Math 641 **Modern Algebra 2** Spring 2013

JERZY WOJCIECHOWSKI April 23, 2013

Contents

1 Algebraic Closures.

1.1 Algebraic Elements.

Definition. Let K be a field with a subfield F and $a \in K$. We say that a is *algebraic over* F if and only if there exists a nonzero polynomial $f(x)$ in $F[x]$ such that $f(a) = 0$.

Remark. If a is algebraic over F then there exists a unique monic, irreducible polynomial over F with root a. Such a polynomial is called the *minimal polynomial* of a over F.

1.2 Algebraic Extensions.

Definition. Let F be a field and K be an extension of F. Then K is *algebraic over F* iff every element of K is algebraic over K.

1.3 Algebraically Closed Fields.

Definition. A field K is *algebraically closed* if and only if every polynomial over K splits over K, that is, every nonconstant polynomial over K is a product of linear (of degree 1) polynomials over K.

Remark. Given a field K, if every nonconstant polynomial over K has a root in K, then K is algebraically closed.

1.4 Algebraic Closure.

Definition. Let K be a field and L be an extension of K. We say that L is an *algebraic closure* of K if and only if the following two conditions hold:

1. L is algebraic over K.
2. L is algebraically closed.

1.5 Existence of Algebraic Closures.

Theorem. *For every field K there exists an algebraic closure L of K.*

1.6 Uniqueness of Algebraic Closures.

Theorem. *If K_1, K_2 are fields, $f : K_1 \to K_2$ is an isomorphism and L_1, L_2 are algebraic closures of K_1, K_2, respectively, then f can be extended to an isomorphism $f' : L_1 \to L_2$.*

Corollary. *If L_1 and L_2 are algebraic closures of a field K, then there exists an isomorphism $f : L_1 \to L_2$ such that the restriction $f \restriction K$ of f to K is the identity function.*

2 Splitting Fields and Normal Field Extensions.

2.1 Splitting Field.

Definition. Let f be a nonconstant polynomial over a field F and let K be an extension of F. We say that K is a *splitting field* of f over F if:

1. f is a product of linear polynomials over F, and
2. $K = F(a_1, \dots, a_n)$ where $a_1, \dots, a_n$ are the roots of f in K.

2.2 Homework 1 — due January 16.

Exercise. If K is a splitting field of some nonconstant polynomial f over F, then K is algebraic over F.

2.3 Existence of Splitting Fields.

Remark. Let F be a field, f be a nonconstant polynomial over F and $a_1, \dots, a_n$ be the roots of f in the algebraical closure F^{a} of F. Then the polynomials $x - a_1, \dots, x - a_n$ are the only irreducible factors of $f(x)$ in $F^{\mathrm{a}}[x]$.

Theorem. *If F is any field and f is a nonconstant polynomial over F then there exists a splitting field of f over F.*

Proof. Let F^{a} be an algebraic closure of F and $a_1, \dots, a_n$ be the roots of f in F^{a}. Define $K := F(a_1, \dots, a_n)$ in F^{a}. Then the polynomials $x - a_1, \dots, x - a_n$ are the only irreducible factors of $f(x)$ so

$$f(x) = c\,(x - a_1)^{k_1} \dots (x - a_n)^{k_n}$$

for some $c \in F$ and $k_1, \dots, k_n \in \mathbb{Z}^+$. Thus K is a splitting field of f over F. □

2.4 Uniqueness of Splitting Fields.

Theorem. *Let F be a field, f be a nonconstant polynomial over F and K_1, K_2 be splitting fields of f over F. Then there is an isomorphism $\varphi : K_1 \to K_2$ such that $\varphi \restriction F = id_F$ (the restriction of φ to F is the identity function).*

Proof. Let $K_1^{\mathrm{a}}, K_2^{\mathrm{a}}$ be algebraic closures of K_1, K_2, respectively. Then they are also algebraic closures of F so there is an isomorphism $\psi : K_1^{\mathrm{a}} \to K_2^{\mathrm{a}}$ such that $\psi \restriction F = \mathrm{id}_F$.

Let $a_1, \dots, a_n$ be the roots of f in K_1 and $b_i := \psi(a_i)$ for each $i = 1, \dots, n$. Since

$$f(x) = c\,(x - a_1)^{k_1} \dots (x - a_n)^{k_n}$$

for some $c \in F$ and $k_1, \dots, k_n \in \mathbb{Z}^+$, applying ψ to the coefficients in above equation between polynomials gives

$$f(x) = c\,(x - b_1)^{k_1} \dots (x - b_n)^{k_n}$$

Thus $b_1, \dots, b_n$ are the roots of f in K_2.

Since K_1 and K_2 are splitting fields of f over F, we have $K_1 = F(a_1, \dots, a_n)$ and $K_2 = F(b_1, \dots, b_n)$. Let $\varphi := \psi \restriction K_1$. Since $\varphi \restriction F = \mathrm{id}_F$ and $\varphi(a_i) = b_i$ for each $i = 1, \dots, n$, the image of φ is K_2. □

2.5 Splitting Field of a Set of Polynomials.

Definition. Let F be a field and $\mathscr{F} = \{f_i : i \in I\}$ be a set of nonconstant polynomials over F. The splitting field of $\mathscr{F}$ over F is a field K such that:

1. Each polynomial $f_i(x)$ splits into linear factors over K.

2. If A is the set of all root in K of all f_i, then $K = F(A)$.

Field embeddings. If F and K are fields then the *embedding* of F in K is a ring homomorphism $F \to K$.

Remark. Since fields have only two ideals, any field embedding is injective. It does not have to be surjective. An embedding is surjective if and only if it is an isomorphism.

Embeddings over a subfield. If F is a subfield of the fields K and L and $\varphi : K \to L$ is an embedding, then we say that φ is *over F* when $\varphi \restriction F = \mathrm{id}_F$. If φ is an isomorphism or an automorphism (when $K = L$) and $\varphi \restriction F = \mathrm{id}_F$, then we say that it an isomorphism or automorphism over F.

Theorem. *Let $\mathscr{F} = \{f_i : i \in I\}$ be a family of nonconstant polynomials over F.*

1. *There exists a splitting field of $\mathscr{F}$ over F.*

   Proof. Let F^{a} be an algebraic closure of F and A be the set of all roots of all the polynomials in $\mathscr{F}$. Then $F(A)$ is a splitting field of $\mathscr{F}$ over F. □

2. *If K_1 and K_2 are splitting fields of $\mathscr{F}$ over F then there is an isomorphism $\varphi : K_1 \to K_2$ over F (such that $\varphi \restriction F = id_F$).*

   Proof. Exercise. □

2.6 Homework 2 — due January 18.

Exercise. Prove the second assertion of the theorem in section 2.5.

2.7 Normal Field Extensions.

Motivation. Let $A \subseteq B$ be sets, G be the group of permutations σ of B such that $\sigma\restriction A$ is a permutation of A and H be the subgroup of G consisting of those permutations σ for which $\sigma\restriction A = \mathrm{id}_A$. Then H is a normal subgroup of G.

Theorem. *Let F be a field and $K \subseteq F^{\mathrm{a}}$ be a field extension of F. The following conditions are equivalent.*

1. *Every automorphism of F^{a} over F restricted to K is an automorphism of K.*

2. *Every embedding of K in F^{a} over F is an automorphism of K.*

3. *K is the splitting field of a family of polynomials over F.*

4. *Every irreducible polynomial over F that has a root in K splits over K.*

Proof. We will show that 1. ⇒ 2. ⇒ 1., that 1. ⇒ 3. and that 1. ⇒ 4. ⇒ 1.. The proof that 3. ⇒ 1. is left as an exercise.

1. ⇒ 2. Let $\varphi : K \to F^{\mathrm{a}}$ be an embedding over F. We need to show that the image $L = \varphi(K)$ is equal to K. Since $\varphi : K \to L$ is an isomorphism and F^{a} is the algebraic closure of both K and L, the isomorphism φ can be extended to an automorphism ψ of F^{a}. By 1., the restriction $\psi\restriction K$ is an automorphism of K.

2. ⇒ 1. Every automorphism of F^{a} restricted to K is an embedding of K in F^{a}.

1. ⇒ 3. For each $a \in K$, let f_a be the minimal polynomial of a over F. We will show that K is the splitting field of $\mathscr{F} = \{f_a : a \in K\}$. If A is the set of all roots in K of all the polynomials in $\mathscr{F}$, then $A = K$ so $F(A) = K$. It remains to show that every polynomial in $\mathscr{F}$ splits over F. Suppose, to the contrary, that for some $a \in K$ there is a root $b \in F^{\mathrm{a}} \setminus K$ of f_a. Then there is an isomorphism $\varphi : F(a) \to F(b)$ over F with $\varphi(a) = b$ and φ can be extended to an automorphism ψ of F^{a}. By 1., $\psi\restriction K$ is an automorphism of K. Since $\psi(a) = \varphi(a) = b \notin K$, we have a contradiction.

1. ⇒ 4. Let f be an irreducible polynomial over F with a root a in K. Suppose, to the contrary, that f does not split over K. Then f has a root $b \in F^{\mathrm{a}} \setminus K$. Then a and b have the same minimal polynomial (equal to $c^{-1}f$ where c is the leading coefficient of f) so there is an isomorphism $\varphi : F(a) \to F(b)$ over F with $\varphi(a) = b$. The isomorphism φ can be extended to an automorphism ψ of F^{a}. By 1., $\psi\restriction K$ is an automorphism of K. Since $\psi(a) = \varphi(a) = b \notin K$, we have a contradiction.

4. ⇒ 1. Let φ be an automorphism of F^{a} over F. Let $a \in K$ and f be the minimal polynomial of a over F. By 4., f splits over K. Since φ maps roots of f to roots of f, it follows that $\varphi(a) \in K$. Since f has finitely many roots in K, there is a root b of f in K with $\varphi(b) = a$. Thus $\varphi\restriction K$ is an automorphism of K. □

Definition. A field K satisfying the conditions of the theorem is called a normal extension of F.

Example. Let $F = \mathbb{Q}$ be the field of rational numbers.

1. The field $F\left(\sqrt{2}\right)$ is a normal extension of F.

2. The field $F\left(\sqrt[3]{2}\right)$ is an extension of F that is not normal.

3. The field $F\left(\sqrt[3]{2},\omega\right)$ with $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i\in\mathbb{C}$ is a normal extension of F.

2.8 Homework 3 — due January 23.

Exercise. Prove that 3. ⇒ 1. in the theorem of section 2.7.

3 Separable Field Extensions.

3.1 Separable Degree of a Finite Field Extension.

Definition. Let F be a field and $K\subseteq F^{\mathrm{a}}$ be a finite extension of F ($[K:F]$ is finite). The separable degree of K over F, denoted $[K:F]_s$ is the number of embeddings of K into F^{a} over F.

Lemma. *Let F be a field $a\in F^{\mathrm{a}}$ and $K=F(a)$. Then $[K:F]_s\leq[K:F]$.*

Proof. Let f be the minimal polynomial of a over F and $a_1,\dots,a_n$ be all the roots of f in F^{a}. If φ is an embedding of $F(a)$ into F^{a} over F, then $\varphi(a)\in\left\{a_1,\dots,a_n\right\}$. Since every element of $F(a)$ is of the form $b_0+b_1a+\cdots+b_{m-1}a^{m-1}$ with $b_0,\dots,b_{m-1}\in F$ where $m=\deg\left(f\right)$, the value $\varphi(a)$ uniquely determines φ. For each $i=1,\dots,n$ the elements a and a_i have the same minimal polynomial over F so there exists an embedding $F(a)\to F^{\mathrm{a}}$ over F mapping a to a_i. $[K:F]_s=n$. Since $n\leq\deg\left(f\right)$ and $[K:F]=\deg\left(f\right)$, the result follows. □

Remark. The proof above shows that $[K:F]_s=[K:F]$ unless the minimal polynomial f of a over F has multiple roots in F^{a}. We will show later that such a situation is possible.

Proposition. *Let F be a field and $E\subseteq K\subseteq F^{\mathrm{a}}$ be finite extensions of F. Then $[K:F]_s=[K:E]_s[E:F]_s$.*

Proof. Let $\sigma_1,\dots,\sigma_n$ be all the embeddings of E in F^{a} over F where $n=[E:F]_s$. For each $i=1,\dots,n$, let $\varphi_{i1},\dots,\varphi_{im_i}:K\to F^{\mathrm{a}}$ be all the extensions of σ_i to an embedding of K in F^{a}. If $i\neq i'$, then for arbitrary j we have $\varphi_{ij}\restriction E=\sigma_i$ and for arbitrary j' we have $\varphi_{i'j'}\restriction E=\sigma_{i'}\neq\sigma_i$ implying that $\varphi_{ij}\neq\varphi_{i'j'}$. If $\psi:K\to F^{\mathrm{a}}$ is any embedding over F, then $\psi\restriction E$ is an embedding of E in F^{a} over F so $\psi=\varphi_{ij}$ for some i and j. Thus to complete the proof of $[K:F]_s=[K:E]_s[E:F]_s$, it suffices to show that $m_i=[K:E]_s$ for each $i=1,\dots,n$.

Let $i\in\{1,\dots,n\}$ be fixed and denote $\varphi=\varphi_{i1}$. Since $\varphi\restriction E=\varphi_{ij}\restriction E$ for any $j\in\left\{1,\dots,m_i\right\}$, it follows that $\varphi(b)=\varphi_{ij}(b)$ for any $b\in E$ and consequently $\left(\varphi^{-1}\circ\varphi_{ij}\right)\restriction E=\mathrm{id}_E$. Thus for each $j=1,\dots,m_i$, the map $\varphi^{-1}\circ\varphi_{ij}$ is an embedding of K in F^{a} over E. Moreover, if $j\neq j'$, then $\varphi^{-1}\circ\varphi_{ij}\neq\varphi^{-1}\circ\varphi_{ij'}$. Thus $m_i=[K:E]_s$. □

Theorem. *Let F be a field and $K\subseteq F^{\mathrm{a}}$ be finite over F. Then $[K:F]_s\leq[K:F]$.*

Proof. There are $a_1,\dots,a_n \in K$ such that $K = F(a_1,\dots,a_n)$. Let $F_0 = F$ and $F_i = F_{i-1}(a_i)$ for each $i = 1,\dots,n$. Then

$$[K:F]_s = [F_n:F_0]_s = [F_n:F_{n-1}]_s\,[F_{n-1}:F_{n-2}]_s \dots [F_2:F_1]_s\,[F_1:F_0]_s\,.$$

Since

$$[K:F] = [F_n:F_0] = [F_n:F_{n-1}]\,[F_{n-1}:F_{n-2}]\dots[F_2:F_1]\,[F_1:F_0]\,,$$

and since $[F_i:F_{i-1}]_s \le [F_i:F_{i-1}]$ for each $i = 1,\dots,n$, it follows that $[K:F]_s \le [K:F]$. □

3.2 Separable Field Extensions.

Finite separable field extensions.

Definition. A finite field extension $K \supseteq F$ is *separable* iff $[K:F]_s = [K:F]$.

Remark. Let $K \supseteq F$ be a finite extension and $a_1,\dots,a_n \in K$ be such that $K = F(a_1,\dots,a_n)$. If $F_0 = F$ and $F_i = F_{i-1}(a_i)$ for each $i = 1,\dots,n$, then K is separable over F if and only if F_i is separable over F_{i-1} for every $i = 1,\dots,n$.

Separable elements.

Definition. Let $K \supseteq F$ be a field extension and $a \in K$ be algebraic over F. We say that a is *separable* over F iff $F(a)$ is separable over F.

Remark. a is separable over F iff the minimal polynomial of a over F has no multiple roots in F^{a}.

Separable polynomials.

Definition. Let F be field. A polynomial f over F is *separable* iff it has no multiple roots in F^{a}.

Proposition. *Let F be a field.*

1. *If a polynomial f over F is separable, then any of its roots is separable over F.*
2. *If $K \subseteq F^{\mathrm{a}}$ is an extension of F, then any element of F^{a} that is separable over F is separable over K.*

Proof. 1. is clear and the proof of 2. is an exercise. □

Theorem. *Let K be a finite extension of a field F. The following conditions are equivalent.*

1. *$[K:F] = [K:F]_s$, that is K is separable over F.*
2. *Each element of K is separable over F.*
3. *$K = F(A)$ for some subset $A \subseteq K$ whose elements are separable over F.*

Proof. 1. ⇒ 2. Suppose that K is separable over F and $a \in K$. Then $F \subseteq F(a) \subseteq K$ and

$$[K:F]_s = [K:F(a)]_s\,[F(a):F]_s \le [K:F(a)]\,[F(a):F] = [K:F].$$

Since $[K:F]_s = [K:F]$, it follows that $[F(a):F]_s = [F(a):F]$ so a is separable over F.

2. ⇒ 3. Take $A = K$.

3. ⇒ 1. Since K is finite over F, we have $K = F(a_1,\ldots,a_n)$ for some $a_1,\ldots,a_n \in A$. Then a_{i+1} is separable over F, hence over $F(a_1,\ldots,a_i)$, for each $i = 1,\ldots,n-1$. If $F_0 = F$ and $F_i = F_{i-1}(a_i)$ for each $i = 1,\ldots,n$, then each F_i is separable over F_{i-1} implying that K is separable over F. □

Separable field extensions.

Definition. Let K be an algebraic extension of a field F. We say that K is *separable* over F iff every element of K is separable over F.

Corollary. *Let K be an algebraic extension of a field F. The following conditions are equivalent.*

1. *Every element of K is separable over F, that is K is separable over F.*
2. *If E is a subfield of K containing F and finite over F then $[E:F]_s = [E:F]$ (that is, E is separable over F).*
3. *There is a subset $A \subseteq K$ consisting of elements that are separable over F such that $K = F(A)$.*

Proof. 1. ⇒ 2. Assume that K is separable over F and $E \subseteq K$ is a finite extension of F. Since every element of E is separable over F, the field E is separable over F.

2. ⇒ 1. Assume that every subfield of K containing F that is finite over F is separable over F. Let $a \in K$. Then $F(a)$ is a finite extension of F so it is separable over F. Thus a is separable over F. Since every element of K is separable over F, the field K is separable over F.

1. ⇒ 3. Take $A = K$.

