Abstract Algebra I Notes

UIUC MATH 500, F'08

Jingjin Yu

1 Groups

08/25/08 - 08/27/08

Definition 1.1 Semigroups, monoids, groups, rings and commutative rings. For a map $G \times G \to G$, consider the following properties:

1) Closure,
2) Association,
3) Identity,
4) Inverse,
5) Commutative.

A set G with a composition law $G \times G \to G$ is called :

a ***semigroup*** if it satisfies 1-2,
a ***monoid*** if it satisfies 1-3,
a ***group*** if it satisfies 1-4,
a ***abelian group*** if it satisfies 1-5.

Definition 1.2 A ***subgroup*** H of group G is a subset of G that is also a group with the same map of $G \times G \to G$.

Example 1.3 $\mathbb{Z} > 0$: semigroup; $\mathbb{Z} \geqslant 0$: monoid; $\mathbb{Z}$: group.

Definition 1.4 A group ***homomorphism*** is a function $f : G \to H$ s.t. $f(xy) = f(x)f(y)$. If f is injective, surjective, and bijective, then we call them ***monomorphism***, ***epimorphism***, ***isomorphism***.

Example 1.5 $(\mathbb{Z}, +) \to (\mathbb{Q}, +)$ is an injective homomorphism; but there does not exist a nonzero homomorphism $(\mathbb{Q}, +) \to (\mathbb{Z}, +)$. Suppose not then $f(1) \neq 0$ and $nf(1/n) = f(n \cdot 1/n) = f(1) \Rightarrow f(1/n) \neq 0$. But no matter what $f(1)$ is, it cannot be infinity and there are some n such that $0 < f(1)/n = f(1/n) < 1$. This is not possible since $f(1/n) \in \mathbb{Z}$.

Definition 1.6 A permutation of a set X is a bijection $X \to X$:

$$\begin{pmatrix} 1 \ldots\ldots n \\ a_1 \ldots\ldots a_n \end{pmatrix}$$

Definition 1.7 The ***symmetric group*** on a set X is the collection of all permutations on X with notation $\text{Symm}(X)$. If $X = \{1, \ldots, n\}$, we write S_n for $\text{Symm}(X)$.

Remark. We have injection $\phi : S_n \to S_{n+1}$ by extending any permutation f with $f(n+1) = n+1$. We may define $S_\infty = \cup_{n=1}^{\infty} S_n$. If we let $X = \{1, 2, \ldots\}$, then $S_\infty \neq \text{Symm}(X)$ since the permutation $\sigma = (2, 1, 4, 3, 6, 5 \ldots) \in \text{Symm}(X)$, but $\sigma \notin S_\infty$.

Theorem 1.8 Let $f : G \to H$ be a homomorphism.

(1) f is a monomorphism if and only if $\ker f = \{e\}$.

(2) f is an isomorphism if and only if there eixsts a homomorphism f^{-1} s.t. $f \cdot f^{-1} = 1_H, f^{-1} \cdot f = 1_G$.

PROOF.

(1) ($\Rightarrow$) Clear. ($\Leftarrow$) Suppose $f(x) = f(y)$, then $f(xy^{-1}) = f(1) = 1_H$, by assumption $xy^{-1} = 1 \Rightarrow x = y$.

(2) ($\Rightarrow$) f is invertible, we just need to verify that it is a homomorphism: $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$. ($\Leftarrow$) Clear.

■

08/29/08

Definition 1.9 let $a_1, \ldots, a_r$ be distinct elements of $X = \{1, 2, \ldots, n\}$, and let $Y = X \backslash \{a_1, \ldots, a_r\}$. If $f \in S_n$ fixes every element in Y and $f(a_i) = a_{i+1}$ for $i = 1, r-1$ and $f(a_r) = a_1$, then f is called an r***-cycle*** and we write $f = (a_1, \ldots, a_r)$. A 2-cycle is called a ***transposition***.

Definition 1.10 Two permutations α, β are disjoint if

(1) $\alpha(k) \neq k \Rightarrow \beta(k) = k$, and

(2) $\beta(k) \neq k \Rightarrow \alpha(k) = k$.

Proposition 1.11 Every permutation $\alpha \in S_n$ is a composite (product) of disjoint cycles.

PROOF. By induction on the number of elements that moved by α.

(case $m = 0$) $\alpha = (1)$ is the identity.

(case $m > 0$) Choose a_1 with $\alpha(a_1) \neq a_1$ and let $a_2 = \alpha(a_1), \ldots a_{i+1} = \alpha(a_i)$ until we have $a_l \in \{a_1, \ldots, a_{l-1}\}$. We claim that $a_l = a_1$. Suppose not and $a_l = a_i, 1 < i < l$, then $a_l = \alpha(a_{l-1})$ and $a_i = \alpha(a_{i-1})$, which imply that $a_{l-1} = a_{i-1}$, contradicting that a_l is the first repetition.

We may then get a cycle that is disjoint from the rest of the permutation and apply induction hypothesis. ■

Definition 1.12 G is a group and $a, g \in G$, then gag^{-1} is a conjugate of a.

Example 1.13 $G = S_n$, let $\alpha = (a_1, \ldots, a_n) \in S_n$, then for $\tau \in S_n, \tau\alpha\tau^{-1} = (\tau(a_1), \ldots, \tau(a_n))$.

If $a \notin \{\tau(a_i)\}$, then $\tau^{-1}(a) \notin \{a_i\}$, hence it is fixed by α and $\tau\alpha\tau^{-1}(a) = \tau(\tau^{-1}(a)) = a$. On the other hand, if $a = \tau(a_i)$, then $\tau\alpha\tau^{-1}(a) = \tau(\alpha(a_i)) = \tau(a_{i+1})$. Therefore $\tau\alpha\tau^{-1} = (\tau(\alpha_1), \ldots, \tau(\alpha_n))$.

Definition 1.14 An automorphism is an isomorphism between a group G and itself.

Proposition 1.15 Define $\Phi_g : G \to G, a \mapsto gag^{-1}$, Φ_g is an automorphism.

PROOF. gag^{-1} a homomorphism since $gabg^{-1} = gag^{-1}gbg^{-1}$. Obviously Φ_g is surjective; it is injective since $gag^{-1} = gbg^{-1} \Rightarrow a = b$. ■

Definition 1.16 $\mathrm{Inn}(G) = \{\Phi_g : g \in G\}$ is the set of inner automorphism.

Definition 1.17 A subgroup K of G is normal if $gkg^{-1} \in K$ for all $g \in G, k \in K$.

Lemma 1.18 K is normal if and only if $gK = Kg$ for all $g \in G$.

Theorem 1.19 $K \lhd G$ then $aKbK = abK$ for all $a, b \in G$.

Definition 1.20 The collection $G/K = \{gK : g \in G\}$ forms a group that is the ***quotient group*** of G over K.

Theorem 1.21 (First isomorphism theorem) Let $f : G \to H$ be homomorphism of groups, then

$$G/\ker f \simeq \mathrm{im} f$$

and $\ker f \lhd G$, $\mathrm{im} f \subseteq H$.

Theorem 1.22 (Second isomorphism theorem) Let $K \subseteq G$, $N \lhd G$, then KN is a subgroup of G, $N \cap K \lhd K$ and

$$NK/N \simeq K/(N \cap K)$$

.

Theorem 1.23 (Third isomorphism theorem) Let $K, N \lhd G, K \subseteq N$ then N/K is normal in G/K and

$$(G/K)/(N/K) \simeq (G/N)$$

.

09/03/08

Lemma 1.24 Every $\sigma \in S_n$ is a product of transpositions.

PROOF. We get the disjoint cycles and then from them it is easy to get the transpositions. ■

Definition 1.25 If G is a group and X is a set, then a ***(left) group action*** of G on X is a binary function $G \times X \to X$ denoted $(g, x) \mapsto g \cdot x$ which satisfies associativity and $e \cdot x = x$ for all $x \in X$.

