cap L)$.

  Let x be in L but not in $M \cap L$. Thus, $x \notin M$. But M is the field whose elements are fixed by H. So there is a β in H for which $\beta(x) \neq x$. Then $(\theta(\beta))(x) \neq x$. So $x \notin \Phi(\theta(H))$. Thus, $\mathrm{Gal}(L : M \cap L) \subseteq \theta(H)$.

  Now $\mathrm{Gal}(L : M \cap L) = \theta(H) \cong H = \mathrm{Gal}(N : M)$.

Subsection 7

An Example

Example

- Consider the Galois group $G = \mathrm{Gal}(\mathbb{Q}(v,i):\mathbb{Q})$, where $v = \sqrt[4]{2}$.
  The field $\mathbb{Q}(v,i)$ is the splitting field of $X^4 - 2$ over $\mathbb{Q}$.
  If $\xi \in G$, then, $\xi(i) = \pm i$ and $\xi(v) \in \{v, iv, -v, -iv\}$.
  There are 8 elements in the group G:

$$\begin{array}{ll} \iota : v \mapsto v, i \mapsto i; & \lambda : v \mapsto v, i \mapsto -i; \\ \alpha : v \mapsto iv, i \mapsto i; & \mu : v \mapsto iv, i \mapsto -i; \\ \beta : v \mapsto -v, i \mapsto i; & \nu : v \mapsto -v, i \mapsto -i; \\ \gamma : v \mapsto -iv, i \mapsto i; & \rho : v \mapsto -iv, i \mapsto -i. \end{array}$$

The Multiplication Table of G

- The multiplication in G is given by:

	ι	α	β	γ	λ	μ	ν	ρ
ι	ι	α	β	γ	λ	μ	ν	ρ
α	α	β	γ	ι	μ	ν	ρ	λ
β	β	γ	ι	α	ν	ρ	λ	μ
γ	γ	ι	α	β	ρ	λ	μ	ν
λ	λ	ρ	ν	μ	ι	γ	β	α
μ	μ	λ	ρ	ν	α	ι	γ	β
ν	ν	μ	λ	ρ	β	α	ι	γ
ρ	ρ	ν	μ	λ	γ	β	α	ι

Examples of the computation:

- $\alpha(\lambda(v)) = \alpha(v) = iv$; $\alpha(\lambda(i)) = \alpha(-i) = -i$. So $\alpha\lambda = \mu$.
- $\lambda(\alpha(v)) = \lambda(iv) = \lambda(i)\lambda(v) = -iv$; $\lambda(\alpha(i)) = \lambda(i) = -i$; So $\lambda\alpha = \rho$.

Subgroups of G and Corresponding Subfields

- The group $G = \mathrm{Gal}(\mathbb{Q}(v,i):\mathbb{Q})$ has three subgroups of order 4:

$$H_1 = \{\iota, \alpha, \beta, \gamma\},\ H_2 = \{\iota, \beta, \lambda, \nu\},\ H_3 = \{\iota, \beta, \mu, \rho\}.$$

It has five subgroups of order 2:

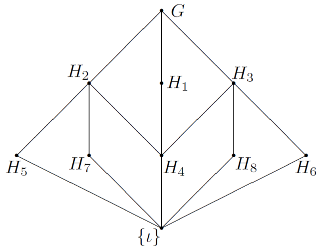
$$H_4 = \{\iota, \beta\},\ H_5 = \{\iota, \lambda\},\ H_6 = \{\iota, \mu\},\ H_7 = \{\iota, \nu\},\ H_8 = \{\iota, \rho\}.$$

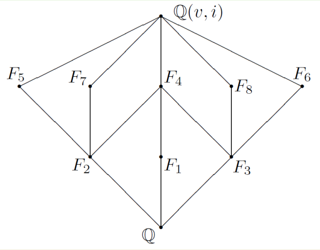
We can compute the corresponding subfields of $\mathbb{Q}(v,i)$.
  - $\Phi(H_1) = \mathbb{Q}(i)$;
  - $\Phi(H_2) = \mathbb{Q}(v^2) = \mathbb{Q}(\sqrt{2})$;
  - $\Phi(H_3) = \mathbb{Q}(i\sqrt{2})$.

We also find the ones corresponding to the order 2 subgroups.
  - $\Phi(H_4) = \mathbb{Q}(i, \sqrt{2})$;
  - $\Phi(H_5) = \mathbb{Q}(v)$;
  - $\Phi(H_6) = \mathbb{Q}((1+i)v)$;
  - $\Phi(H_7) = \mathbb{Q}(iv)$;
  - $\Phi(H_8) = \mathbb{Q}((1-i)v)$.

Lattice of Subgroups and Lattice of Subfields

- The lattice of subgroups of G is shown on the left





and the lattice of subfields E, such that $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(v,i)$, an upside down version of it, is shown on the right, with $F_i := \Phi(H_i)$.

- We look at normal subgroups and extensions.

Normal Subgroups	H_1	H_2	H_3	H_4
Normal Extensions	$\mathbb{Q}(i)$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(i\sqrt{2})$	$\mathbb{Q}(i,\sqrt{2})$
Polynomials Splitting	X^2+1	X^2-2	X^2+2	$(X^2+1)(X^2-2)$

Remarks

- Note that $\mathrm{Gal}(\mathbb{Q}(v,i),\mathbb{Q})$ is not abelian, although both

$$\mathrm{Gal}(\mathbb{Q}(v,i),\mathbb{Q}(i)) = \{\iota,\alpha,\beta,\gamma\}$$

and

$$\mathrm{Gal}(\mathbb{Q}(i),\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(v,i),\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(v,i),\mathbb{Q}(i))$$

are abelian.

- The example is easier than most, since we can easily factorize X^4-2 over the complex field.

  On the other hand, If we start with an irreducible polynomial such as

$$f = 2X^5 - 4X^4 + 8X^3 + 14X^2 + 7,$$

then it is by no means a trivial matter to determine the Galois group.