3. ⇒ 1. Assume $A \subseteq K$ is such that every element of A is separable over F and $K = F(A)$. Let $\mathscr{B}$ be the family of all finite subsets of A. Note that $K = \bigcup_{B\in\mathscr{B}} F(B)$. (The inclusion $\bigcup_{B\in\mathscr{B}} F(B) \subseteq K$ is obvious and the inclusion $K \subseteq \bigcup_{B\in\mathscr{B}} F(B)$ follows from the observation that $\bigcup_{B\in\mathscr{B}} F(B)$ is a subfield of K^{a} containing A.) Since $F(B)$ is finite dimensional over F and each element of B is separable over F, it follows that every element of $F(B)$ is separable over F. Since any element of K belongs to $F(B)$ for some $B \in \mathscr{B}$, the proof is complete. □

3.3 Homework 4 — due January 28.

Exercise. Prove part (2) of the proposition in section 3.2.

4 Non-separable Extensions Exist.

4.1 Field of Fractions of an Integral Domain.

Definition. Let D be an integral domain. A field of fraction of D is a field F that extends D (that is D is a subring of F) such that for every $a \in F$ there are $b, c \in D$ with $a = bc^{-1}$.

Proposition. *Let D be an integral domain, F be a field of fractions of D and $f : D \to K$ be an embedding (injective homomorphism) where K is a field. Then there is exactly one extension of f to an embedding $g : F \to K$.*

Proof. For $a \in F$ there are $b, c \in D$ such that $a = bc^{-1}$. Define $g(a) = f(b)f(c)^{-1}$.

(1) g is well-defined.

Proof. Suppose $a = b_1c_1^{-1} = b_2c_2^{-1}$. Then $b_1c_2 = b_2c_1$ so $f(b_1)f(c_2) = f(b_2)f(c_1)$. Thus $f(b_1)f(c_1)^{-1} = f(b_2)f(c_2)^{-1}$. □

(2) g is a homomorphism.

Proof. Exercise. □

(3) If $h : F \to K$ is another embedding extending f, then $h = g$.

Proof. If $a \in F$ with $a = bc^{-1}$ where $b, c \in D$, then $b = ac$ so

$$f(b) = h(b) = h(a)h(c) = h(a)f(c),$$

implying that $h(a) = f(b)f(c)^{-1}$. □

□

Corollary. *Let D be an integral domain and F_1, F_2 be fields of fractions of D. Then there is an isomorphism $f : F_1 \to F_2$ such that $f \restriction D = id_D$.*

Theorem. *For every integral domain D there exists a field of fractions of D.*

Proof. Let $D^* = D \setminus \{0\}$ and $\sim$ be the equivalence relation on $D \times D^*$ defined by $(a, b) \sim (c, d)$ iff $ad = bc$. Denote by $\frac{a}{b}$ the equivalence class of $\sim$ that contains the pair $(a, b) \in D \times D^*$. Let

$$F = \left\{ \frac{a}{b} : (a, b) \in D \times D^* \right\}.$$

Define addition on F by $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and multiplication by $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$. It is routine to verify that the addition and multiplication in F are well-defined and that F is a field.

Let $f : D \to F$ be defined by $f(a) = \frac{a}{1}$. Then f is an embedding so the element a of D can be identified with its image $f(a)$ in F. After this identification D becomes a subring of F. It is clear that F is a field of fractions of D. □

4.2 Homework 5 — due January 30.

Exercise. Prove part (2) of the proof of the proposition in section 4.1.

4.3 Derivative of a Polynomial and Multiple Roots.

Definition. Let F be a field and $f(x) = a_n x^n + \cdots + a_0$ be a polynomial over F. The *derivative* f' of f is defined by

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1.$$

Remark. If f, g are polynomials over a field F, then $\left(fg\right)' = f'g + fg'$.

Multiple roots of a polynomial. Let F be a field, f be a polynomial over F and $a \in F^{\mathrm{a}}$ be a root of f. We say that a is a *multiple root* if $(x-a)^2$ divides $f(x)$ in $F^{\mathrm{a}}[x]$.

Proposition. *Let F be a field and f be a polynomial over F. Then f has no multiple roots in F^{a} if and only if $f(x)$ and $f'(x)$ are relatively prime in $F[x]$.*

Proof. Assume that $f(x)$ and $f'(x)$ are relatively prime in $F[x]$. Since $F[x]$ is a principal ideal domain, there are $h(x)$ and $k(x)$ in $F[x]$ such that

$$1 = hf + kf'.$$

Suppose, to the contrary, that f has a multiple root $a \in F^{\mathrm{a}}$. Then $f(x) = (x-a)^2 g(x)$ for some $g(x) \in F^{\mathrm{a}}[x]$. Thus

$$f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x),$$

so a is a root of f' as well. Then

$$1 = h(a)f(a) + k(a)f'(a) = 0,$$

which is a contradiction.

Assume that f has no multiple root in F^{a}. If $a \in F^{\mathrm{a}}$ is a root of f, then $f(x) = (x-a)g(x)$ for some $g(x) \in F^{\mathrm{a}}[x]$ and $g(a) \neq 0$. Thus $f'(x) = g(x) + (x-a)g'(x)$ and so $f'(a) = g(a) \neq 0$. Thus $f(x)$ and $f'(x)$ have no common roots in F^{a}. Suppose, to the contrary, that $f(x)$ and $f'(x)$ have a non-constant common factor $h(x)$ in $F[x]$. Then h has a root in F^{a} which is a common root of f and f' giving us a contradiction. Thus $f(x)$ and $f'(x)$ are relatively prime in $F[x]$. □

Corollary. *Let F be a field and $f(x) \in F[x]$ be irreducible. Then f is separable if and only if $f'(x) \neq 0$.*

Proof. Assume that $f'(x)$ is nonzero and $\deg\left(f\right) = n$. Then $\deg\left(f'\right) < n$ so any common divisor $g(x)$ of $f(x)$ and $f'(x)$ in $F[x]$ must have degree smaller than n. Since f is irreducible, $g(x)$ is a constant polynomial so $f(x)$ and $f'(x)$ are relatively prime. Thus f has no multiple roots and hence is separable.

If f is separable, then it has no multiple roots so f and f' are relatively prime. Thus $f' \neq 0$. □

4.4 An Algebraic Non-separable Extension.

Irreducible and prime elements of an integral domain.

Definition. Let D be an integral domain and $a \in D$. Then a is *irreducible* iff it is not zero, not a unit and if $a = bc$ for some $b, c \in D$, then b or c is a unit. The element a is *prime* iff it is not zero, not a unit and whenever $a \mid bc$ for some $b, c \in D$, then $a \mid b$ or $a \mid c$.

Primitive polynomials.

Definition. Let D be an integral domain. A polynomial $f(x) \in D[x]$ is *primitive* iff the coefficients of f are relatively prime (have no common divisors except for units).

Eisenstein criterion.

Theorem. *Let D be an integral domain with field of fractions F and*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in D[x]$$

be a nonzero polynomial. Let $p \in D$ be a prime element such that $p \mid a_i$ for every $i = 0, 1, \ldots, n-1$ but $p \nmid a_n$ and $p^2 \nmid a_0$.

1. *If moreover $f(x)$ is primitive, then it is irreducible in $D[x]$.*
2. *If D is a unique factorization domain, then $f(x)$ is irreducible in $F[x]$.*

Example. Let $D = \mathbb{Z}_2[x]$ be the integral domain of polynomials with coefficients in the field $\mathbb{Z}_2$ and F be the field of fractions of D. Since D is a principal ideal domain, it is a unique factorization domain. The element $x \in D$ is irreducible hence it is prime. Thus the polynomial $f\left(y\right) = y^2 - x \in D\left[y\right]$ is irreducible in $F\left[y\right]$. Since $f'\left(y\right) = 2y = 0$, the polynomials f and f' are not relatively prime and so f has multiple roots. Explicitly, if $a \in F^{\mathrm{a}}$ is a root of $f\left(y\right)$, then $a^2 = x$ and $f\left(y\right) = \left(y - a\right)^2$.

Thus f is an irreducible polynomial over F that is not separable. The field $F(a)$ is an algebraic extension of F that is not separable over F. We have $[F(a) : F] = 2$ but $[F(a) : F]_s = 1$.

4.5 Homework 6 — due February 1.

Exercise. Let p be a prime, $D = \mathbb{Z}_p[x]$ and F be the field of fractions of D. Then the polynomial $y^p - x$ is irreducible over F but is not separable.

5 When Every Algebraic Extension is Separable.

5.1 Characteristic of a Ring

Definition. Let R be a ring and $\varphi : \mathbb{Z} \to R$ be the ring homomorphism defined by $\varphi(n) = n \cdot 1_R$. The kernel of φ is a principal ideal of $\mathbb{Z}$ with a unique non-negative generator which is called the *characteristic* of R. The characteristic of R will be denoted by $\mathrm{char}(R)$.

Remarks.

1. The characteristic of a ring R is the smallest positive integer n such that

$$\underbrace{1_R + 1_R + \cdots + 1_R}_{n} = 0_R$$

   is such n exists and is equal 0 otherwise.

2. The only ring with characteristic 1 is the trivial ring.

Proposition. *If D is an integral domain, then the characteristic of D is either 0 or a prime integer.*

Proof. Suppose $m \neq 0$ is the characteristic of D. Suppose $m = k \cdot \ell$, where $k, \ell \geq 2$. Let $\varphi : \mathbb{Z} \to D$ be the ring homomorphism defined by $\varphi(n) = n \cdot 1_D$. Then $0_D = \varphi(k \cdot \ell) = \varphi(k)\varphi(\ell)$ implying that $\varphi(k)$ or $\varphi(\ell)$ equals 0_D, which is a contradiction. □

5.2 Prime Subfield.

Definition. Let K be a field. The *prime subfield* of K is the intersection of all subfields of K.

Remark. The prime subfield always exists.

Proposition. *Let K be a field with a prime subfield F. If $char(K) = 0$, then F is isomorphic to $\mathbb{Q}$, if $char(K) = p$ where p is a prime, then F is isomorphic to $\mathbb{Z}_p$.*

Proof. Let $\varphi : \mathbb{Z} \to K$ be the ring homomorphism defined by $\varphi(n) = n \cdot 1_K$. If the characteristic of K is 0, then φ is injective and φ extends uniquely to an embedding $\psi : \mathbb{Q} \to K$. Since every subfield E of K contains $\psi(\mathbb{Q})$, we have $F = \psi(\mathbb{Q})$ so F is isomorphic to $\mathbb{Q}$.

If $\operatorname{char}(K) = p$ is a prime, then $\ker(\varphi) = p\mathbb{Z}$ and the Fundamental Homomorphism Theorem for rings implies that the image $\varphi(\mathbb{Z})$ is isomorphic to the quotient ring $\mathbb{Z}/p\mathbb{Z}$ which is isomorphic to $\mathbb{Z}_p$. Since every subfield E of K contains $\varphi(\mathbb{Z})$, it follows that $F = \varphi(\mathbb{Z})$ is isomorphic to $\mathbb{Z}_p$. □

5.3 Homework 7 — due February 4.

Exercise. Let K be a field, F be the prime subfield of K and φ be any automorphism of K. Prove that φ is over F, that is, prove that $\varphi(a) = a$ for every $a \in F$.

5.4 Perfect Fields.

Definition. A field F is *perfect* iff any algebraic extension of F is separable over F.

Remark. A field F is perfect if and only if every irreducible polynomial over F is separable.

Theorem. *Any field of characteristic* 0 *is perfect.*

Proof. Let F be a field of characteristic 0 and

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

be irreducible where $n \geq 1$ and $a_n \neq 0$. Then $f'(x) = n a_n x^{n-1} + \cdots + a_1$. Since $\text{char}(F) = 0$ it follows that $n a_n \neq 0$. Thus $f'(x) \neq 0$ and consequently f is separable. Since every irreducible polynomial over F is separable, the field F is perfect. □

Remark. We will show later that every finite field is perfect.

6 Finite Fields.

6.1 Possible Cardinalities of Finite Fields.

Theorem. *The cardinality of a finite field is a positive power of a prime integer.*

Proof. Let K be a finite field and F be its prime subfield. Since F is finite, it is isomorphic to $\mathbb{Z}_p$ for some prime p. Let $b_1, \ldots, b_n \in K$ be a basis of K over F. Since every element is a unique linear combination of $b_1, \ldots, b_n$ with coefficients from F, we have $|K| = p^n$. □

6.2 Uniqueness of Finite Fields.

Proposition (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.*

Proof. If $a, b \in G$, then the function $f : aH \to bH$ defined by $f(ah) = bh$ is a bijection. Thus any two left cosets of H in G have the same number of elements. Since the left cosets of H in G form a partition of G, the result follows. □

The multiplicative group of a field.

Definition. Let F be a field. The *multiplicative group* of F is the group $F^* = F \setminus \{0\}$ under multiplication.

Theorem. *Let K be a finite field of cardinality p^n. Then K is a splitting field of the polynomial $x^{p^n} - x$ over its prime subfield. In particular, all fields of cardinality p^n are isomorphic.*

Proof. The order of any $a \in K^*$ in the group K^* is a divisor of $|K^*| = p^n - 1$ so $a^{p^n-1} = 1$ and $a^{p^n} = a$. Since $0^{p^n} = 0$ as well, all the elements of K are roots of the polynomial $f(x) = x^{p^n} - x$. Since f can have at most p^n roots in K^{a}, it splits over K. Since each element of K is a root of f, the field K is a splitting field of f over the prime subfield of K. □

6.3 Existence of Finite Fields.

Lemma. *If K is a field of prime characteristic p and $a, b \in K$, then $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ for any positive integer n.*

Proof. By binomial formula

$$(a+b)^p = \binom{p}{0} a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + \binom{p}{p} b^p.$$

If $1 \le i \le p-1$, then

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

is divisible by p since the numerator is divisible by p but the denominator is not. Thus $(a+b)^p = a^p + b^p$.

We complete the proof using induction. Suppose that $(a+b)^{p^{n-1}} = a^{p^{n-1}} + b^{p^{n-1}}$. Then

$$(a+b)^{p^n} = \left((a+b)^{p^{n-1}}\right)^p = \left(a^{p^{n-1}} + b^{p^{n-1}}\right)^p = \left(a^{p^{n-1}}\right)^p + \left(b^{p^{n-1}}\right)^p = a^{p^n} + b^{p^n}.$$

□

Proposition. *If a nonempty subset H of a finite group G is closed under the group operation, then H is a subgroup of G.*

Proof. Exercise. □

Theorem. *For every prime integer p and any positive integer n there exists a field with p^n elements.*

Proof. Let F be the field $\mathbb{Z}_p$ and $f(x)$ be the polynomial $x^{p^n} - x$ over F. Since $f'(x) = -1$, the polynomial $f(x)$ has p^n distinct roots in $\mathbb{Z}_p^{\mathrm{a}}$. Let K be the splitting field of $f(x)$ over F and

$$L = \left\{a \in K : f(a) = 0\right\}.$$

Since L has p^n elements, to complete the proof, it suffices to show that L is a subfield of K. Since L contains 0 and 1 an is finite, the proposition implies that we only need to show that L is closed under addition and multiplication. In case of multiplication, it is obvious, and in case of addition it follows from the lemma. □

Notation. For a prime p and a positive integer n the unique (up to isomorphism) field with $q = p^n$ elements is denoted by $\mathbb{F}_q$.

6.4 Homework 8 — due February 6.

Exercise. Prove the proposition in section 6.3.

6.5 Perfect Fields of Prime Characteristic.

Frobenius mapping.

Definition. Let F be a field of prime characteristic p. The *Frobenius mapping* is the function $\varphi : F \to F$ defined by $\varphi(a) = a^p$.

Remark. The Frobenius mapping φ is an embedding and if F is finite, then it is an isomorphism. Moreover, the restriction of φ to the prime subfield $\mathbb{F}_p$ of F is the identity on $\mathbb{F}_p$.

Lemma. *Let F be a field of prime characteristic p and*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$$

We have $f'(x) = 0$ if and only if $a_i = 0$ for every i which is not divisible by p.

Theorem. *Let F be a field of prime characteristic p. If the Frobenius mapping $F \to F$ is an isomorphism, then F is perfect.*

Proof. Suppose that the Frobenius mapping is an isomorphism. Let K be an algebraic extension of F and $a \in K$. We want to show that a is separable over F. Let f be the minimal polynomial over F. Suppose, to the contrary, that a is not separable over F. Then f has multiple roots in K^{a} so $f' = 0$. Thus

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{kp} x^{kp}.$$

Since the Frobenius mapping $F \to F$ is surjective, for each $i = 0, \ldots, k$, there is $b_i \in F$ such that $a_{ip} = b_i^p$. Thus

$$f(x) = b_0^p + b_1^p x^p + b_2^p x^{2p} \cdots + b_k^p x^{kp} = \left(b_0 + b_1 x + b_2 x^2 + \cdots + b_k x^k\right)^p,$$

contradicting the irreducibility of f over F. Since any algebraic extension of F is separable, the field F is perfect. □

Corollary. *Any finite field is perfect. Any field of prime characteristic that is algebraic over its prime field is perfect.*

Proof. Exercise. □

Proposition. *Let F be a field of prime characteristic p such that the Frobenius map $\varphi : F \to F$ is not surjective and $a \in F$ be such that $f(x) = x^p - a \in F[x]$ has no roots in F. Then $f(x)$ is irreducible but not separable in $F[x]$. In particular, F is not perfect.*

Proof. Clearly $f(x)$ is not separable so we only need to show that it is irreducible. Let $b \in F^{\mathrm{a}}$ be a root of f. Then $f(x) = (x-b)^p$ and the minimal polynomial $g(x)$ of b over F is a divisor of $f(x)$ so $g(x) = (x-b)^d$ for some integer d with $1 \le d \le p$. We need to show that $d = p$. Suppose $d < p$. Then $g(x) = x^d - d\,b\,x^{d-1} + \ldots$ implying that $d\,b \in F$ and consequently that $b \in F$ which is a contradiction. □

6.6 Homework 9 — due February 8.

Exercise. Prove the corollary in section 6.5.

6.7 Multiplicative Group of a Finite Field.

Cyclic groups.

Definition. A group G is *cyclic* iff there is $a \in G$ such that a generates G, that is no proper subgroup of G contains a.