Definition 1.26 ***Orbit*** of $x \in X$ is $O(x) = \{gx : g \in G\}$. Stablizer $G_x = \{g \in G : x = gx\}$.

Proposition 1.27 If G acts on a set X, then

$$|X| = \sum_i |O(x_i)|,$$

in which different $O(x_i)$'s are pairwise disjoint.

Remark. Every transposition is a conjugate of another one. Conjugation take a r-cycle to another r-cycle. Conjugation takes subgroups to subgroups.

09/05/08 - 09/08/2008

Remark. Category: see notes. Low importance for now.

09/10/08

Definition 1.28 For $G = \langle X|R\rangle$, G is ***finitely generated*** if there exists a presentation such that X is finite. G is ***finitely presented*** if more over R is finite.

Lemma 1.29 (1) Let $H \subseteq G$ be a subgroup then H acts on G on the right. The orbit of $g \in G$ is the ***left coset*** $gH = \{gh : h \in H\}$; G is a disjoint union of left cosets g^H.

Lemma 1.30 (2)Let now $X = G/H = \{kH : k \in G\}$, then G acts on X on the left by $G \times X \to X, (g, kH) \mapsto gkH$.

Lemma 1.31 (3)Let G be a finite group and $H \subseteq G$ a subgroup, then $gH \to H, k \mapsto g^{-1}k$ is a bijection and $|gH| = |H|$ for all $g \in G$.

Definition 1.32 For a subgroup $H \subseteq G$, the number of left cosets of H is called the ***index*** of H in G, denoted $[G : H]$.

Theorem 1.33 (Lagrange) For a finite group G and a subgroup H,

$$[G : H] = |G|/|H|.$$

Proof. From (3) we know cosets are of size $|H|$ and they are disjoint by (1). Therefore, the number of them is $|G|/|H|$. The proof of (1), (2), and (3) are trivial. ■

Definition 1.34 For a subgroup H of group G, $N_G(H)$ is the ***normalizer*** of H in G. That is, $N_G(H)$ is the largest subgroup of G such that $H \lhd N_G(H)$.

Corollary 1.35 The number of conjugates gHg^{-1} of H is $[G : N_G(H)]$.

PROOF. We first show that if G acts on a set X, then $|O(x)| = [G : G_x]$. G_x is a subgroup of G, by Lagrange, $G/G_x = [G : G_x]$. We wish to establish a bijection between $G/G_x = \{gG_x\}$ and $O(x)$ (not a homomorphism). We may define $\varphi : gG_x \mapsto gx$ as the mapping. It is well defined since $gG_x = hG_x \Rightarrow g = hfx$ for some $f \in G_x$; but then $fx = x$ hence $gx = hx$. φ is an injection since if $gx = hx$, then $h^{-1}gx = x \Rightarrow h^{-1}g \in G_x \Rightarrow h^{-1}gG_x = G_x \Rightarrow gG_x = hG_x$. φ is obviously surjective. Therefore it is a bijection.

With above, and the fact that G acts on H with conjugation with stablizer is $N_G(H)$. Here our set is $X = \{gHg^{-1}\}$ and we let $x = H$. ■

09/12/08 - 09/15/2008

Theorem 1.36 (Cauchy) If $|G|$ has a prime p as a factor, then G has an element of order p.

SKETCH OF PROOF. If G is abelian with trivial center, then the abelian case of Cauchy applies. For G with non-trivial center, we prove via induction over $|G|$. If $|G| = p$, then it is obvious. If not, let $|G| = mp$ and for any $x \in G$, check the centralizer G_x. This is a subgroup of G and if $p \mid |G_x|$, induction gives that G_x has an element of order p. If this is not the case for all G_x, then p does not divide $\sum_i [G : G_{x_i}]$ and by $|G| = |C(G)| + \sum_i [G : G_{x_i}]$, the center $C(G)$ contain p as a factor. The induction hypothesis again applies. ■

Lemma 1.37 $|G| = p^2$, p prime, then G is abelian.

PROOF. G has nontrivial center since otherwise $|G| = 1 + \sum_i [G : G_{x_i}]$ but then $p^2 = 1 + mp$. If $|C(G)| = p^2$ we are done since its G and abelian. If $|C(G)| = p$ (cyclic and abelian, by definition of center), $C(G)$ is normal in G, $G/C(G)$ is of order p and is cyclic; let $\langle aC(G)\rangle$ be a generator of the quotient group. Now for any $g_1, g_2 \in G$, $g_1 \in (aC(G))^{n_1}, g_2 \in (aC(G))^{n_2}$ for some n_1, n_2. Then $g_1 = a^{n_1}c_1^{n_1}, g_1 = a^{n_2}c_2^{n_2}$ for some $c_1, c_2 \in C(G)$. Then $g_1g_2 = a^{n_1}c_1^{n_1}a^{n_2}c_2^{n_2} = a^{n_1+n_2}c_1^{n_1}c_2^{n_2} = a^{n_2}c_2^{n_2}a^{n_1}c_1^{n_1} = g_2g_1$. G is then abelian. ■

Definition 1.38 A ***Sylow p-subgroup*** of a finite group G is a maximal p-subgroup P.

Lemma 1.39 (5.33) Let P be a Sylow p-subgroup of a finite group G, then

(1) Every conjugate of P is again a Sylow p-subgroup.

(2) $|N_G(P)/P|$ is prime to P.

(3) If $a \in G$ has order some powers of p and if $aPa^{-1} = P$, then $a \in P$.

PROOF.

(1) Suppose $Q = gPg^{-1}$ is not Sylow (not maximal), then $|Q| < |P|$ but $P = g^{-1}Qg$ implies $|P| \leqslant |Q|$. Contradiction.

(2) Suppose not, then $|N_G(P)/P|$ contains p as a factor and by Cauchy, $N_G(P)/P$ contains an element aP of order p. $\langle aP\rangle$ is then a subgroup of $N_G(P)/P$ of order p. The elements of $P, aP, a^2P, \ldots, a^{p-1}P$ is a subgroup of $N_G(P)$. Therefore, P is not Sylow.

(3) $aPa^{-1} = P \Rightarrow a \in N_G(P)$; but by (2) a cannot be of order divisible by p.

■

Theorem 1.40 (5.34) Let G be a finite group of order $p_1^{e_1} \dots p_t^{e_t}$, and let P be a Sylow p-subgroup of G for some prime $p = p_j$.

(1) Every Sylow p-subgroup is conjugate to P.

(2) If there are r_j Sylow p_j-subgroups, then r_j is a divisor of $|G|/p_j^{e_j}$ and $r_j \equiv 1 \mod p_j$.

PROOF.

(2) Let $X = \{P_1 = P, P_2, \dots, P_{r_j}\}$ be the Sylow p-subgroups conjugate to P. Let Q be any Sylow p-subgroup of G, let it act on X by conjugation. The orbit of an element of X, P_i, satisfies $|O(P_i)| = [Q : Q_{P_i}]$. If we let $Q = P$, the only orbit of size 1 is $O(P)$; this is true because for any $P_i \neq P$, if $a \in P$ makes $aP_ia^{-1} = P_i$, then by 5.33(3) $a \in P_i$. Therefore there must be some $a \in P$ s.t. $aP_ia^{-1} \neq P_i$, otherwise $P = P_i$. This gives us that $r_j = |X| = 1 + pm \equiv 1 \mod p$.

(1) If $Q \notin X$ is a Sylow p-subgroup, then above would suggest that $|X| \equiv 0 \mod p$, contradiction.

■

Corollary 1.41 A finite group G has a unique Sylow p-subgroup P for some prime p iff $P \lhd G$.

PROOF. ($\Rightarrow$) For $g \in G$, if $Q = gPg^{-1} \neq P$, then Q is another Sylow p-subgroup, contradicting that P is unique. Therefore $gPg^{-1} = P$ for all $g \in G$, $P \lhd G$. ($\Leftarrow$) Since for all $g \in G, gPg^{-1} = P$, P has no conjugate and is unique. ■

Theorem 1.42 (Sylow, 5.36) If G is a finite group of order $p^e m$ in which p is prime and $p \nmid m$, then every Sylow p-subgroup of G has order p^e.

PROOF. $[G : P] = [G : N_G(P)][N_G(P) : P]$. We know the number of conjugates of P in G is $[G : N_G(P)]$ and $p \nmid [G : N_G(P)]$. P is the unique Sylow p-subgroup in $N_G(P)$ by previous corollary, so $p \nmid [N_G(P) : P]$. Therefore $p \nmid [G : P]$, and the rest follows. ■

09/17/08

Theorem 1.43 $|G| = mp^e$, $p \nmid m$, then there is a Sylow p-subgroup of G with order p^e.

Theorem 1.44 Let G be a group of order $|G| = p_1^{e_1} p_2^{e_2} \dots$ for distinct primes s.t. there is a single Sylow p-subgroup for $p = p_1, p_2, \dots, p_k$. Then $G \simeq P_1 \times P_2 \times \dots$.

Remark. See notes for proofs.

Definition 1.45 A ***normal series*** of a group G is a sequence of subgroups such that

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = \{1\},$$

The ***factor groups*** of this series are the quotient groups

$$G_0/G_1, G_1/G_2, \ldots, G_{n-1}/G_n.$$

A group is called ***solvable*** if it has a normal series with all factor groups having prime order.

Definition 1.46 A ***composition series*** is a normal series with simple factor groups. The ***composition factors*** are the non-trivial factors.

Proposition 1.47 Every finite group has a composition series

PROOF. Proof via induction. Let G be a smallest such group; take H be its maximal normal subgroup such that G/H is simple (existence by the remark below). Then H has a composition series and G as well. Contradiction. ■

Remark. Correspondence theorem is useful $G_1/H \lhd G_0/H \Leftrightarrow G_1 \lhd G_0$ with H normal in G_0.

09/19/08 - 09/22/08

Definition 1.48 ***Refinement*** of a normal series $\{G_i\}$ is a sequence $\{N_j\}$ that contains the original sequence as a subsequence.

Lemma 1.49 (Zassenhaus Lemma, Butterfly Lemma) Given four subgroups $A \lhd A^*, B \lhd B^*$ of a group G, then $A(A^* \cap B) \lhd A(A^* \cap B^*), B(B^* \cap A) \lhd B(B^* \cap A^*)$ and there is an isomorphism

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \simeq \frac{B(B^* \cap A^*)}{B(B^* \cap A)}.$$

Theorem 1.50 (Schreier Refinement Theorem) Any two normal series for a group G have equivalent refinements.

Theorem 1.51 (Jordan-Holder) Any two composition series of a group G are equivalent.

Remark. The above theorems can be proved in that sequence.

Lemma 1.52 Let P be a sylow p-subgroup of G, and let $N = N_G(p)$, then $N_G(N) = N$.

PROOF. Let $x \in N_G(N)$, then $xNx^{-1} = N$ and $xPx^{-1} = P' \subseteq N$ since $P \subseteq N$. P is normal in N, hence it is the only Sylow p-group in N (since all Sylow p-groups of G are conjugates); therefore $P = P'$ and $xPx^{-1} = P \Rightarrow x \in N_G(P) = N$. ■

Lemma 1.53 In a group with $\gamma_n(G) = \{e\}$, the only subgroup H with $N_G(H) = H$ is $H = G$.

PROOF. We show that if $H \subsetneq G$, then $H \subsetneq N_G(H)$. Since $H \neq G$ and $G = \gamma_0(G) \geqslant \gamma_1(G) \geqslant \ldots \geqslant \gamma_n(G) = \{e\}$, $\exists i$ s.t. $H \subsetneq \gamma_i$ and $\gamma_{i+1} \subseteq H$. Let $a \in \gamma_i \backslash H$, then for any $g \in G$, $[g, a] = gag^{-1}a^{-a} \in \gamma_{i+1} \subseteq H$. If $g = h \in H$, we have $hah^{-1}a^{-1} = h'$ for some $h' \in H$. Then $ah^{-1}a^{-1} = h^{-1}h' \in H \Rightarrow aHa^{-1} \subseteq H \Rightarrow a \in N_G(H)$. But $a \notin H$, so $H \subsetneq N_G(H)$. ■

Lemma 1.54 A group if nilpotent if and only if the derived series stablize at the identity. TFAE:

(1) The group G has a descending central series with $\gamma_n(G) = \{e\}$ from some n.

(2) The group G is a direct product of its p-subgroups ($\Leftrightarrow$ Every Sylow p-subgroup is normal in G).

PROOF.

(1) $\Rightarrow$ (2): For any Sylow p-subgroup P of G, let $N = N_G(P)$. By Lemma 1.52, $N_G(N) = N$. By Lemma 1.53, $N_G(N) = N \Leftrightarrow N = G$. So $N_G(P) = G$, implying that every Sylow p-subgroup is normal in G. Let the Sylow p-subgroups be $P_1, \ldots, P_n$. We have $P_i \cap P_j = \{1\}$ for $i \neq j$ since any non-zero element of P_i must have order greater than 1 and divides p_i, therefore P_i, P_j cannot share any non-zero elements. Take any elements $a_i \in P_i, a_j \in P_j$, since $a_i P_j a_i^{-1} = P_j$, $a_i a_j a_i^{-1} = a_j' \Rightarrow a_i a_j a_i^{-1} a_j^{-1} = a_j' a_j^{-1} \in P_j$. Similarly, $a_j a_i^{-1} a_j^{-1} = a_i' \Rightarrow a_i a_j a_i^{-1} a_j^{-1} = a_i a_i' \in P_i$. This implies $a_i a_j a_i^{-1} a_j^{-1} = 1 \Rightarrow a_i a_j = a_j a_i$. Thus any element of G can be expressed uniquely in the form $a_1 a_2 \ldots a_n$, meaning that G is a direct product of its p-subgroups.

(2) $\Rightarrow$ (1): We only need to show that each P_i is nilpotent, the direct product properties then that G is nilpotent as well. So we only need to show that any p-group is nilpotent, which is proved in the next three results.

■

Lemma 1.55 If G is a nilpotent group, then $Z(G) \neq \{1\}$.

PROOF. If G is nilpotent, then from the lower central series, there exists $\gamma_i \subset G$, $[\gamma_i, G] = \{1\}$. For any element $g_i \in \gamma_i, g \in G$, $g_i g g_i^{-1} g^{-1} = 1 \Rightarrow g_i g = g g_i$. Since $\gamma_i \neq \{1\}$, $Z(G) \neq \{1\}$. ■

Lemma 1.56 If $G/Z(G)$ is nilpotent, then G is nilpotent.

PROOF. $G \cong G/Z(G) \times Z(G)$. Let the lower central series of G be $\{\gamma_i\}$ and that of $G/Z(G)$ be $\gamma_1', \ldots, \gamma_i', \ldots, \gamma_n'$. We show inductively that $\gamma_i Z(G)/Z(G) \subseteq \gamma_i'$. We have $\gamma_{i+1} Z(G)/Z(G) = [\gamma_i, G] Z(G)/Z(G)$. An element of $[\gamma_i, G] Z(G)/Z(G)$ has the form

$$g_i g g_i^{-1} g^{-1} Z(G) = g_i Z(G) g Z(G) g_i^{-1} Z(G) g^{-1} Z(G)$$

hence

$$\gamma_{i+1} Z(G)/Z(G) = [\gamma_i, G] Z(G)/Z(G) \subseteq [\gamma_i Z(G)/Z(G), G/Z(G)] \subseteq [\gamma_i', G/Z(G)] = \gamma_i'.$$

This gives us that $\gamma_n \subseteq Z(G)$ and $\gamma_{n+1} = \{1\}$. ■

Corollary 1.57 Every p-group is nilpotent.