Remark. Any cyclic group is isomorphic either to the additive group $\mathbb{Z}$ or the additive group $\mathbb{Z}_n$ for some positive integer n.

Theorem. *If F is a field and G is a finite subgroup of the multiplicative group F^*, then G is cyclic. In particular, if F is finite, then F^* is cyclic.*

Proof. Let $a \in G$ be an element of maximal order in G. If the order m of a equals $n = |G|$, then a generates G so G is cyclic. Otherwise, since the order of any element of G divides m (exercise), $b^m = 1$ for any element $b \in G$ and the polynomial $x^m - 1$ has $n > m$ roots, which is a contradiction. □

6.8 Homework 10 — due February 11.

Exercise. Let G be a finite abelian group of order n and $a \in G$ be an element of the maximal order. If the order of a is m, then the order of any element of G is a divisor of m.

7 The Primitive Element Theorem.

7.1 Primitive elements.

Remark. Recall that if F is a field, K is an extension of F and $a \in K$ is algebraic over F, then $F(a)$ is finite over F. Also, every finite extension is algebraic.

Definition. Let K be a finite extension of a field F. If $K = F(a)$ for some $a \in K$, then we say that a is a *primitive element* of K over F.

7.2 A Finite Extension with no Primitive Element.

Example. Let F be the field of fractions of the integral domain $\mathbb{F}_2[x, y]$ and K be the splitting field of the polynomial

$$(z^2 - x)(z^2 - y) \in F[z]$$

over F. If $a \in K$ is a root of $z^2 - x$ and $b \in K$ is a root of $z^2 - y$, then $K = F(a, b)$. Clearly, K is finite over F. However, K has no primitive element over F.

Proof. Suppose, to the contrary, that there exists $c \in K$ such that $K = F(c)$. Since $z^2 - x$ is irreducible over F and $z^2 - y$ is irreducible over $F(a)$, it follows that $1, a, b, ab$ is a basis of K over F. Thus we have

$$c = \alpha + \beta a + \gamma b + \delta ab$$

with $\alpha, \beta, \gamma, \delta \in F$ and

$$c^2 = \alpha^2 + \beta^2 a^2 + \gamma^2 b^2 + \delta^2 a^2 b^2 = \alpha^2 + \beta^2 x + \gamma^2 y + \delta^2 xy \in F.$$

Thus c is a root of a quadratic polynomial over F implying that $[F(c) : F] \leq 2$. Since $[K : F] = 4$ we have a contradiction. □

Remark. Note that if $\alpha, \beta \in F$ are distinct and we take $c = a + \alpha b$ and $d = a + \beta b$, then $a, b \in F(c, d)$ so $K = F(c, d)$. Since $K \neq F(c)$ and $K \neq F(d)$ it follows that $F(c) \neq F(d)$. Since F is infinite, we have infinitely many intermediate fields E, (with $F \subseteq E \subseteq K$).

7.3 The Main Result.

Theorem. *Let K be a finite extension of a field F.*

1. *The following conditions are equivalent*

   (a) K has a primitive element over F.

   (b) The number of intermediate fields E (such that $F \subseteq E \subseteq K$) is finite.

   Proof. (b) ⇒ (a)

   Assume that the number of intermediate fields is finite. If F is finite, then K is finite so K^* is cyclic and $K = F(a)$ where a is a generator of the group K^*. Thus we can assume that F is infinite.

   Let $a, b \in K$. There are only finitely many fields of the form $F(a + cb)$ with $c \in F$. Since F is infinite, it follows that $F(a + c_1 b) = F(a + c_2 b)$ for some $c_1, c_2 \in F$ with $c_1 \neq c_2$. Thus the field $F(a + c_1 b)$ contains both $a + c_1 b$ and $a + c_2 b$. Thus

   $$(a + c_1 b) - (a + c_2 b) = (c_1 - c_2) b \in F(a + c_1 b).$$

   Since $c_1 - c_2 \neq 0$, it follows that $b \in F(a + c_1 b)$ and hence also $a \in F(a + c_1 b)$ implying that $F(a, b) = F(a + c_1 b)$.

   Since K is a finite extension of F, there are $a_1, \ldots, a_n \in K$ with $K = F(a_1, \ldots, a_n)$. Assume that n is as small as possible. If $n \geq 2$, then there is $c \in F$ such that $F(a_1, a_2) = F(a')$, where $a' = a_1 + c a_2$. Thus $K = F(a', a_3, \ldots, a_n)$ contradicting the minimality of n. Thus $n = 1$ and $K = F(a)$ for some $a \in K$.

   (a) ⇒ (b)

   Assume that $K = F(a)$ for some $a \in K$ and let f be the minimal polynomial of a over F. Let $\mathscr{E} = \{E : F \subseteq E \subseteq K\}$ be the set of intermediate fields. If $E \in \mathscr{E}$ and f_E is the minimal polynomial of a over E, then f_E divides f. Since $F^{\mathrm{a}}[x]$ is a unique factorization domain, f has only finitely many different monic divisors in $F^{\mathrm{a}}[x]$. Consider the assignment of the polynomial f_E to the field $E \in \mathscr{E}$. To show that $\mathscr{E}$ is finite, it suffices to show that this assignment is injective.

Suppose that $E, E' \in \mathscr{E}$ and $f_E = f_{E'}$. Let $f_E = a_0 + a_1 x + \cdots + a_n x^n$ and $L = F(a_0, \ldots, a_n)$. Since f_E is irreducible over E and $L \subseteq E$ it follows that f_E is irreducible over L. Thus $f_L = f_E$ implying that $[L : F] = [E : F]$. Thus $f_L = f_E$ implying that $[L : F] = [E : F]$. Since $L \subseteq E$ we must have $L = E$. Similarly $L = E'$ implying that $E = E'$ and consequently that the assignment $E \mapsto f_E$ is injective. □

2. *If K is separable over F then it has a primitive element over F.*

Proof. Without loss of generality, F is infinite. We can also assume that $K = F(a, b)$ for some $a, b \in K$ since otherwise we can use induction. Let $n = [K : F]_s = [K : F]$ and $\sigma_1, \ldots, \sigma_n$ be all distinct embeddings of K in F^{a}. Consider the polynomial

$$f(x) = \prod_{i \neq j} \big(\sigma_i(a) - \sigma_j(a) + \big(\sigma_i(b) - \sigma_j(b)\big) x\big).$$

If $i \neq j$, then either $\sigma_i(a) \neq \sigma_j(a)$ or $\sigma_i(b) \neq \sigma_j(b)$. Thus each factor in the above factorization of f is nonzero implying that f is nonzero and since F is infinite, there is $c \in F$ such that $f(c) \neq 0$. Thus if $i \neq j$, then

$$\sigma_i(a + cb) = \sigma_i(a) + c\sigma_i(b) \neq \sigma_j(a) + c\sigma_j(b) = \sigma_j(a + cb).$$

If $d = a + cb$, then all the elements $\sigma_1(d), \ldots, \sigma_n(d)$ are distinct. If g is the minimal polynomial of d over F, then $\sigma_1(d), \ldots, \sigma_n(d)$ are all roots of g so the degree of g is at least n. Thus $[F(d) : F] \geq n$ implying that $F(d) = K$. □

8 Introduction to Galois Theory.

8.1 Closure Operators.

Definition. Let X be a set. A *closure operator* on X is a function $\Gamma : \mathscr{P}(X) \to \mathscr{P}(X)$ where $\mathscr{P}(X)$ is the family of all subsets of X, such that for every $A, B \subseteq X$ we have:

1. $A \subseteq \Gamma(A)$;
2. $A \subseteq B$ implies that $\Gamma(A) \subseteq \Gamma(B)$;
3. $\Gamma(A) = \Gamma(\Gamma(A))$.

A subset $A \subseteq X$ is said to be Γ-*closed* iff $\Gamma(A) = A$.

Examples of closure operators.

1. Let G be a group and for any $A \subseteq G$ let $\Gamma_1(A)$ be the smallest subgroup of G containing A. Then Γ_1 is a closure operator on G. A subset $H \subseteq G$ is Γ_1-closed if and only if H is a subgroup of G.

2. Let G be a group and for any $A \subseteq G$ let $\Gamma_2(A)$ be the smallest normal subgroup of G containing A. Then Γ_2 is a closure operator on G. A subset $H \subseteq G$ is Γ_2-closed if and only if H is a normal subgroup of G.

3. Let K be a field and for $A \subseteq K$ let $\Gamma_3(A)$ be the smallest subfield of K containing A. Then Γ_3 is a closure operator on K. A subset F of K is Γ_3-closed if and only if F is a subfield of K.

4. Let X be a topological space and for $A \subseteq X$ let $\Gamma_4(A)$ be the closure of A with respect to the topology on X. Then Γ_4 is a closure operator on X. A subset Y of X is Γ_4-closed if and only if Y is closed with respect to the topology on X.

5. Let X be a set and for $A \subseteq X$ let $\Gamma_5(A) = A$. Then Γ_5 is a closure operator on X and any subset of X is Γ_5-closed.

6. Let X be a set and for $A \subseteq X$ let $\Gamma_6(A) = X$. Then Γ_6 is a closure operator on X and the only Γ_6-closed subset of X is X itself.

Proposition. *Let Γ be a closure operator on a set X and $\mathscr{C}$ be the family of all Γ-closed subsets of X. If $\mathscr{F} \subseteq \mathscr{C}$ is a subfamily of $\mathscr{C}$, then the intersection $\bigcap \mathscr{F} = \bigcap_{A \in \mathscr{F}} A$ of all the sets in $\mathscr{F}$ belongs to $\mathscr{C}$. (We assume here that if $\mathscr{F} = \varnothing$, then $\bigcap \mathscr{F} = X$.)*

Proof. Exercise. □

Remark. Let Γ be a closure operator on a set X and $\mathscr{C}$ be the family of all Γ-closed subsets of X.

1. If $\mathscr{F} \subseteq \mathscr{C}$ then the intersection $\bigcap \mathscr{F}$ is the greatest lower bound in $\mathscr{C}$ on $\mathscr{F}$ with respect to the inclusion relation.

2. If $\mathscr{F} \subseteq \mathscr{C}$ then the union $\bigcup \mathscr{F} = \bigcup_{A \in \mathscr{F}} A$ of all sets in $\mathscr{F}$ may not belong to $\mathscr{C}$.

The join operation for a family of subsets.

Definition. Let Γ be a closure operator on a set X and $\mathscr{C}$ be the family of all Γ-closed subsets of X. If $\mathscr{F} \subseteq \mathscr{C}$, then the *join* of $\mathscr{F}$ denoted $\bigvee \mathscr{F}$ is the closure $\Gamma\left(\bigcup \mathscr{F}\right)$ of the union of $\mathscr{F}$.

Remark. If $\mathscr{F} \subseteq \mathscr{C}$ then the join $\bigvee \mathscr{F}$ is the least upper bound in $\mathscr{C}$ on $\mathscr{F}$ with respect to the inclusion relation.

Proof. Note that $\bigvee \mathscr{F}$ belongs to $\mathscr{C}$ since

$$\Gamma\left(\bigvee \mathscr{F}\right) = \Gamma\left(\Gamma\left(\bigcup \mathscr{F}\right)\right) = \Gamma\left(\bigcup \mathscr{F}\right) = \bigvee \mathscr{F}.$$

The set $\bigvee \mathscr{F}$ is an upper bound on $\mathscr{F}$ since for every $A \in \mathscr{F}$ we have

$$A \subseteq \bigcup \mathscr{F} \subseteq \Gamma\left(\bigcup \mathscr{F}\right) = \bigvee \mathscr{F}.$$

It remains to show that $\bigvee \mathscr{F}$ is the least upper bound on $\mathscr{F}$. Suppose that $B \in \mathscr{C}$ is an upper bound on $\mathscr{F}$. Then $\bigcup \mathscr{F} \subseteq B$ which implies that

$$\bigvee \mathscr{F} = \Gamma\left(\bigcup \mathscr{F}\right) \subseteq \Gamma(B) = B.$$

Since $\bigvee \mathscr{F} \subseteq B$ for any $B \in \mathscr{C}$ that is an upper bound on $\mathscr{F}$, it follows that $\bigvee \mathscr{F}$ is the least upper bound on $\mathscr{F}$. □

Example. Let K be a field and $\mathscr{F}$ be a family of subfields of K. Consider the closure operator Γ_3 on K from the example above. Then the join $\bigvee \mathscr{F}$ is the smallest subfield of K containing all the subfields from $\mathscr{F}$.

Remark. A partially ordered set S such that for every subset $T \subseteq S$ there exists the least upper bound and the greatest lower bound on T in S is called a *complete lattice*. Thus, given a closure operator Γ on a set X, the family of Γ-closed subsets of X ordered by inclusion is a complete lattice.

8.2 Homework 11 — due February 15.

Exercise. Prove the proposition in section 8.1.

8.3 Abstract Galois Connections.

Definition. Let X and Y be sets and $R \subseteq X \times Y$ be a relation. Let $\sigma : \mathscr{P}(X) \to \mathscr{P}(Y)$ be the function such that $b \in \sigma(A)$ iff aRb for every $a \in A$. Similarly, let $\pi : \mathscr{P}(Y) \to \mathscr{P}(X)$ be such that $a \in \pi(B)$ iff aRb for every $b \in B$. We will say that the functions σ and π establish the *Galois connection* (between subsets of X and subsets of Y) determined by R.

Remark. The functions σ and π reverse the inclusion relation, that is, if $A' \subseteq A \subseteq X$ then $\sigma(A) \subseteq \sigma(A')$ and if $B' \subseteq B \subseteq Y$ then $\pi(B) \subseteq \pi(B')$.

Lemma. *Let X and Y be sets with $R \subseteq X \times Y$ and let σ and π establish the Galois connection determined by R.*

1. *For every $A \subseteq X$, we have $A \subseteq \pi\sigma(A)$ and for every $B \subseteq Y$, we have $B \subseteq \sigma\pi(B)$.*

   Proof. Let $A \subseteq X$ and $a \in A$. Then aRb for every $b \in \sigma(A)$ so $a \in \pi\sigma(A)$. Thus $A \subseteq \pi\sigma(A)$.

   Similarly $B \subseteq \sigma\pi(B)$ for every $B \subseteq Y$. □

2. *For every $A \subseteq X$, we have $\sigma\pi\sigma(A) = \sigma(A)$ and for every $B \subseteq Y$ we have $\pi\sigma\pi(B) = \pi(B)$.*

Proof. Let $A \subseteq X$ and $B = \sigma(A) \subseteq Y$. Then $\sigma\pi(B) \supseteq B$ so $\sigma\pi\sigma(A) \supseteq \sigma(A)$. Since $\pi\sigma(A) \supseteq A$ and σ reverses the inclusion, it follows that $\sigma(\pi\sigma(A)) \subseteq \sigma(A)$. Thus $\sigma\pi\sigma(A) = \sigma(A)$.

Similarly $\pi\sigma\pi(B) = \pi(B)$ for every $B \subseteq Y$. □

Proposition. *Let X and Y be sets with $R \subseteq X \times Y$ and let σ and π establish the Galois connection determined by R.*

1. *The function $\pi\sigma : \mathscr{P}(X) \to \mathscr{P}(X)$ is a closure operator on X and $\sigma\pi : \mathscr{P}(Y) \to \mathscr{P}(Y)$ is a closure operator on Y.*

Proof. We will verify that $\pi\sigma$ is a closure operator on X. We need to verify the three axioms for closure operators.

1. We have $A \subseteq \pi\sigma(A)$ for every $A \subseteq X$ by the lemma.
2. Since both σ and π reverse the inclusion relation, for every $A \subseteq A' \subseteq X$ we have $\sigma(A) \supseteq \sigma(A')$ implying that $\pi\sigma(A) \subseteq \pi\sigma(A')$.
3. For every $A \subseteq X$, we have $\pi\sigma\pi\sigma(A) = \pi\sigma(A)$ since $\pi\sigma\pi(A) = \pi(A)$ by the lemma.

The proof that $\sigma\pi$ is a closure operator on Y is similar. □

2. *If $A \subseteq X$ then A is closed (meaning $\pi\sigma$-closed) if and only if $A = \pi(B)$ for some $B \subseteq Y$. Correspondingly, if $B \subseteq Y$ then B is closed (meaning $\sigma\pi$-closed) if and only if $B = \sigma(A)$ for some $A \subseteq X$.*

Proof. Assume that $A \subseteq X$ is closed. Then $\pi\sigma(A) = A$. Let $B = \sigma(A)$. Then $A = \pi(B)$.

Now assume that $A = \pi(B)$ for some $B \subseteq Y$. Then the lemma implies that

$$\pi\sigma(A) = \pi\sigma\pi(B) = \pi(B) = A,$$

so A is closed.

The proof that $B \subseteq Y$ is closed iff $B = \sigma(A)$ for some $A \subseteq X$ is similar. □

3. *The function σ restricted to the family of the closed subsets of X is a bijection onto the family of the closed subsets of Y with π being its inverse.*

Proof. Let $\mathscr{X}$ and $\mathscr{Y}$ be the families of all closed subsets of X and Y respectively. We want to show that $\sigma \restriction \mathscr{X}$ is a bijection onto $\mathscr{Y}$ and that $\pi \restriction \mathscr{Y}$ is the inverse of $\sigma \restriction \mathscr{X}$.

Let $A, A' \in \mathscr{X}$ be such that $\sigma(A) = \sigma(A')$. Then $A = \pi(B)$ and $A' = \pi(B')$ for some $B, B' \subseteq Y$. Then $A = \pi(B) = \pi\sigma\pi(B) = \pi\sigma(A)$ and similarly $A' = \pi\sigma(A')$. Since $\sigma(A) = \sigma(A')$ it follows that $A = A'$. Thus $\sigma \restriction \mathscr{X}$ is injective.