PROOF. Let P acts on itself via conjugation, it is easy to see that P has non-trivial center and this is true for all $P/Z(P)$ (also p-group). We can apply the previous lemma inductively to get that P is nilpotent. ■

Lemma 1.58 A group is solvable if and only if the lower central series stablizes at the identity, or TFAE:

(1) The group G has a derived series with $G^{(n)} = \{e\}$ for some n.

(2) The composition factors of G are cyclic of prime order.

PROOF.

(1) $\Rightarrow$ (2): Derived series has abelian factor groups, the refinement then gives what we need. Let $F_1 = G^{(0)}/G^{(1)}$, then F_1 is abelian; it then has a normal series with prime factors since all subgroups of an abelian group are normal. Applying correspondence theorem then gives us the refinement from $G^{(0)}$ to $G^{(1)}$ we need.

(2) $\Rightarrow$ (1): Assume that G has a normal series $G = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_n = \{e\}$ with prime (cyclic and abelian) factor groups. We need to show that $G^{(i)} \subseteq G_i$. This is straightforward by Jordan-Holder: the refinement of $G^{(0)} \rhd G^{(1)} \rhd \ldots$ is the same as $G = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_n = \{e\}$; since there are no normal subgroups between G and G_1, we have the conclusion.

■

Proposition 1.59 A nilpotent group G is solvable.

PROOF. Nilpotent $\Rightarrow$ $G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \ldots \geqslant \gamma_n(G) = \{e\}$ for some n. For derived series, $G = G^{(0)} \geqslant G^{(1)} \geqslant \ldots$, we have $[G_{i-1}, G_{i-1}] = G^{(i)} \subseteq \gamma_{i+1}(G) = [G, \gamma_i(G)]$. So $G^{(n-1)} \leqslant \gamma_n(G) = \{e\}$. ■

Lemma 1.60 G solvable then its subgroups are solvable.

PROOF. $H \subseteq G$, then the derived series of H is contained in the derived series of G and must reach $\{e\}$. ■

Lemma 1.61 G is solvable, $N \lhd G$, then G/N is solvable.

PROOF. $N \lhd G$, then $G \geqslant N \geqslant 1$ refines to the normal series of G: $G^0 \geqslant G^1 \geqslant \ldots \geqslant N \geqslant \ldots \geqslant 1$. $G^0/N \geqslant G^1/N \geqslant \ldots \geqslant N/N$ gives us the normal series of G/N. ■

Lemma 1.62 G a group, $N \lhd G$, $N, G/N$ both solvable, then G is solvable.

PROOF. Show that $G^i N/N \leqslant (G/N)^i$, this gives that for some k, $G^k N/N = N/N$ hence $G^k \subseteq N$. Since N normal, G^k has a normal series that completes the whole normal sereis of G. ■

Theorem 1.63 The direct product of nilpotent groups is again nilpotent.

PROOF. This is straightfoward if we go to lower central series. ■

2 Rings

09/24/08

Remark. For the material covered here, the role of ***prime*** and ***maximal*** ideals are very important; for the part involving PID/UFD, irreducible element generates prime ideal is key to many proofs. The noetherian properties are introduced at last; with Zorn's lemma, some additional results can be proved.

Definition 2.1 Semigroups, monoids, groups, rings and commutative rings.
For a map $G \times G \to G$, consider the following properties:
1) Closure,
2) Association,
3) Identity,
4) Inverse,
5) Commutative.

A set G with a composition law $G \times G \to G$ is called :
a ***semigroup*** if it satisfies 1-2,
a ***monoid*** if it satisfies 1-3,
a ***group*** if it satisfies 1-4,
a ***abelian group*** if it satisfies 1-5.

A ***ring*** R is a set together with two maps:
$+ \quad : R \times R \to R$ (addition), and
$. \quad : R \times R \to R$ (multiplication),
such that the set R is an abelian group under addition (satisfying properties 1-5) and a monoid under multiplication (satisfying properties 1-3). Also, the distributive law holds:

$$a(b+c) = ab + ac, \forall a, b, c \in R$$

R is an ***commutative ring*** if the multiplication is commutative.

Example 2.2 Example of rings.
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings. $\mathbb{Q}[x]$ is the ring of polynomials in the variable x, with coefficients in $\mathbb{Q}$.
$2\mathbb{Z}$ is ***not*** a ring since there is no multiplicative identity.
$\mathbb{Z}/n\mathbb{Z}$ is a commutative ring.
$\{\bar{0}, \bar{2}, \bar{4}\} = 2\mathbb{Z}/6\mathbb{Z} \subseteq \mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$, $\mathbb{Z}/6\mathbb{Z}$ and $2\mathbb{Z}/6\mathbb{Z}$ are rings. $1_R = \bar{4}$ in $2\mathbb{Z}/6\mathbb{Z}$:

	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

Definition 2.3 . A subset $S \subseteq R$ of a ring R is called a ***subring*** if
1) $a - b \in S, \forall a, b \in S$,
2) $ab \in S, \forall a, b \in S$, and
3) $1_S = 1_R$.

If S is a subring, then S is itself a ring.

Example 2.4 Subring.
$\mathbb{Z}$ is a subring of $\mathbb{Q}$.
$S = 2\mathbb{Z}/6\mathbb{Z}$ is a ring, but it is not a subring of $R = \mathbb{Z}/6\mathbb{Z}$ because $\bar{4} = 1_S \neq 1_R = \bar{1}$.

Definition 2.5 An ***integral domain*** is a commutative ring R with :
1) $1_R \neq 0_R$, and
2) $\forall a, b \in R, ab = 0 \Rightarrow a = 0$ or $b = 0$.

Remark. The second criterion above is equivalent to for $a, b, c \in R, c \neq 0$, then $ac = bc \Rightarrow a = b$. That is, the ***cancellation law*** holds.
Property 2) in the above definition is equivalent to saying that for $a, b, c \in R, ac = bc, c \neq 0 \Rightarrow a = b$.

Definition 2.6 $\forall a, b \in R$, we say b ***divides*** a in R if there exists $q \in R$ such that $a = qb$ (if R is commutative, $a = qb = bq$). A divisor of 1_R is called a ***unit***; a divisor of 0_R is called a zero divisor if $q \neq 0$.

With above definition, if b is a unit, then $qb = 1_R$ for some $q \in R$.

Example 2.7 Let $R = \mathbb{Z}/2\mathbb{Z}$,
$a \in R$ is a unit $\Leftrightarrow (a, n) = 1$,
$a \in R$ is a zero $\Leftrightarrow (a, n) \neq 1$.

Definition 2.8 A ***field*** is a commutative ring with $1 \neq 0$ such that every non-zero element is a unit.

Proposition 2.9 Every field is an integral domain.

PROOF. Let F be a field and $a, b \in F$ s.t. $ab = 0$. Suppose that $a \neq 0$, then a is a unit in F with $qa = 1_F$. Therefore, $b = 1b = qab = q0 = 0$. ■

Proposition 2.10 Every ***finite*** integral domain is a field.

PROOF. Let R be the domain and $a \in R, a \neq 0$. Define a homomorphism $f : R \to R$ by $f : x \mapsto ax$. The map is well defined since every element x is mapped to ax (not one to many). The map is an injection since $ax = ay \Rightarrow a(x - y) = 0$; R is a domain so $a \neq 0 \Rightarrow x - y = 0 \Rightarrow x = y$. Since the map is from finite R to R and injective, it is also surjective.
Since the map is a bijection, there exist $x \in R, ax = 1_R$. Hence a is a unit. ■

Example 2.11 Integral domains that are not fields: $\mathbb{Z}$, $\mathbb{Q}[x]$.

Remark. [***the following till next lecture not covered in class***] Every subring of a domain is then itself a domain since the cancellation law carries over to the subring. Since fields are domains, it follows that every subring of a field is a domain. The converse is also true: every domain is a subring of a field. We have:

Theorem 2.12 If R is a domain, then there is a field F containing R as a subring. Moreover, F can be chosen s.t. for each $f \in F$, there are $a, b \in R$ with $b \neq 0$ and $f = ab^{-1}$ (b^{-1} is the multiplicative inverse of b).

Remark. In section 3.4 of text, we have the following results:

Theorem 2.13 Assume that k is a field and that $f(x), g(x) \in k[x]$ with $f(x) \neq 0$. Then there are unique polynomials $q(x), r(x) \in k[x]$ with

$$g(x) = q(x)f(x) + r(x)$$

and either $r(x) = 0$ or $\deg(r) < \deg(f)$.

Corollary 2.14 Assume that R is a field and that $f(x), g(x) \in R[x]$ with $f(x) \neq 0$ is a monic polynomial. Then there exist $q(x), r(x) \in k[x]$ with

$$g(x) = q(x)f(x) + r(x)$$

and either $r(x) = 0$ or $\deg(r) < \deg(f)$.

Lemma 2.15 Let $f(x) \in k[x]$, where k is a field, and let $u \in k$. Then there is $q(x) \in k[x]$ with

$$f(x) = q(x)(x - u) + f(u).$$

Proposition 2.16 If $f(x) \in k[x]$, where k is a field, then a is a root of $f(x)$ in k if and only if $x - a$ divides $f(x)$ in $k[x]$.

Theorem 2.17 Let k be a field and let $f(x) \in k[x]$. If $f(x)$ has degree n, then $f(x)$ has at most n roots in k.

Remark. In Corollary 2.14, $q(x), r(x)$ are not stated as unique, therefore above is not true for polynomials in $R[x]$ for arbitrary commutative ring R.

Corollary 2.18 Every nth root of unity in $\mathbb{C}$ is equal to

$$e^{2\pi ik/n} = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}),$$

where $k = 0, 1, \ldots, n - 1$.

Corollary 2.19 Let k be any field, perhaps finite. If $f(x), g(x) \in k[x]$, if $\deg(f) \leqslant \deg(g) \leqslant n$, and if $f(a) = g(a)$ for $n + 1$ elements $a \in k$, then $f(x) = g(x)$.

PROOF. Let $h(x) = f(x) - g(x)$, $h(x)$ cannot have more than n roots in k. ■

Lemma 2.20 (3.30)The multiplicative group $E^* = E\backslash\{0\}$ of finite field E is cyclic.

PROOF. The proof is by showing that E^* has at most one cyclic group of order equal to each unique divisor of $|E^*|$. For a divisor of $|E^*|$, say d, suppose there are two subgroups S, T of order d. Then the elements of $S \bigcup T$ are all roots of $x^d - 1$ in the multiplicative group. But $|S \bigcup T| > d$, and $x^d - 1$ has too many roots in E^* (by theorem 3.25). Therefore, there is at most one subgroup of order as each divisor of $|E^*|$. Then by theorem 2.86 in the text, $|E^*|$ is cyclic. ■

Theorem 2.21 If k is a field, and $f(x), g(x) \in k[x]$, then their gcd, $d(x)$, is a linear combination of $f(x)$ and $g(x)$ in $k[x]$; that is there are $s(x), t(x) \in k[x]$ s.t.

$$d(x) = s(x)f(x) + t(x)g(x).$$

Monic $\gcd(f(x), g(x))$ is unique.

Lemma 2.22 Let k be a field, let $p(x), f(x) \in k[x]$, and let $d(x) = (p, f)$ be there gcd. If $p(x)$ is a monic irreducible, then $d(x) = 1$ if $p(x) \nmid f(x)$; $d(x) = p(x)$ if $p(x) \mid f(x)$.

Theorem 2.23 [Euclid's Lemma] Let k be a field and let $f(x), g(x) \in k[x]$. If $p(x)$ is irreducible in $k[x]$, and $p(x) \mid f(x)g(x)$, then $p(x) \mid f(x)$ or $p(x) \mid g(x)$. This works similarly if $p(x) \mid f_1(x)f_2(x)\dots f_m(x)$.

PROOF. Assume that $p(x) \nmid f(x)$, then $\gcd(p, f) = 1 \Rightarrow 1 = sp + tf \Rightarrow g = spg + tfg$. $p \mid fg$, then $p \mid g$. ■

Definition 2.24 Let k be a field. $f(x), g(x) \in k[x]$ are ***relative primes*** if $\gcd(f, g) = 1$.

09/26/08

Definition 2.25 $\varphi : R \to S$ is a ***homomorphism of rings*** if

(1) $\varphi(1_R) = 1_S$,

(2) $\varphi(a + b) = \varphi(a) + \varphi(b)$, and

(3) $\varphi(ab) = \varphi(a)\varphi(b)$.

We have that $\ker\varphi = \{r \in R : \varphi(r) = 0\}$ and $\text{im}\varphi = \{\varphi(r) : r \in R\}$.

Definition 2.26 $I \subset R$ is a left R-ideal if

(1) $0 \in I$,

(2) $\forall a, b \in I, a + b \in I$, and

(3) $\forall a \in I, r \in R, ra \in I$.

Example 2.27 $\ker\varphi \in R$ is a left R-ideal. That is, kernel of a ring homomorphism $R \to S$ is an R-ideal in S.

The only ideals of a field f is $\{0\}$ and f; but f may contain nonzero proper subrings. For example, $\mathbb{Z}$ in $\mathbb{Q}$.

Theorem 2.28 (Correspondence Theorem of Rings) The R/I-ideals, $\{J/I\}$, are in bijection with R-ideals $\{J : I \subseteq J \subseteq R\}$.

PROOF. [trivial, to be filled in, for now, see book (page 320, proposition 6.1) for details.] ■

Definition 2.29 An ideal $I \subseteq R$ is a ***prime ideal*** if $I \neq R$, and $ab \in I \Rightarrow a \in I$ or $b \in I$.

Example 2.30 Prime ideals.

(1) $5\mathbb{Z} \subseteq \mathbb{Z}$ is a prime ideal.

(2) $6\mathbb{Z} \subseteq \mathbb{Z}$ is not a prime ideal; $6 \in 6\mathbb{Z}, 6 = 2 \times 3$, but $2, 3 \notin 6\mathbb{Z}$.

Proposition 2.31 $I \subseteq R$ is a prime ideal $\Leftrightarrow$ R/I is a domain.

PROOF.

"$\Rightarrow$" For $ab \in R/I$, if $(a+I)(b+I) = ab + I = 0 + I$, then $ab \in I$. I is prime hence $a \in I$ or $b \in I$. We may assume that $a \in I$; we then have $a + I = I$.

"$\Leftarrow$" For $ab \in I$, since $0 + I = ab + I = (a+I)(b+I)$ and R/I is a domain, $a + I = I$ or $b + I = I$; therefore, $a \in I$ or $b \in I$.

■

Definition 2.32 An ideal $I \subseteq R$ is a maximal ideal if $I \neq R$ and if for all R-ideal J, $I \subseteq J \subseteq R \Rightarrow I = J$ or $J = R$.

Proposition 2.33 Every maximal ideal is a prime ideal.