Let $B \in \mathscr{Y}$. Then $B = \sigma(A)$ for some $A \subseteq X$. Let $A' = \pi(B)$. Then $A' \in \mathscr{X}$ and

$$\sigma\left(A'\right) = \sigma\pi(B) = \sigma\pi\sigma(A) = \sigma(A) = B.$$

Thus $\sigma \restriction \mathscr{X}$ is a surjection onto $\mathscr{Y}$. The proof also shows that $\pi\sigma(A) = A$ for every $A \in \mathscr{X}$ and $\sigma\pi(B) = B$ for every $B \in \mathscr{Y}$. Thus $\pi \restriction \mathscr{Y}$ is the inverse of $\sigma \restriction \mathscr{X}$. □

4. *Consider the correspondence between the closed subsets of X and the closed subsets of Y established by the bijections σ and π. If $\mathscr{F}$ is a family of closed subsets of X and $\mathscr{G}$ is the corresponding family of closed subsets of Y, then $\bigcap \mathscr{F}$ corresponds to $\bigvee \mathscr{G}$ and $\bigvee \mathscr{F}$ corresponds to $\bigcap \mathscr{G}$.*

   Proof. Let $\mathscr{X}$ and $\mathscr{Y}$ be the families of all closed subsets of X and Y respectively. Then $\mathscr{F} \subseteq \mathscr{X}$ and $\mathscr{G} \subseteq \mathscr{Y}$. Since $\sigma \restriction \mathscr{X}$ is an order reversing bijection onto $\mathscr{Y}$ the image of the greatest lower bound $\bigcap \mathscr{F}$ on $\mathscr{F}$ in $\mathscr{X}$ is the least upper bound on $\mathscr{G}$ in $\mathscr{Y}$ which is $\bigvee \mathscr{G}$.

   Similarly $\bigvee \mathscr{F}$ corresponds to $\bigcap \mathscr{G}$. □

Remark (*). Let X be any set and Γ be any closure operator on X. Then there exists a set Y and a relation $R \subseteq X \times Y$ such that $\Gamma = \pi\sigma$ where $\sigma : \mathscr{P}(X) \to \mathscr{P}(Y)$ and $\pi : \mathscr{P}(Y) \to \mathscr{P}(X)$ establish the Galois connection determined by R.

Proof. Let Y be the set of all Γ-closed subsets of X and define $R \subseteq X \times Y$ so that for $x \in X$ and $y \in Y$ we have xRy iff $x \in y$. Then Y and R satisfy the required condition (exercise). □

Example. Let K be a field extension of a field F and $G = \mathrm{Aut}_F(K)$ be the group of automorphisms of K over F. Consider the Galois connection determined by the relation $R \subseteq K \times G$ defined by aRg iff $g(a) = a$.

Remark. Any closed subset of K is a subfield of K containing F and any closed subset of G is a subgroup of G.

Proof. Let σ and π establish the Galois connection determined by R. Let E be a closed subset of K. Then $E = \pi(B)$ for some $B \subseteq G$. Since $g(a) = a$ for every $a \in F$ and every $g \in B$, it follows that $F \subseteq E$. If $a, b \in E$, then $g(a) = a$ and $g(b) = b$ for every $g \in B$ implying that

$$g(a+b) = g(a) + g(b) = a + b.$$

Thus $a + b \in E$. Similarly, we show that E is closed under subtraction, multiplication and division by nonzero elements. Thus E is a subfield of K containing F.

Let H be a closed subset of G. Then $H = \sigma(A)$ for some $A \subseteq K$. Since $\mathrm{id}_K(a) = a$ for every $a \in A$, it follows that $\mathrm{id}_K \in H$. If $g, h \in H$ then $g(a) = a$ and $h(a) = a$ for every $a \in A$ implying that

$$gh(a) = g(h(a)) = g(a) = a$$

for every $a \in A$ so $gh \in H$. Also $g^{-1}(a) = a$ for every $a \in A$ so $g^{-1} \in H$. Thus H is a subgroup of G. □

Example. Consider the Galois connection from the example above in the following situations:

1. Let $F = \mathbb{Q}$ and $K = F\left(\sqrt[3]{2}\right)$. Then K is separable over F but is not normal over F. The group G is trivial and K is the only closed subset of K.

2. Let F be the field of fractions of the polynomial ring $\mathbb{F}_2[x]$ and K is the splitting field of the polynomial $y^2 - x \in F[y]$ over F. Then K is normal over F but is not separable over F. The group G is trivial and K is the only closed subset of K.

3. Let F be the field of fractions of $\mathbb{F}_2[x, y]$ and K be the splitting field of the polynomial $(z^2 - x)(z^2 - y)$ over F. Again K is normal but not separable over F. There are infinitely many intermediate fields E (with $F \subseteq E \subseteq K$) but the group G is trivial and K is the only closed subset of K.

4. Let $X = \{x_1, x_2, \ldots\}$ be a set of variables and F be the field of fractions of the integral domain $\mathbb{Q}[X]$ of all polynomials in the variables $x_1, x_2, \ldots$ with rational coefficients.

   - Let K be the splitting field of the set $\mathscr{F} \subseteq F[y]$ of polynomials in over F, where $\mathscr{F} = \left\{y^2 - x_i : i = 1, 2, \ldots\right\}$. Note that K is normal and separable over F.

   - Let $a_i \in K$ be a root of $y^2 - x_i$ for each $i = 1, 2, \ldots$ and $F_n = F(a_1, \ldots, a_n)$ for each $n = 1, 2, \ldots$. Then

   $$K = F(a_1, a_2, \ldots) = \bigcup_{n=1}^{\infty} F_n.$$

   For each subset $A \subseteq \{1, \ldots, n\}$ let a_A be the product $\prod_{i \in A} a_i$ (assuming that $a_\varnothing = 1$). Then the set $\{a_A : A \subseteq \{1, \ldots, n\}\}$ is a basis of F_n over F. It follows that the set consisting of all a_A with A being a finite subset of $\{1, 2, \ldots\}$ is a basis of K over F.

   - The group G is isomorphic to the direct product $\prod_{i=1}^{\infty} G_i$ with each G_i being equal to $\mathbb{Z}_2$. An element $(s_1, s_2, \ldots) \in \prod_{i=1}^{\infty} G_i$ corresponds to the automorphism of K over F which maps a_i to itself when $s_i = 0$ and to $-a_i$ when $s_i = 1$.

   - Let H be the subgroup of G consisting of the elements of G that correspond to the direct sum $\bigoplus_{i=1}^{\infty} G_i$, where the direct sum $\bigoplus_{i=1}^{\infty} G_i$ consists of those elements $(s_1, s_2, \ldots)$ of direct product $\prod_{i=1}^{\infty} G_i$ for which $s_i = 0$ for all i except finitely many.

   - Let $b \in K$. Then $b = F_n$ for some n so $b = \sum_{A \subseteq \{1, \ldots, n\}} c_A a_A$ for some $c_A \in F$. Suppose $\sigma(b) = b$ for every $\sigma \in H$. If $A \subseteq \{1, \ldots, n\}$ is nonempty, say $i \in A$, then there is $\sigma \in H$ with $\sigma(a_i) = -a_i$ and $\sigma(a_j) = a_j$ for all $j \neq i$. Then $\sigma(c_A a_A) = -c_A a_A$ implying that $c_A = 0$. Thus

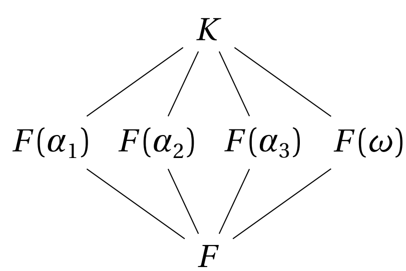
   $$b = c_\varnothing a_\varnothing = c_\varnothing \in F.$$

   implying that $\pi(H) = F$ and so $\sigma\pi(H) = G$.

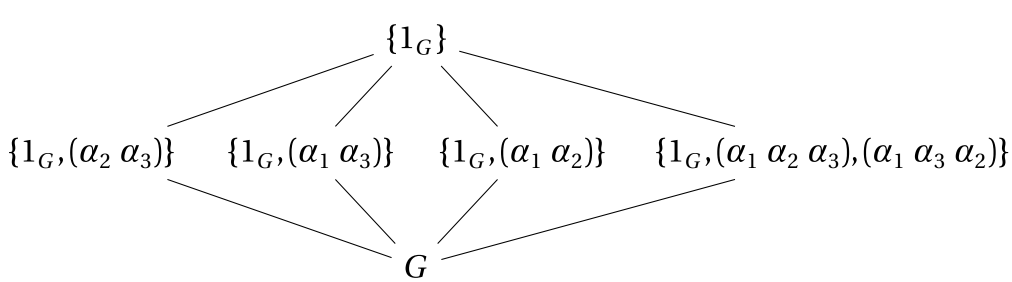
- Since H is a proper subgroup of G with G being the $\sigma\pi$-closure of H, the subgroup H is not a closed subset of G.

5. Let $F=\mathbb{Q}$ and K be the splitting field of the polynomial $f(x)=x^3-2$ over F. Then K is normal and separable over F. Let $\alpha_1=\sqrt[3]{2}$, $\alpha_2=\omega\sqrt[3]{2}$ and $\alpha_3=\omega^2\sqrt[3]{2}$, where $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$, be the roots of $f(x)$. The group G is isomorphic to S_3 (all permutations of the set $\{\alpha_1,\alpha_2,\alpha_3\}$ of the roots of $f(x)$).

   - There are six subgroups of G:
     - the trivial subgroup G_1 consisting of identity,
     - three subgroups G_2, G_3, G_4 generated by a transposition:
       G_2 consists of the identity and the transposition exchanging α_2 with α_3,
       G_3 consists of the identity and the transposition exchanging α_1 with α_3,
       G_4 consists of the identity and the transposition exchanging α_1 with α_2.
     - the subgroup G_5 consisting of identity and both 3-cycles, and
     - the group $G_6=G$.
   - There are six intermediate fields:
     - the field F_1 equal to K itself,
     - the three subfields generated by a root of f over F namely:
       $F_2=F(\alpha_1)$,
       $F_3=F(\alpha_2)$,
       $F_4=F(\alpha_3)$,
     - the subfield $F_5=F(\omega)$ generated by ω over F,
     - the subfield $F_6=F$.
   - Every subgroup of G is a closed subset of G and every intermediate field is a closed subset of K with the subgroup G_i corresponding to the subfield F_i for each $i=1,\dots,6$. Here is the resulting lattice of intermediate fields.



   And here is the corresponding lattice of the subgroups of G.



Remark. We will prove later that if K is both normal and separable over F, then any intermediate field is a closed subset of K and that if the group G is finite, then any subgroup of G is a closed subset of G.

8.4 Homework 12 — due February 22.

Exercise. Finish the proof of the remark (*) in section 8.3.

8.5 Galois Field Extensions and the Galois Correspondence.

Galois Field Extension.

Definition. Let F be a field and K be an algebraic field extension of F. We say that K is *Galois* over F iff it is both normal and separable over F.

Remark. Let K be a finite Galois extension of a field F with Galois group G. Consider the Galois connection between subsets of K and subsets of G. We will show that every intermediate field is a closed subset of K and every subgroup of G is a closed subset of G. Thus there is a bijection between the set of all intermediate field E with $F \subseteq E \subseteq K$ and all subgroups of G.

The Galois Group.

Definition. When K is Galois over F, then we will denote the group $\text{Aut}_F(K)$ of automorphisms of K over F by $\text{Gal}(K/F)$ and call it the *Galois group* of K over F.

Remark. Let K be a finite field extension of a field F with $G = \text{Aut}_F(K)$. Then K is Galois over F if and only if $|G| = [K : F]$.

Proof. Assume that K is Galois over F. Let $n = [K : F]$. Since K is separable over F, we have n embeddings of K into F^{a} over F. Since K is normal over F, each of those embeddings is an automorphism of K. Thus $|G| = n$.

Assume that $|G| = [K : F]$. Each of the automorphisms of K over F is an embedding of K into F^{a} so $[K : F]_s = [K : F]$. Thus K is separable over F. Since we can have at most $[K : F]$ embeddings of K into F^{a}, there are no other embeddings of K into F^{a} and hence every embedding of K into F^{a} is an automorphism of K. Thus K is normal over F. □

Fixed fields.

Definition. Let K be a field and G be a subgroup of $\text{Aut}(K)$. Let

$$K^G := \{a \in K : \sigma(a) = a \text{ for every } \sigma \in G\}.$$

Then K^G is a subfield of K and say that K^G is the *fixed field* of G.

Every intermediate field of a Galois extension is closed.

Proposition. *Let K be a Galois extension of a field F and G be the Galois group of K over F.*

1. *We have $K^G = F$.*

   Proof. Suppose $a \in K^G$. If φ is an embedding of $F(a)$ in $F^{\mathrm{a}} = K^{\mathrm{a}}$ over F, then φ can be extended to an automorphism of F^{a} whose restriction to K is in G. Since a is fixed by any element of G, it follows that $\varphi(a) = a$ so $[F(a): F]_s = 1$. Since a is separable over F, it follows that $a \in F$. □

2. *K is Galois over any intermediate field E.*

   Proof. Since K is separable over F, for every $a \in K$ the minimal polynomial f of a over F has no multiple roots. The minimal polynomial of a over E is a factor of f so it also has no multiple roots and a is separable over E.

   Since K is normal over F, it is a splitting field of a set of polynomials over F. Then K is a splitting field of the same set of polynomials over E. Thus K is normal over E. □

3. *If E_1 and E_2 are different intermediate fields, then*

   $$Gal(K/E_1) \neq Gal(K/E_2).$$

   Proof. Suppose $\mathrm{Gal}(K/E_1) = \mathrm{Gal}(K/E_2) = H$. Then 1. and 2. imply that $E_1 = K^H = E_2$. □

Remark. Let K be a (finite or infinite) Galois extension of a field F with Galois group G. Consider the Galois connection between subsets of K and subsets of G. Every intermediate field is a closed subset of K.

Proof. Let E be an intermediate field. Then the proposition above implies that K is Galois over E and $K^{\mathrm{Gal}(K/E)} = E$. Thus E is a closed subset of K. □

Every finite subgroup is closed.

Theorem. *Let K be a field, G be a finite subgroup of $Aut(K)$ and $F = K^G$ be the fixed field.*

1. *K is Galois over F.*

   Proof. Let $a \in K$. It suffices to show that a is a root of a polynomial over F that is separable and splits over K. Let $a_1, \dots, a_k$ be all the distinct images of a under the automorphisms from G. Consider the polynomial

   $$f(x) = (x - a_1)(x - a_2)\dots(x - a_k).$$

   The polynomial f is clearly separable and a is a root of it. Since $a_1, \dots, a_k$ are in K, it splits over K.

   It remains to show that the coefficients of f are in F. We claim that

(*) If
$$f(x)=b_0+b_1x+\cdots+b_{k-1}x^{k-1}+x^k,$$
then $\varphi(b_i)=b_i$ for every $\varphi\in G$.

Proof of (*). For each b_i, we have $b_i=h_i(a_1,\dots,a_k)$ where h_i is some composition of the operations of addition, subtraction and multiplication. For example, $b_0=(-1)^k a_1a_2\dots a_k$ and
$$b_1=(-1)^{k-1}\sum_{i=1}^{k}\prod_{j\neq i}a_j.$$
Let $\varphi\in G$. Since φ restricted to $A=\{a_1,\dots,a_k\}$ is a permutation of A, it follows that
$$\big(x-\varphi(a_1)\big)\big(x-\varphi(a_2)\big)\dots\big(x-\varphi(a_k)\big)=f(x).$$
Thus $b_i=h_i\big(\varphi(a_1),\dots,\varphi(a_k)\big)$ for each $i=0,1,\dots,k-1$. Since φ is an automorphism of K it follows that $\varphi(b_i)=h_i\big(\varphi(a_1),\dots,\varphi(a_k)\big)$. Thus $\varphi(b_i)=b_i$ for each i. □

Since
$$F=K^G=\{a\in K:\varphi(a)=a,\text{ for every }\varphi\in G\},$$
if follows that $f(x)\in F[x]$. □

2. $[K:F]=|G|$.

Proof. Suppose $[K:F]<|G|$. Then $[K:F]$ is finite and equals $[K:F]_s$ so $[K:F]_s<|G|$ which is a contradiction since any element of G is an embedding of K into $F^{\mathrm{a}}=K^{\mathrm{a}}$ over F. Thus $[K:F]\geq|G|$. If $[K:F]>|G|$, then there is an intermediate field E with finite $[E:F]>|G|$. Since every element of K is separable over F, the field E is separable over F. Thus $[E:F]_s=[E:F]$ and there is a primitive element $a\in E$ over F. The minimal polynomial of a over F has degree $>|G|$ contradicting the observation in the proof of 1. that such a degree is $\leq|G|$. □

3. Gal(K/F) is equal to G.

Proof. It is clear that $G\subseteq H=\mathrm{Gal}(K/F)$. Since $|H|=[K:F]=|G|$ and G is finite, we have $G=H$. □

Remark. Let K be a finite Galois extension of a field F with Galois group G. Consider the Galois connection between subsets of K and subsets of G. Every subgroup of G is a closed subset of G.

Proof. Let H be a subgroup of G. Since G is finite (we have $|G|=[K:F]$) also H is finite. The theorem above implies that $\mathrm{Gal}\big(K/K^H\big)=H$. Thus H is a closed subset of G. □

Remark. Without the assumption that K is finite over F, not every subgroup of G is a closed subset of G. There is a topology on G (*Krull topology* on G) such that the closed subsets of G are exactly the subgroups of G that are closed in the Krull topology. However, if a subgroup H of G is finite, then H is a closed subset of G. Thus every finite subgroup of G is closed in the Krull topology.

The join of subfields and of subgroups.

Definition. If E_1 and E_2 are subfields of a field K, then E_1E_2 denotes the *join* of E_1 and E_2 which is the intersection of all subfields of K containing the union $E_1 \cup E_2$.

Remark. Note the the join E_1E_2 is equal to $E_1(E_2)$ and to $E_2(E_1)$.

Definition. Let H_1 and H_2 be subgroups of a group G. The *join* $H_1 \vee H_2$ is the intersection of all subgroups of G containing $H_1 \cup H_2$.

Remark. If one (or both) of the subgroups H_1, H_2 is normal in G, then $H_1 \vee H_2 = H_1H_2 = H_2H_1$ where

$$H_1H_2 = \{h_1h_2 : h_1 \in H_1,\ h_2 \in H_2\}.$$

See the exercise in section 8.6.