PROOF. Suppose $I \subseteq R$ is a maximal ideal in R. Suppose I is not prime; then $\exists ab \in I$, $a \notin I, b \notin I$. Then (I, a) is a larger ideal in R; since J is maximal, $(I, a) = R$. Then 1_R is generated by elements $y \in I$ and a such that $1_R = y + ra$, $r \in R$. But then $b = yb + rab$. Both y and rab belong to I, so $b \in I$, contradiction. ■

Proposition 2.34 An R-ideal I is maximal $\Leftrightarrow$ R/I is a field.

PROOF.

"$\Rightarrow$" For $a \in R \backslash I$, I is maximal hence $(I, a) = R$, which gives $1_R = ra + y$ for some $r \in R, y \in I$. Then $ra + y + I = 1 + I$ in R/I. This gives $(r + I)(a + I) = 1 + I$, making $a + I$ a unit.

"$\Leftarrow$" R/I is a field, then the only ideals in R/I are R/I and $\{0\}$. By correspondence theorem for rings, I is a maximal ideal in R.

■

Example 2.35 $\mathbb{Q}[x, y]/(y) \cong \mathbb{Q}[x]$ is a domain but not a field (since for example, $x + 1$ has no inverse in it), (y) is a prime ideal but not a maximal ideal. Note: $(0) \subseteq (y) \subseteq (x, y) \subseteq \mathbb{Q}[x, y]$.

09/29/08

In $\mathbb{Z}$, if $p \mid ab$, then $p \mid a$ or $p \mid b$. This property generalizes.

Lemma 2.36 Let $P \subseteq R$ be a prime ideal, then $IJ \subseteq P \Rightarrow I \subseteq P$ or $J \subseteq P$.

PROOF. For $IJ \subseteq P$, if I, J are not in P, then exist $a \in P \backslash I, b \in P \backslash J$. Now $ab \in IJ \subseteq P$, P prime hence $a \in P$ or $b \in P$, contradiction. ■

Let $I, J \subset R$ be ideals, then $I \bigcap J$ is an R-ideal. $I + J = \{a + b : a \in I, b \in J\}$ is an R-ideal. $IJ = \{a_1 b_1 + a_2 b_2 + \ldots + a_r b_r : a_i \in I, b_i \in J, r \in \mathbb{N}\}$ is an R-ideal.

Definition 2.37 $a, b \in R$ are called ***associates*** if exists a unit $u \in R$, s.t. $a = ub$.

Lemma 2.38 R is a domain. $a, b \in R$ are associates if and only if $(a) = (b)$.

PROOF.

"$\Rightarrow$" a, b are associates, then $a = ub$ for some $u \in R$. Then $(a) \subseteq (b)$. Similarly $(b) \subseteq (a)$; hence $(a) = (b)$.

"$\Leftarrow$" $(a) = (b)$ then $a = ub, b = va$ for some $u, v \in R$. Hence $a = ub = uva$. R is a domain, we may cancel a and get $uv = 1$. Therefore, u, v are units in R.

■

Definition 2.39 An element $r \in R$ is ***irreducible*** if r is not a zero or a unit and if $r = ab$, then a is a unit or b is a unit. We then have $(r) = (a)$ or $(r) = (b)$.

Lemma 2.40 If (p) with $p \neq 0$ is a prime ideal, then p is irreducible.

PROOF. $(p) \subseteq R$ is prime ideal hence p is not a unit; otherwise $(p) = R$. Let $p = ab$. We get $(p) \subseteq (a), (p) \subseteq (b)$. Since $ab \in (p)$, we may assume that $a \in (p)$; then $a = rp$ for some $r \in R$. We then have $(a) \subseteq (p)$. Hence $(p) = (a)$ and p, a are associates. This gives that p is irreducible. ■

Definition 2.41 R ia ***principal ideal domain (PID)*** if R is a domain and every ideal in R is generated by a single element in R.

Example 2.42 $\mathbb{Z}$, $\mathbb{Q}$ are PIDs; $\mathbb{Q}[x, y]$ is not a PID. In fact, every field is a PID since the only ideals in a field is the zero ideal and the whole field.

Remark. For any PID R and $a, b \in R$, we can prove that they have a gcd δ and there are $r, s \in R$ s.t. $\delta = ra + sb$. Furthermore, for any irreducible element $p \in R$ and $xy \in R$, $p \mid xy \Rightarrow p \mid x$ or $p \mid y$. This works for any PID, hence for any field. We formally prove it in the following theorem.

Theorem 2.43 (3.57)

(1) Every $\alpha, \beta \in R$ has a gcd, δ, which is a linear combination of α and β in the form: $\delta = r\alpha + s\beta$ for some $r, s \in R$.

(2) Furthermore, if p is an irreducible element of R and $p \mid ab$ for some $ab \in R$, then $p \mid a$ or $p \mid b$.

PROOF.

(1) If one or both of α, β are zero, then the conclusion is trivially true; assume they are not zeros. Let $I = (\alpha, \beta)$, the ideal generated by α and β. R is a PID, then $I = (\delta)$ for some $\delta \in R$. We claim that $\delta = \gcd(\alpha, \beta)$. Obviously $\delta \mid \alpha, \beta$ and is a linear combination of the form $\delta = r\alpha + s\beta$ for some $r, s \in R$, since $\delta \in (\alpha, \beta)$. On the other hand, for any common divisor σ of α, β, $\sigma \mid \alpha \Rightarrow \sigma\alpha' = \alpha$ for some $\alpha' \in R$, similarly $\sigma\beta' = \beta$. Therefore $\delta = r\alpha + s\beta = \sigma(r\alpha' + s\beta')$ and $\sigma \mid \delta$.

(2) $p = ab$, p is irreducible, then either $(p) = (a)$ or $(p) = (b)$, therefore $p \mid a$ or $p \mid b$.

■

Proposition 2.44 In a PID R, (p) is a prime ideal if and only if p is irreducible.

PROOF.

"⇒" By Lemma 2.40.

"⇐" We show that if p is irreducible then (p) is maximal in R, hence prime. Suppose not, then exists ideal J such that $(p) = I \subsetneq J \subsetneq R$. R is a PID, therefore $J = (q)$ for some $q \in R$. We have $q = rq$ for some $r \in R$. p is irreducible, therefore either r or q must be a unit. If r is a unit, then $I = (p) = (q) = J$; if q is a unit, then $J = (q) = R$. Both contradict the assumption that $I \subsetneq J \subsetneq R$.

■

Definition 2.45 A domain R is a ***unique factorization domain (UFD)*** if

(1) Every $r \in R$ is either 0, or a unit, or a product of irreducible elements.

(2) Every nonzero element has a unique factorization into irreducible elements. That is, if $r = up_1p_2 \dots p_m = vq_1q_2 \dots q_n$ with u, v units and p_i, q_i irreducible, then $m = n$ and there exists a bijection $\sigma : \{p_1, p_2, \dots, p_n\} \to \{q_1, q_2, \dots, q_n\}$ such that p_i and $q_j = \sigma(p_i)$ are associates.

Proposition 2.46 (6.17) Let R be a ring in which ever nonzero $r \in R$ is a product of irreducible elements, then R is UFD if and only if (p) is a prime ideal for every irreducible element p.

PROOF.

"⇒" Suppose R is a UFD, $p \in R$ irreducible. If $ab \in (p)$, then $ab = rp$ for some $r \in R$. p is irreducible, therefore it must be an associate of an irreducible factor of either a or b. Therefore, $a \in (p)$ or $b \in (p)$. (p) is prime.

"⇐" Let $x \in R$ have two factorizations $up_1p_2 \dots p_m = vq_1q_2 \dots q_n$. We prove via induction on $\max(m, n)$. p_1 is an irreducible element in R hence (p_1) is prime by assumption. $vq_1q_2 \dots q_n = x \in (p_1)$, therefore some $q_i \in (p_1)$. Assume $q_i = rp_1$; q_i is also irreducible, therefore p_1, q_i are associates. By induction hypothesis, we have that the two factorizations are equivalent and unique.

■

10/01/08

Proposition 2.47 (6.18)

(1) If R is a commutative ring and $I_1 \subseteq I_2 \dots \subseteq I_n \subseteq \dots$ is an ascending chain of ideals, then $J = \bigcup_{n \geqslant 1} I_i$ is an ideal.

(2) If R is a PID, then there is no infinite strictly ascending chain of ideals $I_1 \subsetneq I_2 \dots \subsetneq I_n \subsetneq \dots$.

(3) Let R be a PID, then every nonzero $r \in R$ is a product of irreducible.

PROOF.

(1) Straightforward verification.

1. $0 \in J$,
2. $\forall a, b \in J$, $a \in I_m, b \in I_n$ for some m, n, therefore $a + b \in I_{\max\{m,n\}} \subseteq J$, and
3. $\forall a \in J, r \in R$, $a \in I_n$ for some n, therefore $ra \in I_n \subseteq J$.

(2) Given any chain $\langle I_j \rangle$, R is a PID, $J = (x)$ for $x \in I_n$ for some n. Then $J = I_n$ and the chain stops there; it cannot be infinite.

(3) Suppose $r \in R$ is not irreducible, then there exists $r_1 s_1$ such that neither r_1 or s_1 is a unit. At least one of r_1 and s_1 is not irreducible; suppose r_1 is not irreducible. Then $r \in (r_1)$ and $(r) \subsetneq (r_1)$ (if $(r) = (r_1)$, then s_1 must be a unit; but s_1 is not a unit). Repeating this we get an infinite chain $(r_1) \subsetneq (r_2) \subsetneq (r_3) \ldots$, which contradicts (2). Therefore, r is a product irreducible elements.

■

Theorem 2.48 (6.19) R is PID $\Rightarrow$ R is UFD.

PROOF. The proof follows directly from above previous two results. ■

Definition 2.49 A domain R is a ***Euclidean domain*** if there exists a ***degree function*** $d : R\backslash\{0\} \to \mathbb{N}$ with the following properties:

(1) $d(a) \leqslant d(ab)$ for all $a, b \in R\backslash\{0\}$, and

(2) For all $a, b \in R, b \neq 0$, $\exists q, r \in R$ s.t. $a = qb + r$ and either $r = 0$ or $d(r) < d(b)$.

Example 2.50 $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}[x]$ are Euclidean domains; $\mathbb{Q}[x, y], \mathbb{Z}[\sqrt{-19}]$ are not.

Theorem 2.51 Every Euclidean domain is a PID.

PROOF. Let I be an R-ideal, choose $b \in I$ s.t. $d(b)$ is minimal; we claim that $I = (b)$. To see this, let $a \in I$, R Euclidean then $a = qb + r$ with $r = 0$ or $d(r) < d(b)$. Suppose $r \neq 0$, since $a, b \in I$, we have $r \in I$ and by the assumption that $d(b)$ is minimal, $d(r) \geqslant d(b)$. Therefore, r must be 0 and $a \in (b)$. ■

Definition 2.52 Let R be a UFD. A polynomial $f(x) \in R[x]$ is ***primitive*** if its coefficients are relatively prime, that is, if $f(x) = a_n x^n + \ldots + a_1 x + a_0$, then the only common divisors of $a_0, a_1, \ldots, a_n$ are units.

Remark. In a UFD, a common divisor is well defined, and we can talk about a greatest common divisor of a and b. d is a *gcd* for a and b if $d' \mid a$ and $d' \mid b$ implies $d' \mid d$. In a UFD, if $a = up_1^{e_1} \ldots p_r^{e_r}$ and $b = vp_1^{f_1} \ldots p_r^{f_r}$. Then $d = \prod_{i=1}^{r} p_i^{\max\{e_i, f_i\}}$ is a *gcd* for a and b.

Proposition 2.53 For a UFD R, if $p(x) \in R[x]\backslash R$ is irreducible, then $p(x)$ is primitive.

PROOF. Suppose $p(x)$ is not primitive, then $\exists q \in R$ s.t. $p(x) = qg(x), \deg(g) > 0$, where q is not a unit. Since $p(x)$ is irreducible, $p(x)$ and q are associates; this makes $g(x)$ a unit. Contradiction. ■

Lemma 2.54 (Gauss's Lemma, 6.23 in the text) Let R be a UFD, if $f(x), g(x) \in R[x]$ are primitive, then $f(x)g(x)$ is primitive.

PROOF. If (p) is a prime ideal in R, then the ring homomorphism $\pi : R \to R/(p), a \mapsto a + (p)$ induces a ring homomorphism $\widetilde{\pi} : R[x] \to R/(p)[x]$ s.t. the coefficients of a_i of $f(x) \in R$ are mapped to $\pi(a_i)$. If $h(x) = h_0 + h_1x + \ldots + h_rx^r$ is ***not*** primitive, then exists irreducible $p \in R$ s.t. $p \mid h_i$ for all i. Therefore, $\pi(h_i) = h_i + (p) = 0 + (p)$. $\widetilde{\pi}(h(x)) = 0 \in R/(p)[x]$ since all the coefficients are 0.
Suppose now that $f(x)g(x)$ is not prmitive, then $\widetilde{\pi}(f)\widetilde{\pi}(g) = \widetilde{\pi}(fg) = 0 \in R/(p)[x]$. $R/(p)[x]$ is a domain (this can be proved by showing that R is a domain then $R[x]$ is a domain), therefore $\widetilde{\pi}(f) = 0$ or $\widetilde{\pi}(g) = 0$. That is, either $f(x)$ or $g(x)$ are not primitive. Contradiction. ■

10/03/2008

Definition 2.55 For $f(x) \in R[x]$, let $c(f)$ be a *gcd* of the coefficients, and let $f(x) = c(f)f^*(x)$ so that $f^*(x) \in k[x]$ is primitive. $c(f)$ is called the content of f.

Lemma 2.56 (6.24)

(1) For $f(x) \in R[x]$, let $f(x) = c(f)f^*(x)$. The factorization is unique, if $f(x) = rg^*(x)$ with $r \in R$, g^* primitive, then $c(f)$ and r are associates and f^* and g^* are associates.

(2) For $f(x), g(x) \in R[x], c(fg)$ and $c(f)c(g)$ are associates and $(fg)^*$ and f^*g^* are associates.

(3) Let $f(x) \in R[x], g^*(x) \in R[x]$, g^* primitive. If $g^* \mid bf(x), b \in R, b \neq 0$, then $g^* \mid f$.

PROOF.

(1) $rg^* = cf^*$, with $\frac{r}{c} = \frac{u}{v}$ such that u, v are relative primes. Then $ug^* = vf^*$. $u \mid vf^* \Rightarrow u \mid f^* \Rightarrow u$ is a unit. Similarly, v is a unit. Therefore, c, r are associates and g^*, f^* are associates.

(2) $fg = c(fg)(fg)^* = c(f)c(g)f^*g^*$, since f^*, g^* are primitive, so does f^*g^* by Gauss's Lemma. Therefore, by (1) we have that $c(fg)$ and $c(f)c(g)$ are associates and $(fg)^*$ and f^*g^* are associates.

(3) We may write $bc(f)f^*(x) = bf(x) = h(x)g*(x) = c(h)h^*(x)g^*(x)$. $h^*(x)g^*(x)$ and $f^*(x)$ are associates, therefore exists unit $r, rh^*(x)g^*(x) = f^*(x) \Rightarrow g^*(x) \mid f^*(x) \Rightarrow g^*(x) \mid f(x)$.

■

Theorem 2.57 If R is a UFD, then $R[x]$ is a UFD.

PROOF.

(1) Every nonzero element $f(x) \in R[x]$ that is not a unit is a product of irreducible elements. We prove this by induction on $\deg(f)$.