Corollary. *Let K be a finite Galois extension of a field F with Galois group G.*

1. *There is a bijection between the set of all intermediate fields and the set of all subgroups of G.*

2. *The group corresponding to an intermediate field E is the Galois group $Gal(K/E)$.*

3. *The field corresponding to a subgroup H is the fixed field K^H.*

4. *If $E_1 \subseteq E_2$ are intermediate fields and $H_1 \supseteq H_2$ are the corresponding subgroups of G, then $[E_2 : E_1] = [H_1 : H_2]$.*

   Proof. Since K is Galois over both E_1 and E_2, we have $[K : E_1] = |H_1|$ and $[K : E_2] = |H_2|$. Since $[K : E_1] = [K : E_2]\,[E_2 : E_1]$, it follows that

   $$[E_2 : E_1] = \frac{[K : E_1]}{[K : E_2]} = \frac{|H_1|}{|H_2|} = [H_1 : H_2],$$

   as claimed. □

5. *If E_1 and E_2 are intermediate fields and H_1, H_2 are the corresponding subgroups of G, then the join E_1E_2 corresponds to the subgroup $H_1 \cap H_2$ of G, and the intermediate field $E_1 \cap E_2$ corresponds to the join $H_1 \vee H_2$.*

8.6 Homework 13 — due March 1.

Exercise. Let G be a group and H_1, H_2 be subgroups of G.

1. Prove that if $H_1H_2 = H_2H_1$, then H_1H_2 is a subgroup of G.

2. Prove that if H_1 is normal in G, then $H_1H_2 = H_2H_1$.

8.7 Normality in the Galois Correspondence.

Theorem. *Let K be a Galois extension of a field F with Galois group G. Let E be an intermediate field with the corresponding subgroup H of G.*

1. E is normal over F if and only if H is normal in G.

Proof. Let E be an intermediate field and $H = \mathrm{Gal}(K/E)$. Suppose E is normal over F. Let $\varphi \in G$ and $\psi \in H$. To show the normality of H in G we need to verify that $\varphi^{-1}\psi\varphi \in H$, that is that $\varphi^{-1}\psi\varphi(a) = a$ for every $a \in E$. Since E is normal over F, it follows that $\varphi(a) \in E$ so $\psi\big(\varphi(a)\big) = \varphi(a)$ and hence $\varphi^{-1}\psi\varphi(a) = a$.

Now assume that H is normal in G. Let φ' be any automorphism of F^{a} $(= K^{\mathrm{a}})$ over F. Suppose, to the contrary, that E is not normal over F. Then the restriction of φ' to E is not an automorphism of E. Thus there is $a \in E$ such that $b = \varphi'(a) \in K \setminus E$. Since E is the fixed field of H, there is $\psi \in H$ such that $\psi(b) \neq b$. Let φ be the restriction of φ' to K. Then

$$\varphi^{-1}\psi\varphi(a) = \varphi^{-1}\psi(b) \neq \varphi^{-1}(b) = a.$$

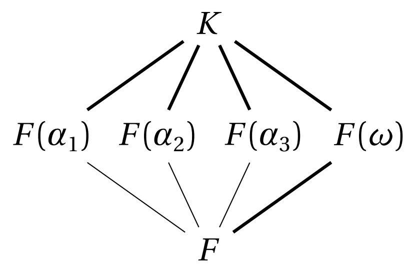
Since $a \in E$, it follows that $\varphi^{-1}\psi\varphi \notin H$ contradicting normality of H in G. □

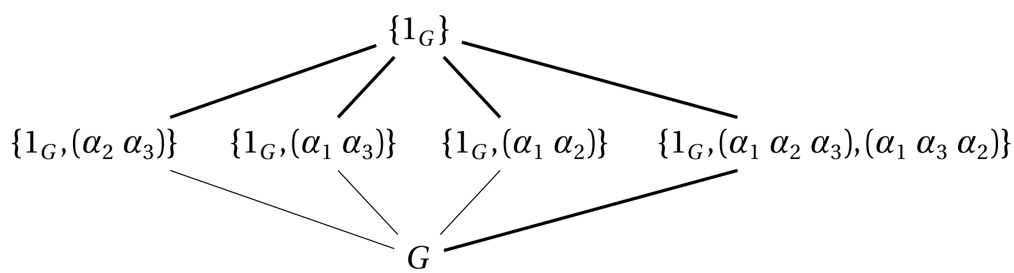
2. If E is a normal over F (hence is Galois over F), then the Galois group Gal(E/F) is isomorphic to the quotient group G/H.

Proof. Let $f : G \to \mathrm{Gal}(E/F)$ assign to $\varphi \in G$ the restriction of φ to E. Then f is a surjective group homomorphism with $H = \ker\big(f\big)$. Thus $\mathrm{Gal}(E/F)$ is isomorphic to G/H. □

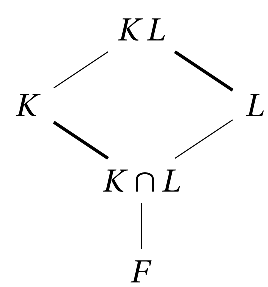
Remark. Let K be a Galois extension of F with $G = \mathrm{Gal}(K/F)$, let $E_1 \subseteq E_2$ be some intermediate fields with the corresponding subgroups $H_1 \supseteq H_2$ of G. Then the field E_2 is normal over E_1 if and only if the group H_2 is normal in H_1. If normality holds, then $\mathrm{Gal}(E_2/E_1)$ is isomorphic to H_1/H_2.

Example. Let $F = \mathbb{Q}$ and K be the splitting field of the polynomial $f(x) = x^3 - 2$ over F. Then K is normal and separable over F. Let $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega\sqrt[3]{2}$ and $\alpha_3 = \omega^2\sqrt[3]{2}$, where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, be the roots of $f(x)$. Let G be the Galois group of K over F with the elements of G represented as the permutations of the set $\{\alpha_1, \alpha_2, \alpha_3\}$ of the roots of $f(x)$. In the pictures below, thick lines denote normality.





Proposition. *Let K be a Galois extension of a field F and L be any field extension of F, with both K and L being subfields of the same field.*



1. *The join KL is Galois over L and K is Galois over $K \cap L$.*

   Proof. Since K is Galois over F it is Galois over any intermediate field so, in particular, over $K \cap L$. In order to show that KL is Galois over L we will prove and use the following claim.

   (*) Every $a \in K$ is a root of a separable polynomial $f_a(x) \in L[x]$ that splits over KL.

   Proof of (*). Let $a \in K$. Since K is Galois over F, the minimal polynomial $f_a(x)$ of a over F is separable and splits over K. Then $f_a(x) \in L[x]$ and f_a splits over KL. □

   Since KL is generated by K over L and every element of K is separable over L, it follows that KL is separable over L. Since KL is the splitting field of the set $\{f_a : a \in K\}$ of polynomials over L, it follows that KL is normal over L. □

2. *If K is finite over $K \cap L$, then the function $\varphi : Gal(KL/L) \to Gal(K/K \cap L)$ assigning to σ the restriction $\sigma \restriction K$ is a group isomorphism.*

   Proof. Since K is normal over $K \cap L$, every automorphism of KL over L restricted to K is an automorphism of K over $K \cap L$. Thus $\varphi \restriction K \in \mathrm{Gal}(K/K \cap L)$. If $\sigma, \tau \in \mathrm{Gal}(KL/L)$, then $(\sigma \circ \tau)\restriction K = (\sigma \restriction K) \circ (\tau \restriction K)$ so the function φ is a group homomorphism. Since $KL = L(K)$, it is clear that φ is injective.

   It remains to show the surjectivity of φ. It suffices to show that $[K : K \cap L] = [KL/L]$. Since K is finite and separable over $K \cap L$, the Primitive Element Theorem implies that K is generated over $K \cap L$ be a single element $a \in K$. Then $KL = L(a)$. Let $f(x)$ be the minimal polynomial of a over $K \cap L$. The result will follow when we show that $f(x)$ is irreducible over L. Since K is normal over $K \cap L$, the polynomial f splits over K implying that every monic divisor of $f(x)$ in $L[x]$ belongs to $(K \cap L)[x]$. Since f is irreducible over $K \cap L$, it follows that it is irreducible over L. □

Remark. The assumption that K is finite over $K \cap L$ in part 2. of the proposition above was only used in the proof of the surjectivity of φ in order to simplify the argument. Without this assumption, the result is still true. The proof however becomes more complicated since we need to consider then the continuity of φ in the Krull topology.

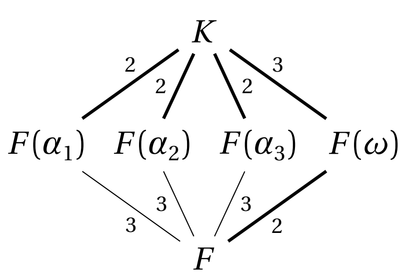
Corollary. *Let K be a finite Galois extension of a field F and E_1, E_2 be intermediate fields. Suppose that one (or both) of E_1, E_2 is normal over $E_1 \cap E_2$. Then $[E_1E_2 : E_1] = [E_2 : E_1 \cap E_2]$ and $[E_1E_2 : E_2] = [E_1 : E_1 \cap E_2]$.*

Remark. When none of the intermediate fields E_1, E_2 is normal over F, then the equalities in the above corollary do not need to hold.

Example. Let $F = \mathbb{Q}$ and K be the splitting field of the polynomial $x^3 - 2$ over F. Let $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\omega$ with $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, and let $E_1 = F(\alpha_1)$ and $E_2 = F(\alpha_2)$. Then $E_1E_2 = K$ and $E_1 \cap E_2 = F$, but $[E_1 : F] = [E_2 : F] = 3$ while $[K : E_1] = [K : E_2] = 2$. Note that none of the fields E_1, E_2 is normal over F.

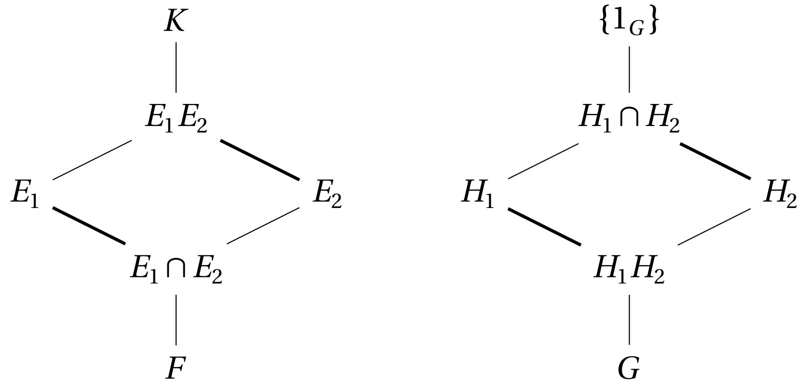
Let $E_3 = F(\omega)$. Then E_3 is normal over F. Now we have $[E_3 : F] = 2 = [K : E_1]$ and $[K : E_3] = 3 = [E_1 : F]$.

In the picture below, bold lines are used when the extension is normal and the numbers denote the degree of the extension.



Remark. Instead of using the proposition, the corollary can be deduced alternatively from the Second Isomorphism Theorem for groups (see section 8.8).

Proof. Let G be the Galois group of K over F and let H_1 and H_2 be the subgroups of G that correspond to the intermediate fields E_1 and E_2. Suppose E_1 is normal over F. Then H_1 is normal in G.



Thus $H_1 \cap H_2$ is normal in H_2 and there is an isomorphism $H_1H_2/H_1 \to H_2/(H_1 \cap H_2)$ implying that

$$[H_1H_2 : H_1] = [H_2 : H_1 \cap H_2],$$

and consequently $[E_1E_2 : E_2] = [E_1 : E_1 \cap E_2]$. □

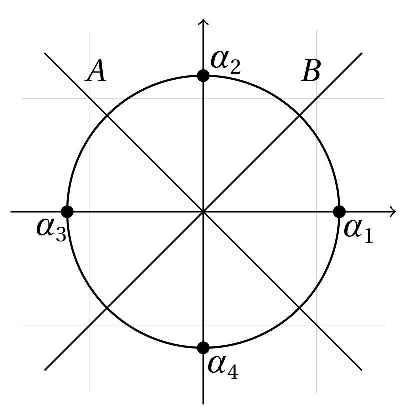
8.8 Homework 14 — due March 4.

Exercise. Let G be a group and H_1, H_2 be subgroups of G with H_1 normal in G. Prove that the quotient H_1H_2/H_1 is isomorphic to $H_2/(H_1 \cap H_2)$. Hint: Define a homomorphism $\varphi : H_1H_2 \to H_2/(H_1 \cap H_2)$ such that $\varphi(h_1h_2) = h_2(H_1 \cap H_2)$ and use the Fundamental Homomorphism Theorem for groups.

Remark. The result in the exercise is often called the *Second Isomorphism Theorem for groups.*

8.9 The Galois Group of $x^4 - 2$ over $\mathbb{Q}$.

- Let $F = \mathbb{Q}$ and K be the splitting field of the polynomial $x^4 - 2$ over F with G being the Galois group of K over F. Let $\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = i\sqrt[4]{2}$, $\alpha_3 = -\sqrt[4]{2}$ and $\alpha_4 = -i\sqrt[4]{2}$ be all the roots of $x^4 - 2$.



- Since $F(\alpha_1)$ has degree 4 over F and $i \notin F(\alpha_1)$, the polynomial x^2+1 is irreducible over $F(\alpha_1)$ so $K = F(\alpha_1, i)$ and $[K : F] = 8$. Consequently, the group G has 8 elements. The root α_1 can be mapped to any of the roots $\alpha_1, \ldots, \alpha_4$ and i can be mapped either to itself or to $-i$. There are 8 choices in total and each of them corresponds to exactly one element of G.

- There is $\varphi \in G$ such that $\varphi(\alpha_1) = \alpha_2$ and $\varphi(i) = i$, and there is $\tau \in G$ such that $\tau(\alpha_1) = \alpha_1$ and $\tau(i) = -i$. Note that φ corresponds to the 4-cycle $(\alpha_1\, \alpha_2\, \alpha_3\, \alpha_4)$ or to the rotation by 90° anticlockwise around the origin. The automorphism τ corresponds to the transposition $(\alpha_2\, \alpha_4)$ or the reflection in the real axis.

- The remaining elements of G are:

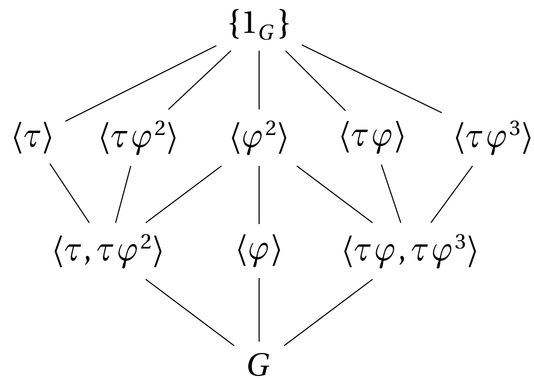
  - the identity 1_G,
  - the composition φ^2 of φ with itself that corresponds to the product $(\alpha_1\, \alpha_3)(\alpha_2\, \alpha_4)$ of two transpositions or to the rotation by 180° around the origin,
  - $\varphi^3 = \varphi^{-1}$ corresponding to the 4-cycle $(\alpha_1\, \alpha_4\, \alpha_3\, \alpha_2)$ or the rotation by 90° clockwise around the origin.
  - the composition $\tau\varphi = \varphi^3\tau$ corresponding to the product $(\alpha_1\, \alpha_4)(\alpha_2\, \alpha_3)$ or to the reflection in line A.
  - the composition $\tau\varphi^2 = \varphi^2\tau$ corresponding to the transposition $(\alpha_1\, \alpha_3)$ or to the reflection in the imaginary axis.
  - the composition $\tau\varphi^3 = \varphi\tau$ corresponding to the product $(\alpha_1\, \alpha_2)(\alpha_3\, \alpha_4)$ or to the reflection in the line B.

- The subgroups of G are

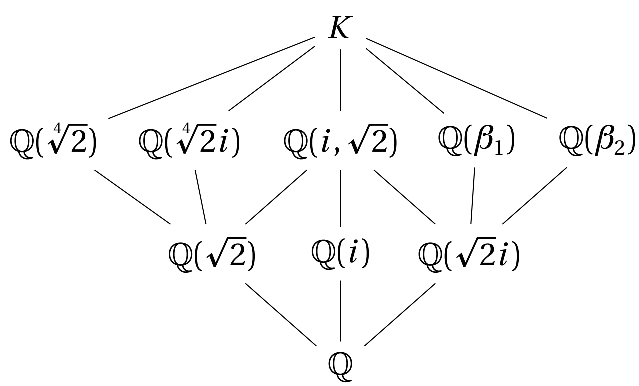
  - the trivial group $\{1_G\}$,
  - five subgroups of order two generated by one of the elements whose order in G is 2, namely the four reflections and rotation by 180°: $\langle\tau\rangle$, $\langle\tau\varphi\rangle$, $\langle\tau\varphi^2\rangle$, $\langle\tau\varphi^3\rangle$, $\langle\varphi^2\rangle$;
  - three subgroups of order four: the subgroup $\langle\varphi\rangle$ consisting of all rotations (including the identity) that is generated by φ, the two subgroups generated by the reflections in two perpendicular lines, either both axis or the lines A and B, namely $\langle\tau, \tau\varphi^2\rangle$ and $\langle\tau\varphi, \tau\varphi^3\rangle$.
  - the group G.

- All subgroups of G of order four are normal in G (subgroups of index two are always normal). The only subgroup of order two that is normal in G is $\langle\varphi^2\rangle$.

- Here is the lattice of the subgroups of G.



The corresponding lattice of the intermediate fields is given below, where $\beta_1 = \alpha_1 + \alpha_4$ and $\beta_2 = \alpha_1 + \alpha_2$.



Remark. The group that appears in the example above is call the *dihedral group* of order 8 and denoted D_8. For each positive integer n, there is a *dihedral group* D_{2n} of order $2n$ that is the group of all symmetries of a regular n-gon. The group D_6 is isomorphic to the group S_3 of all permutations of the set $\{1,2,3\}$. Note that if $n \geq 3$, then the group D_{2n} is not abelian.

8.10 Homework 15 — due March 15.

Exercise. Let $f(x) = x^4 - 3x^2 - 3$ be a polynomial over $F = \mathbb{Q}$ and let K be the splitting field of $f(x)$ over F. Find the Galois group G of K over F and draw the lattice of all intermediate subfields and the corresponding lattice of all subgroups of G. Identify which intermediate fields are normal over F.

9 Sylow Subgroups of a Finite Group.

9.1 A Partial Converse of Lagrange's Theorem.

Example. Let $G = A_4$ be the group of even permutations of the set $\{1,2,3,4\}$. Then G has 12 elements so 6 is a divisor of 12, but G has no subgroup of order 6. Thus the converse of Lagrange's Theorems is false.

Remark. We will show that if G is a finite group, p is a prime and p^n divides the order of G, then G has a subgroup of order p^n. This gives us a partial converse of Lagrange's Theorem.

9.2 Sylow Subgroups.

p-subgroups. Let p be a prime. A p-subgroup of a finite group G is a subgroup whose order is a power of p (including the trivial subgroup).

Sylow p-subgroups. Let G be a finite group and p be a prime. A Sylow p-subgroup of G is a p-subgroup H such that the index $[G:H]$ is not divisible by p.

Remark. We will show that for any prime p any finite group G contains a Sylow p-subgroup and more generally that if p^n divides the order of G, then G has a subgroup of order p^n (see Theorem and Corollary in section 9.7).

9.3 The Fundamental Theorem of Algebra.

Linear Orders. Let X be a set. A *linear order* on X is a binary relation $\leq$ such that

1. $\leq$ is reflexive (for every $a \in X$ we have $a \leq a$).
2. $\leq$ is transitive (for every $a,b,c \in X$ if $a \leq b$ and $b \leq c$ then $a \leq c$).
3. $\leq$ is antisymmetric (for every $a,b \in X$ if $a \leq b$ and $b \leq a$ then $a = b$).
4. $\leq$ is total (for every $a,b \in X$ we have $a \leq b$ or $b \leq a$).

Ordered Fields. An *ordered field* is a field F with a linear order relation $\leq$ such that, for any $a,b \in F$, if $a,b \geq 0$, then $a+b \geq 0$ and $ab \geq 0$.

Remark. Equivalently, an ordered field is a field F with a distinguished set $P \subseteq F$ such that:

1. F is the disjoint union of P, $\{0\}$ and $-P$, where $-P = \{-a : a \in P\}$.
2. $a+b \in P$ and $ab \in P$ for every $a,b \in P$.

The elements of P are called *positive* and correspond to the elements that are ≥ 0 but $\neq 0$.

Elements that are squares. Let F be a field. We say that an element $a \in F$ is a square, if there exists $b \in F$ such that $a = b^2$.

Remark. If F is an ordered field, and $a \in F^*$ is a square, then a is positive. In particular, no ordered field can be algebraically closed.

Proposition. *Any ordered field has characteristic zero.*

Proof. Suppose that F is an ordered field of prime characteristic p. Then 1_F is a square so it is positive implying that $-1_F = \underbrace{1_F + \cdots + 1_F}_{p-1}$ is positive, which is a contradiction. □

Theorem. *Let F be an ordered field such that every polynomial of odd degree over F has a root in F and every positive element of F is a square. If K is a splitting field of the polynomial x^2+1 over F, then K is algebraically closed.*

Proof. Let i be a root of $f(x) = x^2+1$ in F^{a}. Then $K = F(i)$. Let L be any finite extension of K. It suffices to show that $L = K$.

We can assume without loss of generality that L is normal over F (otherwise L can be replaced with the splitting field over F of the minimal polynomial of $a \in L$ such that $L = F(a)$). Then L is a finite Galois extension of F. Let G be the Galois group of L over F and H be a Sylow 2-subgroup of G. Let $E = L^H$ be the corresponding fixed field.

$$\begin{array}{ccc} L & \qquad\qquad & \{1_G\} \\ | & & | \\ E & & H \\ | & & | \\ F & & G \end{array}$$

We claim that:

(*) $E = F$.

Proof of (*). We have then $[E:F] = [G:H]$ so $[E:F]$ is odd. Let $a \in E$ be arbitrary. Then

$$[E:F] = [E:F(a)]\,[F(a):F],$$

implying that $[F(a):F]$ is odd. Let $g(x)$ be the minimal polynomial of a over F. Then $g(x)$ has odd degree and is irreducible over F. Since any polynomial over F of odd degree has a root in F, it follows that $g(x)$ has degree 1. Thus $a \in F$. □

Since $E = F$, it follows that $H = G$ so G is a 2-group. Let J be the subgroup of G corresponding to K and suppose, to the contrary, that $L \neq K$. Then J is a nontrivial group whose order is 2^k for some integer $k \geq 1$. Let J' be a subgroup of J of order 2^{k-1} and K' be the corresponding field.

$$\begin{array}{ccc} L & \qquad\qquad & \{1_G\} \\ | & & | \\ K' & & J' \\ | & & | \\ K & & J \\ | & & | \\ F & & G \end{array}$$

Then $[J : J'] = 2$ so K' is an extension of K of degree 2. To complete the proof it remains to show that K has no proper extensions of degree 2 (exercise). □

Corollary. *The field $\mathbb{C}$ of complex numbers is algebraically closed.*

9.4 Homework 16 — due March 20.

Exercise. Finish the proof of the theorem in section 9.3.

9.5 Group Actions.

Definition. Let G be a group and X be a set. An *action* of G on X is a group homomorphism $G \to S(X)$, where $S(X)$ is the group of all permutations of X. If $\varphi : G \to S(X)$ is an action of G on X then we will also say that $\big(\varphi(g)\big)(a)$ is the result of g acting on a and denote it by $g(a)$.

Example. Let G be a group. Then G acts on itself by conjugation.

Formally, the homomorphism $\varphi : G \to S(G)$ is such that if $a \in G$ then the permutation $\varphi(a) : G \to G$ is the conjugation by a, that is for $b \in G$ we have $\big(\varphi(a)\big)(b) = a\,b\,a^{-1}$. φ is a homomorphism since

$$\begin{aligned} \big(\varphi(ac)\big)(b) &= acb(ac)^{-1} \\ &= acbc^{-1}a^{-1} \\ &= a\Big(\big(\varphi(c)\big)(b)\Big)a^{-1} \\ &= \big(\varphi(a)\big)\Big(\big(\varphi(c)\big)(b)\Big) \\ &= \big(\varphi(a)\varphi(c)\big)(b) \end{aligned}$$

so $\varphi(ac) = \varphi(a)\varphi(c)$.

Orbits of a Group Action.

Definition. Let G act on a set X. Let $\sim$ be the equivalence relation on X given by $a \sim b$ iff there is $g \in G$ with $b = g(a)$. The equivalence classes of $\sim$ are called the orbits of this action.

Stabilizers.

Definition. Let G act on a set X. If $a \in X$, then let $G_a = \left\{g \in G : g(a) = a\right\}$ be the *stabilizer* of a in G.

Remark. The stabilizer G_a is a subgroup of G.

9.6 Class Formula.

Theorem. *Let G be a group acting on a finite set X and $a_1, \dots, a_n$ be representatives of the orbits of the action. Then $|X| = \sum_{i=1}^{n} \left[G : G_{a_i}\right]$, where G_{a_i} is the stabilizer of a_i.*

Proof. Let A_i be the orbit containing a_i for each $i = 1, \dots, n$. It suffices to show that $\left|A_i\right| = \left[G : G_{a_i}\right]$. Let G/G_{a_i} be the set of all left cosets of G_{a_i} in G. Define $f : G/G_{a_i} \to A_i$ so that $f\left(bG_{a_i}\right)$ is the result $b(a_i)$ of b acting on a_i. We have $bG_{a_i} = b'G_{a_i}$ iff $b^{-1}b' \in G_{a_i}$ iff $b^{-1}b'(a_i) = a_i$ iff $b'(a_i) = b(a_i)$ implying that f is well-defined and injective. Clearly f is surjective. □

Center of a group.

Definition. The *center* Z of a group G is the set of all $a \in G$ that commute with every element of G.

Remark. If G acts on itself by conjugation, then the center of G is the set of all $a \in G$ such that the singleton $\{a\}$ is an orbit of G.

Centralizer of an element of a group.

Definition. If G is a group and $a \in G$, then the *centralizer* C_a of a in G is the set of all elements of G that commute with a.

Remark. If G acts on itself by conjugation, then the stabilizer of $a \in G$ in this action is the centralizer C_a.

Conjugacy classes.

Definition. Let G be a group. The orbits when G acts on itself by conjugation are called *conjugacy classes.*

Corollary. *Let G be a finite group and $a_1, \dots, a_n$ be representatives of conjugacy classes that are not singletons. Then*

$$|G| = |Z| + \sum_{i=1}^{n} \left[G : C_{a_i}\right],$$

where Z is the center of G.

9.7 The First Sylow Theorem — Existence of Sylow Subgroups.

Proposition. *Let G be a finite abelian group and p be a prime dividing the order of G. The G has an element of order p.*

Proof. We use induction on the order of G. Let $a \in G$ be not equal to 1_G. If the order of a is divisible by p, say is equal to kp, then $a^k \in G$ has order p. Otherwise, let $H = \langle a \rangle$ be the cyclic subgroup of G generated by a. Since p divides the order of G/H, it follows from the inductive hypothesis that there is an element $bH \in G/H$ of order p. Thus p divides the order of b in G (see the exercise in section 9.9) and we can repeat the argument from above. □

Theorem. *Let G be a finite group and p be a prime. There exists a Sylow p-subgroup of G.*

Proof. We use induction on the order of G. If G is trivial the result is obvious. Assume G is not trivial. If there is a proper subgroup H of G with $[G:H]$ not divisible by p, then the inductive hypothesis implies that H has a Sylow p-subgroup which is then a Sylow p-subgroup of G. Suppose not. Then p divides the order of G. Let $a_1, \ldots, a_n$ be representatives of the nontrivial (that are not singletons) conjugacy classes of G. Then the index $\left[G : C_{a_i}\right]$ is divisible by p for each i so the Class Formula implies that the order of the center Z of G is divisible by p. Thus there is an element $a \in Z$ of order p. Let $H = \langle a \rangle$ be the cyclic subgroup of G generated by a. Since $a \in Z$, the subgroup H is normal in G. By the inductive hypothesis G/H contains a Sylow p-subgroup which is of the form K/H for some subgroup K of G containing H (by Correspondence Theorem). Then $[G:K] = [G/H : K/H]$ is not divisible by p so K is a Sylow p-subgroup of G. □

Corollary. *If G is a finite group and p is a prime such that p^n divides the order of G, then G has a subgroup of order p^n.*

Proof. The theorem above implies that we can assume, without loss of generality, that G is a p-group. We use induction on n. If $n = 0$, the result is obvious. Assume $n \geq 1$. Then G is nontrivial so it has a nontrivial center Z (exercise). Then Z contains an element of order p which implies that G has a normal subgroup H of order p. By the inductive hypothesis (and the Correspondence Theorem for groups) the group G/H contains a subgroup K/H of order p^{n-1}, where K is a subgroup of G containing H. Then the order of K is p^n. □

9.8 Homework 17 — due March 22.

Exercise. Let p be a prime integer and G be a nontrivial finite p-group. Prove that the center Z of G is nontrivial.

9.9 Homework 18 — due April 1.

Exercise. Let G be a group and H be a subgroup of G. Let $a \in G$ be an element of a finite order m. Let k be the smallest positive integer such that $a^k \in H$ and ℓ be the order of a^k in H. Prove that $k\ell = m$.

9.10 More on Sylow Subgroups.

Fixed point of a group action.

Definition. Let G be a group acting on a set X. A *fixed point* of this action is an element $a \in X$ such that $\sigma(a) = a$ for every $\sigma \in G$.

Lemma. *Let p be a prime integer and G be a finite p-group acting on a finite set X. Then the number of fixed points of this action is congruent to $|X|$ modulo p.*

Proof. For any $a \in X$ the cardinality of the orbit of a is equal to $[G : G_a]$, where G_a is the stabilizer of a. If a is not a fixed point, then G_a is a proper subgroup of G so the index $[G : G_a]$ is divisible by p. Thus the class formula implies the result. □

Normalizer of a subgroup.

Definition. Let G be a group and H be a subgroup of G. The *normalizer* of H in G is the set of all $g \in G$ such that $gH = Hg$.

Remark. Note that the normalizer of H in G is a subgroup of G containing H. It is the largest subgroup of G in which H is normal. Also H is normal in G if and only if the normalizer of H in G is equal to G.

Group acting on the set of its subgroups by conjugation.

Definition. Let G be a group and X be the set of all subgroups of G. The action of G on X by *conjugation* is defined by

$$g(H) = gHg^{-1} = \{ghg^{-1} : h \in H\},$$

for any $g \in G$ and $H \in X$.

Remark. Note that H is a fixed point of the action above if and only if H is normal in G. If H is any subgroup of G, then the stabilizer of H in that action is the normalizer of H in G.

The action above can also be considered when X is any set of subgroups of G that is closed under conjugation. We can also consider the action on X be any subgroup of G.

Proposition. *Let G be a finite group, p be a prime integer, H be a p-subgroup of G, P be a Sylow p-subgroup of G and X be the set of all conjugates of P by elements of G. Consider the action of H on X by conjugation. Then there exists a fixed point of this action. Any such fixed point contains H.*

Proof. Consider the action of G on X by conjugation first. This action has only one orbit equal to X. Thus $|X| = [G : N]$, where N is the stabilizer of P in that action, hence the normalizer of P in G. Since N contains P, it follows that $[G : N]$ is not divisible by p. Thus $|X|$ is not divisible by p.

Now consider the action of H on X by conjugation. The number of fixed points of this action is congruent to $|X|$ modulo p so it is nonzero. Let Q be a fixed point of this action. Then $hQh^{-1} = Q$ for any $h \in H$ so $H \subseteq N'$ where N' is the normalizer of Q in G. We claim that $H \subseteq Q$.

Suppose, to the contrary, that H is not a subset of Q. Then $HQ \neq Q$. Note that HQ is a subgroup of N' since Q is normal in N'. Since HQ/Q is isomorphic to $H/(H \cap Q)$, it follows that the index $[HQ : Q]$ is a positive power of p. That is a contradiction since Q is a Sylow p-subgroup of G. □

Conjugate subgroups.

Definition. Let G be a group and H and J be subgroups of G. We say that H and J are conjugate in G if there exists $g \in G$ such that $J = gHg^{-1}$.

Remark. Any two subgroups of G that are conjugate are isomorphic. The converse does not have to be true.

Example. Let $H = \mathbb{Z}_2 \times \{0\}$ and $J = \{0\} \times \mathbb{Z}_2$ be subgroups of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then H and J are isomorphic but they are not conjugate in G. Since G is abelian, two subgroups of G are conjugate if and only they are equal.

Theorem. *Let G be a finite group and p be a prime integer.*

(1) *Any p-subgroup of G is contained in a Sylow p-subgroup of G.*

Proof. Let H be a p-subgroup of G and P be a Sylow p-subgroup of G. Consider the action of H by conjugation on the set X of all conjugates of P by elements of G. Let Q be a fixed point of this action. Then Q is a Sylow p-subgroup containing H. □

(2) *Any two Sylow p-subgroups of G are conjugate.*

Proof. Let H and P be Sylow p-subgroups of G. Consider again the action of H by conjugation on the set X of all conjugates of P by elements of G and let Q be a fixed point of this action. Then $H \subseteq Q$ implying that $H = Q$. Since Q is a conjugate of P, it follows that H is a conjugate of P. □

(3) *The number of Sylow p-subgroups of G is congruent to* 1 *modulo p.*

Proof. Note that any fixed point of the action in the proof of (2) must be equal to H so there is only one fixed point. Therefore $|X| \equiv 1$ modulo p. □

(4) *The number of Sylow p-subgroups of G is a divisor of $|G|$.*

Proof. Consider the action of G by conjugation on the set X of all Sylow p-subgroups of G. Since X is the only orbit of this action, its size (equal to the index of the stabilizer of any element of X) must be a divisor of $|G|$. □

Corollary. *Let G be a finite group and p be a prime integer.*

1. *Any two Sylow p-subgroups of G are isomorphic.*
2. *If G is abelian, then it has a unique Sylow p-subgroup.*

Remark. As a consequence, any subgroup of the symmetric group S_4 of order 8 is isomorphic to the dihedral group D_8.

9.11 Homework 19 — due April 3.

Exercise. Let p be a prime integer, G be a finite group, H be a Sylow p-subgroup of G and N be the normalizer of H in G. Prove that if J is any p-subgroup of G contained in N, then $J \subseteq H$.

10 Solving Polynomials by Radicals.

10.1 Radical Field Extensions.

Definition. Let F be a field of characteristic zero and K be a field extension of F. We say that K is *radical* over F iff there exists a chain $F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n = K$ of fields such that for each $i = 1, \ldots, n$ we have $F_i = F_{i-1}(a_i)$ for some $a_i \in F_i$ such that there is a positive integer n_i with $a_i^{n_i} \in F_{i-1}$.

Remark. Any radical field extension is a finite extension.

Example. Let

$$a = \sqrt[5]{\frac{7+\sqrt[12]{7}}{\sqrt[11]{\sqrt[7]{15}+\sqrt[3]{5}}} + \sqrt[17]{19} + 78} \in \mathbb{R}$$

and $K = \mathbb{Q}(a)$. Then K is a radical extension of $\mathbb{Q}$. Indeed, if $F_1 = \mathbb{Q}\big(\sqrt[12]{7}\big)$, $F_2 = F_1\big(\sqrt[7]{15}\big)$, $F_3 = F_2\big(\sqrt[3]{5}\big)$, $F_4 = F_3\ \sqrt[17]{19}$ and $F_5 = F_4\Big(\sqrt[11]{\sqrt[7]{15}+\sqrt[3]{5}}\Big)$, then the chain

$$\mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq F_3 \subseteq F_4 \subseteq F_5 \subseteq K$$

demonstrate that K is a radical extension of $\mathbb{Q}$.

Polynomials solvable by Radicals.

Definition. Let F be a field of characteristic zero and f be a polynomial over F. We say that f is *solvable by radicals* over F iff there exists a radical extension K of F such that $f(x)$ splits in $K[x]$.

Remark. Intuitively, a polynomial $f(x) \in F[x]$ is solvable by radicals over F if and only if its roots can be expressed in terms of the elements of F using algebraical operations like addition, subtraction, multiplication and division together with the operation of taking roots of some degree n that is a positive integer (picking one of the roots of an equation of the form $x^n = a$).

Note that f is solvable by radicals over F if and only if the splitting field of f over F can be extended to a radical extension of F.

Proposition. *Let F be a field of characteristic zero and f be a polynomial of degree ≤ 4 over F. Then f is solvable by radicals over F.*

Proof. The result is obvious when the degree of f is 1 and when it is 2, then we can use the quadratic formula.

Assume that $\deg(f) = 3$. Without loss of generality, we can assume that f is monic. Let $f(x) = x^3 + bx^2 + cx + d$ with $b, c, d \in F$. Substituting $x = y - b/3$, we get

$$g(y) = \left(y - \frac{b}{3}\right)^3 + b\left(y - \frac{b}{3}\right)^2 + c\left(y - \frac{b}{3}\right) + d = y^3 + py + q$$

for some $p, q \in F$. Let $s \in F$. Substituting $y = z + s/z$ and multiplying by z^3, we get

$$\left(\left(z + \frac{s}{z}\right)^3 + p\left(z + \frac{s}{z}\right) + q\right)z^3 = z^6 + (3s + p)z^4 + qz^3 + s(3s + p)z^2 + s^3.$$

When $s = -p/3$, we get $h(z) = z^6 + qz^3 - p^3/27$. It is clear that there is a radical extension E of F such that h splits over E and that there is a radical extension K of E such that g splits over K. Then K is a radical extension of F and f splits over K implying that f is solvable by radicals over F.

Assume that $\deg(f) = 4$. Without loss of generality, we can assume that f is irreducible and of the form

$$f(x) = x^4 + px^2 + qx + r$$

for some $p, q, r \in F$. If $q = 0$, then it is clear that f is solvable by radicals over F. Assume thus that $q \neq 0$. Suppose we find b, c, d in some radical extension E of F such that

$$f(x) = (x^2 + b)^2 - (cx + d)^2.$$

Then it is clear that f is solvable by radicals over E. Consequently, we will be able to conclude that f is solvable by radicals over F. We need

$$x^4 + (2b - c^2)x^2 - 2cdx + b^2 - d^2 = x^4 + px^2 + qx + r.$$

Thus $2b - c^2 = p$, $-2cd = q$ and $b^2 - d^2 = r$ which gives us

$$b = \frac{p + c^2}{2}, \qquad d = -\frac{q}{2c}, \qquad \left(\frac{p + c^2}{2}\right)^2 - \left(\frac{q}{2c}\right)^2 = r.$$

Expanding the last equation gives a cubic equation for c^2. Thus there is a radical extension E of F containing c and consequently also b and d. □

10.2 Homework 20 — due April 5.

Exercise. Prove that the polynomial $x^5 - 14x + 7$ over $\mathbb{Q}$ has exactly three real roots.

10.3 Solvable groups.

Definition. A group G is *solvable* iff there exists a chain of groups $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{1_G\}$ such that for each $i = 1, \ldots, n$, the group G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is abelian.

Remark. Any abelian group is solvable. If G is an abelian group then the chain $G \supseteq \{1_G\}$ demonstrate solvability of G.

Example. The group S_3 is solvable. The chain $S_3 \supseteq A_3 \supseteq \{1_{S_3}\}$ demonstrate solvability of S_3. The group S_4 is also solvable. That is demonstrated by the chain

$$S_4 \supseteq A_4 \supseteq V \supseteq \{1_{S_4}\},$$

where $V = \{1_{S_4}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. The fact that V is normal in A_4 follows from the fact that it is normal in S_4 which follows from the corollary below.

Cycle shape of a permutation.

Definition. Let n be a positive integer and $\tau \in S_n$. The *cycle shape* of τ is the sequence $(a_1, a_2, \ldots, a_n)$ of nonnegative integers, where a_i is the number of cycles of length i appearing in the unique representation of τ as a product of disjoint cycles.

Proposition. *Let n be a positive integer and $\tau, \sigma \in S_n$. Then τ and σ are conjugate in S_n (there exists $\gamma \in S_n$ such that $\sigma = \gamma\tau\gamma^{-1}$) if and only if the permutations τ and σ have the same cycle shape.*

Proof. Note that if $(b_1\ b_2\ \ldots\ b_m) \in S_n$ is a cycle of length m and $\gamma \in S_n$ is any permutation, then $\gamma(b_1\ b_2\ \ldots\ b_m)\gamma^{-1}$ is the cycle $(\gamma(b_1)\ \gamma(b_2)\ \ldots\ \gamma(b_m))$ which also is of length m. It follows that any conjugate of a permutation τ has the same cycle shape as τ.

Conversely, if $(b_1\ b_2\ \ldots\ b_m)$ and $(c_1\ c_2\ \ldots\ c_m)$ are any two cycles of length m in S_n, then there is a permutation $\gamma \in S_n$ such that $\gamma(b_i) = c_i$ for each $i = 1, 2, \ldots, m$. Then

$$\gamma(b_1\ b_2\ \ldots\ b_m)\gamma^{-1} = (c_1\ c_2\ \ldots\ c_m).$$

A simple modification of that argument shows that if τ and σ have the same cycle shape, then they are conjugate. □

Corollary. *Let n be a positive integer and H be a subgroup of S_n. Then H is normal in S_n if and only if for each cycle shape either H contains all permutations of S_n of that cycle shape, or none of them.*

The relation between solvability of polynomials by radicals and solvable groups.

Remark. Let F be a field of characteristic zero, f be a polynomial over F and K be the splitting field of f over F. We will show that f is solvable by radicals over F if and only if the Galois group of K over F is solvable.

Example. Let $f(x) = x^5 - 14x + 7$ be a polynomial over $\mathbb{Q}$. Note that $f(x)$ is irreducible over $\mathbb{Q}$. Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. We will show later that the group $\mathrm{Aut}_{\mathbb{Q}}(K) = \mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to S_5 (the group of all permutations of the set $\{1, \ldots, 5\}$). We will also show that the group S_5 is not solvable. It will follow that $f(x)$ is not solvable by radicals over $\mathbb{Q}$.

Quotients of solvable groups are solvable.

Lemma. *Let G be a group, H be a normal subgroup of G and N be a subgroup of H that is normal in G. Then H/N is a normal subgroup of G/N and the quotient group $(G/N)/(H/N)$ is isomorphic to G/H.*

Proof. Exercise. □

Remark. The result in the lemma above is often called the Third Isomorphism Theorem for Groups.

Theorem. *Let G be a solvable group and H be a normal subgroup of G. Then the quotient group G/H is also solvable.*

Proof. Let $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{1_G\}$ be such that for each $i = 1, \ldots, n$, the group G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is abelian. Consider the chain

$$G/H = HG_0/H \supseteq HG_1/H \supseteq \ldots \supseteq HG_n/H = H/H = \{H\}$$

of subgroups of G/H.

We want to show, for each $i = 1, 2, \ldots, n$, that HG_i/H is a normal subgroup of HG_{i-1}/H and that the quotient $(HG_{i-1}/H)/(HG_i/H)$ is abelian. It suffices to verify that HG_i is a normal subgroup of HG_{i-1} and the quotient HG_{i-1}/HG_i is abelian. If $h'g' \in HG_i$ and $hg \in HG_{i-1}$, then

$$(hg)(h'g')(hg)^{-1} = hgh'g'g^{-1}h^{-1} = h\left(gh'g^{-1}\right)\left(gg'g^{-1}\right)h^{-1} = hh''\left(g_0h^{-1}g_0^{-1}\right)g_0 = h_0g_0.$$

Since G_i is normal in G_{i-1}, it follows that $g_0 = gg'g^{-1} \in G_i$ and since H is normal in G, it follows that $h'' = gh'g^{-1} \in H$ and $h_0' = g_0h^{-1}g_0^{-1} \in H$. Thus $h_0 = hh''h_0' \in H$ and HG_i is normal in HG_{i-1}.

It remains to show that HG_{i-1}/HG_i is abelian. Let $\varphi : G_{i-1}/G_i \to HG_{i-1}/HG_i$ be defined by $\varphi(gG_i) = gHG_i$. Then φ is well-defined and is a surjective homomorphism. Since the image of an abelian group under a homomorphism is abelian, the result follows. □

10.4 Homework 21 — due April 8.

Exercise. Prove the lemma in section 10.3.

10.5 Subgroups of Finite Symmetric Groups.

Lemma. *Let p be a prime integer, $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p and K be the splitting field of f over $\mathbb{Q}$. Let G be the subgroup of S_p corresponding to the Galois group of K over $\mathbb{Q}$ (treating the automorphism of K over $\mathbb{Q}$ as permutations of the roots of f). Then the following hold.*

1. *G contains a cycle of length p.*

2. *If f has exactly $p-2$ real roots, then G contains a transposition.*

Proof. Let a be a root of f. Then $\left[\mathbb{Q}(a):\mathbb{Q}\right]=p$ implying that $\left[K:\mathbb{Q}\right]$ is divisible by p. Since K is Galois over $\mathbb{Q}$, it follows that $|G|=\left[K:\mathbb{Q}\right]$. Thus $|G|$ is divisible by p and so has an element of order p. Any element of S_p of order p is a cycle of length p.

If f has exactly $p-2$ real roots, then it has two non-real roots one of which is a complex conjugate of the other. The restriction of the complex conjugation to K exchanges the two non-real root and does not move the real roots. Thus G contains a transposition. □

Proposition. *Let p be a prime integer and G be a subgroup of the symmetric group S_p such that G contains a cycle of length p and a transposition. Then $G=S_p$.*

Proof. Let τ be a cycle of length p in G and σ be a transposition in G. Replacing τ with some power τ^i $(1 \le i \le p-1)$ we can assume, without loss of generality, that $\tau=\left(a_0\ a_1\ \dots\ a_{p-1}\right)$ and $\sigma=(a_0\ a_1)$. Note that $\tau\sigma\tau^{-1}=(a_1\ a_2)$ and in general $\tau^j\sigma\tau^{-j}=\left(a_j\ a_{j+1}\right)$ for every $j=1,2,\dots,p-2$. It follows that G contains all transpositions (exercise), hence is equal to S_p. □

10.6 Homework 22 — due April 10.

Exercise. Let n be a positive integer and G be be a subgroup of S_n containing all transpositions of the form $(i\ \ i+1)$ for every $i=1,2,\dots,n-1$. Prove that G contains all transpositions.

10.7 Simple Groups.

Definition. A group G is *simple* if G has exactly two normal subgroup: the trivial subgroup $\left\{1_G\right\}$ and itself.

Remark. An abelian group is simple iff it is isomorphic to $\mathbb{Z}_p$ for some prime p.

Example. There are no simple groups of order 30.

Proof. Let G be a group of order 30. We have $30=2\cdot3\cdot5$. Let n_3 be the number of Sylow 3-subgroups of G and n_5 be the number of Sylow 5-subgroups of G. Then $n_3\equiv1$ modulo 3 and n_3 divides 30. Thus n_3 can only be equal 1 or 10. Similarly, n_5 can only be equal 1 or 6. If $n_3=1$, then the unique Sylow 3-subgroup of G must be normal in G (otherwise its conjugate would be another Sylow 3-subgroup of G) so G is not simple. Similarly if $n_5=1$, then G is not simple. It remains to consider the case when $n_3=10$ and $n_5=6$. Each of the 10 Sylow 3-subgroups of G contains two elements of order 3. Since the intersection of any different Sylow 3-subgroups is trivial (the size of the intersection must divide 3 but not be equal to 3) there are 20 elements of order 3 in G. Similarly, there are $6\cdot4=24$ elements of order 5 in G. Since G has only 30 elements, that is not possible. Thus G is not simple. □

Remark. It can be proved that for any positive integer $n < 60$ that is not a prime, there are no simple group of order n. We will show later that A_5 (the subgroup of S_5 consisting of all even permutations) is simple. Note that $|A_5| = 60$. Thus A_5 is the smallest non-abelian simple group.

Theorem. *Let $n \geq 5$ be an integer. The alternating group A_n is simple.*

Proof. Let H be a nontrivial normal subgroup of A_n. We will show that $H = A_n$. Note that it suffices to show that H contains a cycle of length 3.

(1) If H contains all cycles of length 3, then $H = A_n$.

Proof. Let $\tau \in A_n$. Then $\tau = \tau_1\tau_2 \dots \tau_{2k}$, where each τ_i is a transposition. If τ_{2i-1} and τ_{2i} are not disjoint, then the product $\tau_{2i-1}\tau_{2i}$ is a cycle of length 3. If they are disjoint, then the product $\tau_{2i-1}\tau_{2i}$ is equal to the product of two cycles of length 3. For example $(1\ 2)(3\ 4) = (1\ 2\ 3)(2\ 3\ 4)$. Thus τ is a product of cycles of length 3 and so $\tau \in H$ since H is closed under taking products. □

(2) If H contains at least one cycle of length 3, then $H = A_n$.

Proof. Let $(a\ b\ c) \in H$ and let $(u\ v\ w) \in A_n$ be any cycle of length 3. Then there exists $\tau \in A_n$ such that $(u\ v\ w) = \tau(a\ b\ c)\tau^{-1}$ (exercise). Since H is normal in A_n it follows that $(u\ v\ w) \in H$. Thus H contains all cycles of length 3 and so $H = A_n$ by (1). □

It remains to prove that H must contain a cycle of length 3. Let $\sigma \in H$ be a non-identity element. Consider the representation of σ as a product of disjoint cycles. We are going to consider the following cases:

(a) There is a transposition in the representation of σ.

Let $\sigma = (a\ b)(c\ d\ \dots)\dots$. Let $\tau = (a\ b\ d) \in A_n$. Then

$$\tau\sigma\tau^{-1} = (b\ d)(c\ a\ \dots)\dots \in H$$

and

$$\beta = \sigma^{-1}\tau\sigma\tau^{-1} = (a\ d)(b\ c) \in H.$$

Let $s \in \{1, 2, \dots, n\} \setminus \{a, b, c, d\}$ and $\gamma = (a\ d)(c\ s) \in A_n$. Then

$$\delta = \gamma\beta\gamma^{-1} = (a\ d)(b\ s) \in H$$

implying that $\delta\beta = (b\ c\ s) \in H$. Thus H contains a cycle of length 3.

(b) There is a cycle of length at least 4 in the representation of σ.

Let $\sigma = (a\ b\ c\ d\ \dots)\dots$. Let $\tau = (b\ c\ d) \in A_n$. Then

$$\tau\sigma\tau^{-1} = (a\ c\ d\ b\ \dots)\dots \in H$$

and

$$\sigma^{-1}\tau\sigma\tau^{-1} = (a\ b\ d) \in H.$$

Thus H contains a cycle of length 3.

(c) σ is a product of disjoint cycles of length 3.

Let $\sigma = (a\ b\ c)(u\ v\ w)\dots$. Let $\tau = (a\ u)(b\ v) \in A_n$. Then

$$\tau\sigma\tau^{-1} = (u\ v\ c)(a\ b\ w)\dots \in H$$

and

$$\sigma^{-1}\tau\sigma\tau^{-1} = (b\ v)(c\ w) \in H.$$

It follows from case (a) that H contains a cycle of length 3.

Since in each case we proved that H must contain a cycle of length 3, it follows from (2) that $H = A_n$. □

Corollary. *Let $n \geq 5$ be an integer. The group S_n is not solvable.*

Proof. Let H be a nontrivial proper normal subgroup of S_n. If $H \subseteq A_n$, then H is normal in A_n implying that $H = A_n$ since A_n is simple. Otherwise $HA_n = S_n$ and $H \cap A_n$ is trivial (it is normal in A_n and it cannot be A_n as H is a proper subgroup of S_n). Since HA_n/A_n is isomorphic to $H/(H \cap A_n)$, it follows that $|H| = 2$. Let $\tau \in H$ be the non-identity element. Thus τ is a product of disjoint transpositions. If $(a\ b)$ is a transposition appearing in this representation, and $\sigma = (b\ c)$ for some $c \in \{1, \dots, n\} \setminus \{b, c\}$, then $\sigma\tau\sigma^{-1}$ has the transposition $(a\ c)$ in its representation as the product of disjoint cycles so it does not belong to H contradicting the normality of H.

We have proved that A_n is the only nontrivial proper normal subgroup of S_n. Since A_n is not abelian, it follows that S_n is not solvable. □

10.8 Homework 23 — due April 12.

Exercise. Let $n \geq 5$ and $(a\ b\ c) \in A_n$ be a cycle of length 3. Prove that for every $(u\ v\ w) \in A_n$ there exists $\tau \in A_n$ such that $(u\ v\ w) = \tau(a\ b\ c)\tau^{-1}$.

10.9 From Solvability by Radicals to Solvable Groups.

Proposition. *Let F be a field of characteristic zero, f be a polynomial over F and K be the splitting field of f over F. Then f is solvable by radicals over F if and only if there exists a chain of fields $F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n$ such that*

1. *F_n is Galois over F;*

2. *$K \subseteq F_n$;*

3. *for each $i = 2, \dots, n$ there exists $a_i \in F_i$ and a prime integer p_i such that $a_i^{p_i} \in F_{i-1}$ and $F_i = F_{i-1}(a_i)$;*

4. *F_1 is the splitting field of $x^{p_2 \cdots p_n} - 1$ over $F_0 = F$.*

Proof. If there exists a chain of fields as described, then this chain satisfies, in particular, all the conditions required to demonstrate that f is solvable by radicals over F. Assume now that f is solvable by radicals over F. Then there exists a chain

$$F = F_0' \subseteq F_1' \subseteq \ldots \subseteq F_m'$$

of fields such that f splits over F_m' and for each $i = 1,\ldots,m$ we have $F_i' = F_{i-1}'(a_i)$ for some $a_i \in F_i'$ and a positive integer n_i with $a_i^{n_i} \in F_{i-1}'$. If n_1 is not a prime integer, then $n_1 = q_1 q_2 \ldots q_k$, where $q_1,\ldots,q_k$ are prime integers. Then we can refine the chain between F_0' and F_1' as follows

$$F_0' \subseteq F_0'\left(a_1^{q_2 q_3 \ldots q_k}\right) \subseteq F_0'\left(a_1^{q_3 q_4 \ldots q_k}\right) \subseteq \ldots \subseteq F_0'\left(a_1^{q_k}\right) \subseteq F_1'.$$

Thus we can assume, without loss of generality, that each n_i is a prime integer. Suppose that F^{a} is an algebraic closure of F containing K. Consider all the images of a_1 under the embeddings of F_1' over F_0' into F^{a}. If a_1' is one of them then we can extend the chain by adding $F_{m+1}' = F_m'\left(a_1'\right)$. Note that $\left(a_1'\right)^{n_1} = a_1^{n_1} \in F_0' \subseteq F_m'$. Repeating for all images of a_1, then for all images of a_2, and so on, we get a chain $F = F_0' \subseteq \ldots \subseteq F_t'$ in which the last field F_t' is normal over the F. Let $n = t+1$, p_i be the prime integer such that $F_i' = F_{i-1}'(a_i)$ with $a_i^{p_{i+1}} \in F_{i-1}'$. Let F_1 be the splitting field of $x^{p_2 \cdots p_n} - 1$ over F and let ω be a generator of the group of roots of this polynomial. Then $F_1 = F_0'(\omega)$. Define $F_i = F_{i-1}'(\omega)$ for every $i = 2,3,\ldots,n$. The resulting chain of fields satisfies all the requirements. □

Lemma. *Let G be a cyclic group. Then the group of all the automorphisms of G is abelian.*

Proof. Let g be a generator of G and φ,ψ be automorphisms of G. It suffices to show that $\varphi\psi\left(g\right) = \psi\varphi\left(g\right)$. Let $\varphi\left(g\right) = g^k$ and $\psi\left(g\right) = g^\ell$. Then

$$\varphi\psi\left(g\right) = \varphi\left(g^\ell\right) = \varphi\left(g\right)^\ell = \left(g^k\right)^\ell = g^{k\ell}.$$

Similarly, $\psi\varphi\left(g\right) = g^{\ell k}$ and the proof is complete. □

Theorem. *Let F be a field of characteristic zero.*

(1) *If p is a prime integer such that the polynomial $x^p - 1$ splits in $F[x]$ and $K = F(a)$ for some $a \in F^{\mathrm{a}}$ such that $a^p \in F$, then the group $G = Aut_F(K)$ is cyclic (hence abelian).*

   Proof. If $a \in F$, then G is trivial (hence cyclic). Assume $a \notin F$. Let ω be a generator of the multiplicative group consisting of all the roots of $x^p - 1$. Then $a, a\omega, a\omega^2, \ldots, a\omega^{p-1}$ are all the distinct roots of $x^p - a^p \in F[x]$ and K is the splitting field of $x^p - a^p$ over F and K is Galois over F. In particular, the group G is nontrivial. Let $\varphi \in G$ be any non-identity element and let $k \in \left\{1,2,\ldots,p-1\right\}$ be such such that $\varphi(a) = a\omega^k$. If $\psi \in G$ is any element and $\psi(a) = a\omega^\ell$, where $\ell \in \left\{0,1,\ldots,p-1\right\}$, then there is an integer s such that $sk \equiv \ell$ modulo p so

$$\varphi^s(a) = a\omega^{sk} = a\omega^\ell = \psi(a),$$

   implying that $\psi = \varphi^s$. Thus φ is a generator of G completing the proof that G is cyclic. □

Remark. Note that, it follows that $\varphi, \varphi^2, \ldots, \varphi^p = 1_G$ are all distinct so the group G has order p. Consequently, $[K:F]=p$ and so $x^p - a^p$ is irreducible over F.

(2) *If K is the splitting field of $x^n - 1$ over F for some positive integer n, then $Aut_F(K)$ is abelian.*

Proof. Let G be the set of all the roots of $x^n - 1$ in K. Then G is a finite subgroup of K^* so it is cyclic. Let H be the group of automorphisms of G. The function f : $\mathrm{Aut}_F(K) \to H$ defined by $f\big(\varphi\big) = \varphi \restriction G$ is an injective homomorphism. Thus $\mathrm{Aut}_F(K)$ is isomorphic to the image of f which is a subgroup of H. Since any subgroup of H is abelian, the proof is complete. □

Corollary. *Let F be field of characteristic zero, f be a polynomial over F that is solvable by radicals over F and K be the splitting field of f over F. Then Gal(K/F) is solvable.*

Proof. Since f is solvable by radicals over F there is a chain

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n$$

such that F_n is Galois over F_0, the field K is a subfield of F_n, if $i = 2,3,\ldots,n$, then there is $a_i \in F_i$ and a prime integer p_i with $a_i^{p_i} \in F_{i-1}$, and F_1 is a splitting field of $x^{p_2\cdots p_n} - 1$ over F_0. Then F_i is Galois over F_{i-1} with $\mathrm{Gal}(F_i/F_{i-1})$ being abelian for each $i = 1,2,\ldots,n$. Let $G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n$ the the chain of groups with $G_i = \mathrm{Gal}(F_n/F_i)$ for each $i = 0,1,\ldots,n$. Then G_i is normal in G_{i-1} with G_{i-1}/G_i being isomorphic to $\mathrm{Gal}(F_i/F_{i-1})$, hence abelian, for every $i = 1,2,\ldots,n$. Thus G_0 is solvable. Let $H = \mathrm{Gal}(F_n/K)$. Since K is normal over F, the group $\mathrm{Gal}(K/F)$ is isomorphic to G_0/H which is solvable. □

Example. Let K be the splitting field of the polynomial $f(x) = x^5 - 14x + 7$ over $\mathbb{Q}$. Then $\mathrm{Gal}\big(K/\mathbb{Q}\big)$ is isomorphic to S_5 so it is not solvable. Thus $f(x)$ is not solvable by radicals over $\mathbb{Q}$.

10.10 Homework 24 — due April 19.

Exercise. Let G be a group of order 105. Prove that G is not simple.

10.11 Linear Independence of Characters.

Characters.

Definition. Let X be a set and F be a field. Then F^X (the set of all functions $X \to F$) is a vector space over F. Suppose there is some binary operation of multiplication defined on X (any function $X \times X \to X$ with the image on (a,b) denoted by ab). A function $\sigma : X \to F$ is a *character* in the vector space F^X iff it is not zero (not the constant function assigning 0 to every element of X) and preserves the operation of multiplication, that is, when $\sigma(ab) = \sigma(a)\sigma(b)$ where in F we use the standard multiplication of F as a field.

Theorem (Artin)**.** *Let X be a set with multiplication and F be a field. The set of characters in the vector space F^X is linearly independent.*

Proof. Suppose, to the contrary, that the set of characters in F^X is not linearly independent. Then there are distinct characters $\chi_1, \ldots, \chi_n$ in F^X and $a_1, \ldots, a_n \in F$ not all equal to 0 such that $a_1\chi_1 + \cdots + a_n\chi_n = 0$. Assume that n is as small as possible. Since characters are nonzero functions, we have $n \geq 2$. Since $\chi_1 \neq \chi_2$, there is $b \in X$ such that $\chi_1(b) \neq \chi_2(b)$. Thus for every $c \in X$ we have

$$\begin{aligned} a_1\chi_1(c) + a_2\chi_2(c) + \cdots + a_n\chi_n(c) &= 0, \\ a_1\chi_1(bc) + a_2\chi_2(bc) + \cdots + a_n\chi_n(bc) &= 0. \end{aligned}$$

Multiplying the first equation by $\chi_1(b)$ and using the property that characters preserve multiplication to transform the second equation, we get

$$\begin{aligned} a_1\chi_1(b)\chi_1(c) + a_2\chi_1(b)\chi_2(c) + \cdots + a_n\chi_1(b)\chi_n(c) &= 0, \\ a_1\chi_1(b)\chi_1(c) + a_2\chi_2(b)\chi_2(c) + \cdots + a_n\chi_n(b)\chi_n(c) &= 0. \end{aligned}$$

Subtracting the second equation from the first gives:

$$a_2\big(\chi_1(b) - \chi_2(b)\big)\chi_2(c) + \cdots + a_n\big(\chi_1(b) - \chi_n(b)\big)\chi_n(c) = 0$$

for every $c \in X$. Thus $a_2\big(\chi_1(b) - \chi_2(b)\big)\chi_2 + \cdots + a_n\big(\chi_1(b) - \chi_n(b)\big)\chi_n$ is the zero element of the vector space F^X and $a_2\big(\chi_1(b) - \chi_2(b)\big) \neq 0$ contradicting the minimality of n. □

Corollary. *Let K be a field. Then $Aut(K)$ is a linearly independent subset of the vector space K^K.*

10.12 Norm over a Subfield.

Definition. Let F be a field of characteristic zero and K be a finite extension of F. The *norm* on K over F is a function $N_F^K : K \to F$ defined by $N_F^K(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$, where $\sigma_1, \ldots, \sigma_n$ are all the embeddings of K into K^{a} over F.

Cyclic extensions.

Definition. A field extension K of F is *cyclic* iff it is Galois and the Galois group of K over F is cyclic.

Lemma (Hilbert's Theorem 90)**.** *Let F be a field of characteristic zero and K be a finite cyclic extension of F. Let σ be a generator of $G = Gal(K/F)$ and $\beta \in K$. Then $N_F^K\big(\beta\big) = 1$ if and only if there exists $\alpha \in K^*$ with $\beta = \alpha/\sigma(\alpha)$.*

Proof. If such α exists, then the norm of β is 1. Suppose the norm of β is 1 and let $n = [K : F] = |G|$. Let $\beta_0 = 1$, $\beta_1 = \beta$, $\beta_2 = \beta\sigma\big(\beta\big)$, $\beta_3 = \beta\sigma\big(\beta\big)\sigma^2\big(\beta\big)$, ...,

$$\beta_{n-1} = \beta\sigma\big(\beta\big)\sigma^2\big(\beta\big)\ldots\sigma^{n-2}\big(\beta\big).$$

Note that

$$\beta\sigma(\beta_i)=\beta\sigma(\beta\sigma(\beta)\sigma^2(\beta)\ldots\sigma^{i-1}(\beta))=\beta\sigma(\beta)\sigma^2(\beta)\ldots\sigma^i(\beta)=\beta_{i+1},$$

for every $i=0,1,\ldots,n-2$ and

$$\beta\sigma(\beta_{n-1})=\beta\sigma(\beta)\sigma^2(\beta)\ldots\sigma^{n-1}(\beta)=N(\beta)=1=\beta_0.$$

Since $1_G,\sigma,\sigma^2,\ldots,\sigma^{n-1}$ are distinct characters in the vector space K^K, they are linearly independent implying that the function

$$\beta_0 1_G+\beta_1\sigma+\beta_2\sigma^2+\cdots+\beta_{n-1}\sigma^{n-1}:K\to K$$

is not identically zero. Thus there is $\theta\in K^*$ such that

$$\alpha=\beta_0\theta+\beta_1\sigma(\theta)+\beta_2\sigma^2(\theta)+\cdots+\beta_{n-1}\sigma^{n-1}(\theta)\neq 0.$$

Note that

$$\begin{aligned}\beta\sigma(\alpha) &= \beta\sigma(\beta_0)\sigma(\theta)+\beta\sigma(\beta_1)\sigma^2(\theta)+\cdots+\beta\sigma(\beta_{n-2})\sigma^{n-1}(\theta)+\beta\sigma(\beta_{n-1})\sigma^n(\theta)\\ &= \beta_1\sigma(\theta)+\beta_2\sigma^2(\theta)+\cdots+\beta_{n-1}\sigma^{n-1}(\theta)+\beta_0\theta\\ &= \alpha,\end{aligned}$$

so $\beta=\alpha/\sigma(\alpha)$. □

Primitive roots of 1**.**

Definition. Let F be a field and n be a positive integer. An *primitive n-th root* of 1 is any generator of the multiplicative group consisting of all roots of the polynomial x^n-1 (which is cyclic as a finite subgroup of F^*).

Transitive actions.

Definition. Let G be a group acting on a set X. The action is said to be *transitive* iff there only one orbit (it equal to X then) of the action.

Remark. Let F be a field and K be a splitting field of a polynomial $f(x)\in F[x]$ over F. Consider the action of the group $\mathrm{Aut}_F(K)$ on the roots of $f(x)$ in K. If this action is transitive, then f is irreducible over F.

Corollary. *Let F be a field of characteristic zero with x^n-1 splitting over F. If K is a finite cyclic extension of F with $[K:F]=n$, then there is $\alpha\in K$ such that $K=F(\alpha)$ and $\alpha^n\in F$.*

Proof. Let ζ be a primitive n-th root of 1 in F and G be the Galois group of K over F with generator σ. Then $N(\zeta^{-1})=(\zeta^{-1})^n=1$. Thus $\zeta^{-1}=\alpha/\sigma(\alpha)$ for some $\alpha\in K^*$ so $\sigma(\alpha)=\zeta\alpha$. We have $\sigma(\alpha^n)=(\sigma(\alpha))^n=\alpha^n$ so $\alpha^n\in F$. Since the action of G on the set of roots of $x^n-\alpha^n$ in K is transitive, the polynomial x^n-a^n is irreducible over F and consequently $K=F(\alpha)$. □

10.13 The Commutator Subgroup.

Definition. Let G be a group. The *commutator subgroup* of G is the subgroup generated by the set of all the elements of the form $xyx^{-1}y^{-1}$, where $x, y \in G$. Each such element is called a *commutator.*

Lemma. *The commutator subgroup is normal.*

Proof. Note that conjugating a commutator produces a commutator. Thus the intersection of the commutator subgroup with any of its conjugates contains all the commutators. It follows that the commutator subgroup is normal. □

Proposition. *Let G be a group and H be a normal subgroup of G. Then G/H is abelian if and only if H contains the commutator subgroup of G.*

Proof. Let $g_1, g_2 \in G$. Then the commutator $g_1 g_2 g_1^{-1} g_2^{-1}$ belongs to H if and only if $g_1 g_2 H = g_2 g_1 H$ which holds if and only if

$$\left(g_1 H\right)\left(g_2 H\right) = \left(g_2 H\right)\left(g_1 H\right).$$

Thus G/H is abelian iff H contains all the commutators. □

10.14 More on Solvable Groups.

Proposition. *Let G be a finite group. Then G is solvable if and only if there exists a chain*

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \left\{1_G\right\}$$

of subgroups of G such that G_i is normal in G_{i-1} and G_{i-1}/G_i is cyclic for every $i = 1, 2, \ldots, n$.

Proof. It is clear that if such a chain exists, then G is solvable. Assume that G is solvable. Then there exists a chain

$$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_k = \left\{1_G\right\}$$

of subgroups of G such that H_i is normal in H_{i-1} and H_{i-1}/H_i is abelian for every $i = 1, 2, \ldots, n$. Let $i \in \{1, 2, \ldots, n\}$ and p be a prime integer dividing the order of H_{i-1}/H_i. Then there is a subgroup H' of H_{i-1} containing H_i such that H'/H_i is a subgroup of H_{i-1}/H_i of order p. Then H' is normal in H_{i-1}, H_i is normal in H' and the quotient groups H_{i-1}/H' and H'/H_i are abelian. Then we obtain a chain

$$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_{i-1} \supseteq H' \supseteq H_i \supseteq \ldots \supseteq H_k = \left\{1_G\right\}$$

demonstrating solvability of G with H'/H having order p, hence being cyclic. Repeating that procedure we obtain the required chain of subgroups of G. □

Lemma. *If G is a solvable group, then any subgroup H of G is solvable.*

Proof. If the chain

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_0 = \left\{1_G\right\}$$

demonstrate solvability of G, then

$$H = H_0 \supseteq H_1 \supseteq \ldots \supseteq \{1_H\}$$

demonstrate solvability of H, where $H_i = G_i \cap H$. It is clear that $H_{i-1} \cap H$ is normal in $H_i \cap H$. The group $H_{i-1} \cap H / H_i \cap H$ is abelian since all the commutators of $H_{i-1} \cap H$ belong to $H_i \cap H$. □

Theorem. *Let G be a group and H be a normal subgroup of G. The following conditions are equivalent.*

1. *G is solvable.*

2. *Both H and G/H are solvable.*

Proof. Assume that G is solvable. We have already proved that both H and G/H are solvable. Now assume that both H and G/H are solvable. Let

$$H = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_k = \{1_H\}$$

demonstrate solvability of H and

$$G/H = G_0/H \supseteq G_1/H \supseteq \ldots \supseteq G_n/H = \{H\}$$

demonstrate solvability of G/H. Then

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_k = \left\{1_G\right\}$$

demonstrates solvability of G. □

10.15 From Solvable Group to Solvability by Radicals.

Theorem. *Let F be a field of characteristic zero, f be a polynomial over F and K be the splitting field of f over F with $G = Gal(K/F)$ The following conditions are equivalent.*

1. *The polynomial f is solvable by radicals over F.*

2. *The group $Gal(K/F)$ is solvable.*

Proof. We only need to prove that 2. implies 1. Assume that $\mathrm{Gal}(K/F)$ is solvable. Let $n = [K : F] = |G|$, let E be a splitting field of the polynomial $x^n - 1$ over F and let $L = KE$ be the join of the fields K and E. Then L is Galois over F. Let $G = \mathrm{Gal}(L/F)$ and $H = \mathrm{Gal}(L/K)$. Then $\mathrm{Gal}(K/F)$ is isomorphic to the quotient group G/H. Since L is radical over K, the group H is solvable. Since both G/H and H are solvable, it follows that G is solvable and consequently its subgroup $J = \mathrm{Gal}(L/E)$ is also solvable. Let

$$J = J_0 \supseteq J_1 \supseteq \ldots \supseteq J_k = \left\{1_J\right\}$$

be such that J_i is normal in J_{i-1} with J_{i-1}/J_i being cyclic for each $i = 1, 2, \ldots, k$. Let

$$E = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_k = L$$

be the corresponding chain of subfields of L. Then, for every $i = 1, 2, \ldots, k$, the field E_i is cyclic over E_{i-1} so there is $a_i \in E_i$ and a positive integer n_i such that $a_i^{n_i} \in E_{i-1}$ and $E_i = E_{i-1}(a_i)$. Thus L is a radical extension of F containing K completing the proof. □

Index