- $\deg(f) = 0$. Then $f \in R$, R is UFD.
- $\deg(f) > 0$. $f(x) = c(f)f^*(x)$. $c(f) \in R$, if $f^*(x)$ is an irreducible element then we are done. Suppose not, then $f^*(x) = gh$ such that g, h are not units. $g, h \notin R$, otherwise $f^*(x)$ being primitive implies that g or h is a unit. Therefore, $\deg(g), \deg(h) < \deg(f^*)$. We may then apply induction hypothesis on g^*, h^* to conclude that every $f(x)$ is a product of irreducibles.

(2) Every irreducible $p(x) \in R[x]$ generates a prime ideal. In other words, we want to show that for every $p(x) \in R[x]$, $p \mid fg \Rightarrow p \mid f$ or $p \mid g$. We prove this for two cases based on $\deg(p)$.

- $\deg(p) = 0$. $f(x) = c(f)f^*(x), g(x) = c(g)g^*(x)$. $p \mid fg \Rightarrow p \mid c(fg) \Rightarrow p \mid c(f)c(g)$. $p, c(f), c(g) \in R$ and R is a UFD, (p) is prime, $c(f)c(g) \in (p)$, then $c(f) \in (p)$ or $c(g) \in (p)$. Therefore, $p \mid c(f)$ or $p \mid c(g)$.
- $\deg(p) > 0$. Let $I = (p, f) = R[x]p(x) + R[x]f(x) \subseteq R[x]$, let $m(x) \in I$ be of minimal degree, apply quotient/remainder over $Q[x]$, in which $Q = \mathrm{Frac}(R)$, to f and m,

$$f(x) = m(x)q'(x) + r'(x),$$

$q'(x), r'(x) \in\in Q[x]$. Clearing denominators gives $bf(x) = m(x)q(x) + r(x) \in R[x]$, $b \in R$, s.t. $r(x) = 0$ or $\deg r(x) < \deg m(x)$. $bf(x) \in I$, $m(x) \in I \Rightarrow r(x) \in I$. Therefore $r(x) = 0$ since $m(x)$ is of minimal degree in I. We have that $bf(x) = m(x)q(x) = c(m)m^*(x)q(x)$. It follows that $m^* \mid f(x)$ by Lemma 2.56(3). Similarly $m^*(x) \mid p(x)$. $p(x)$ is irreducible, $m^*(x)$ is a unit or an associate of $p(x)$. Two cases:

i (m^* is a unit). $m \in (p, f) \Rightarrow m = s(x)p(x) + r(x)f(x)$. $mg(x) = s(x)p(x)g(x) + r(x)f(x)g(x)$, $p(x) \mid f(x)g(x)$ hence $p(x) \mid mg(x) \Rightarrow p(x) \mid c(m)m^*g(x)$. $p(x)$ is primitive (since it is irreducible, $p(x) = c(p)p*$ implies that $c(p)$ is a unit), $p(x) \mid g(x)$ by Lemma 2.56(3).

ii (m^* is an associate of $p(x)$). $m^*(x) \mid f(x) \Rightarrow p(x) \mid f(x)$.

■

Corollary 2.58 For k a field, $k[x_1, x_2, \ldots, x_n]$ is a UFD.

PROOF. By induction on n. k is a field; the only ideas are $\{0\}$ and k, which are both generated by a single element. k is then a PID then UFD. We have $k[x]$ is also a UFD as the base case, and we may use $k[x_1, x_2, \ldots, x_{n-1}]$ as induction hypothesis to get that $k[x_1, x_2, \ldots, x_n]$ is a UFD. ■

Corollary 2.59 (Gauss) Let R be a UFD, let $Q = \mathrm{Frac}(R)$ be the field of fraction of R. For $f(x) \in R[x]$, if $f(x) = G(x)H(x)$ is a factorization of $f(x)$ in $Q[x]$, then $f(x)$ has a factorization $f(x) = g(x)h(x) \in R[x]$ such that $\deg g = \deg G, \deg h = \deg H$.

PROOF. By Lemma 2.56(1), we may factor $G(x) = qG^*(x), H(x) = q'H^*(x)$ s.t. $G^*, H^* \in R[x]$ are primitive. Then G^*H^* is also primitive in $R[x]$. $f(x) = c(f)f^*(x) \in R[x]$, this forces $qq' \in R$. Therefore, $(qq')G^* \in R[x]$; a factorization of $f(x) \in R[x]$ is given by $f(x) = [qq'G^*(x)]H^*(x)$. Rest follows. ■

10/06/08

Definition 2.60 A commutative ring R satisfies the ***ascending chain condition (ACC)*** if every ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \ldots \subseteq I_n \subseteq \ldots$ stabilizes.

Definition 2.61 An R-ideal I is ***finitely generated*** or ***f.g.*** if there exist $a_1, a_2, \ldots, a_n \in R$ such that $I = (a_1, a_2, \ldots, a_n)$.

Proposition 2.62 Let R be a ring, the following are equal:

(1) R satisfies ACC,

(2) R satisfies the maximum condition: every nonempty family $\mathcal{F}$ of R-ideals has a maximal element, and

(3) Every R-ideal is f.g..

PROOF.

(1) $((1) \Rightarrow (2))$. R satisfies ACC, let $\mathcal{F}$ be a family of ideals in R. For $I_1 \in \mathcal{F}$, since I_1 is not maximal, $\exists I_2 \in \mathcal{F}$, $I_1 \subsetneq I_2$. Similarly, $\exists I_3 \in \mathcal{F}$ s.t. $I_2 \subsetneq I_3$. Repeating this we get an infinite ascending chain $I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_n \ldots$, contradiction.

(2) $((2) \Rightarrow (3))$. Let $I \subseteq R$, Let $F = \{f.g.\text{R}-ideals \subseteq I\}$. $\mathcal{F}$ has a maximal element M, $M \subseteq I$, and M is f.g.; if $M \neq I$, then exist $a \in I$, $a \notin M$, then (M, a) is a larger ideal than M, contradiction. Therefore, $M = I$ and I is f.g..

(3) Every R-ideal is f.g., for any ascending chain $\langle I_i \rangle$, let $J = \bigcup I_i$, J is an ideal in R and J is f.g. Then there are only finitely different I_i's in the chain and the chain must stabilize.

■

Definition 2.63 A commutative ring R with any of the above properties is called ***noetherian***.

Corollary 2.64 Let R be a noetherian ring. Then every ideal I is contained in some maximal R-ideal of M.

PROOF. Let $\mathcal{F}$ be the family of proper ideals containing I, then $\mathcal{F}$ has a maximal element M that contains I. If M is not maximal ideal in R then exists J, $M \subsetneq J \subsetneq R$. $J \in F$, contradiction. ■

Corollary 2.65 If R is noetherian and J is an R-ideal, then R/J is noetherian.

PROOF. Let I/J be an R/J-ideal with $J \subseteq I \subseteq R$, the generators for I certainly generates I/J. ■

Theorem 2.66 (6.42 in the text, Hilbert Basis Theorem) R is commutative noetherian ring, then $R[x]$ is also a commutative noetherian ring.

PROOF. Let $I \subseteq R[x]$ be an ideal, assume that I is not f.g., we will obtain a contradiction.
Choose $f_0 \in I \subseteq R[x]$ of minimal degree, then $(f_0) \subsetneq I$ (I is not f.g.). Choose $f_1 \in I - (f_0)$ of smallest degree and repeat this procedure, we obtain a sequence of ideals $(f_0) \subsetneq (f_0, f_1) \subsetneq (f_0, f_1, f_2) \subsetneq \ldots$ such that $\deg f_0 \leqslant deg f_1 \leqslant \ldots$. For $(f_0, f_1, \ldots, f_m) \subsetneq I$, consider the ideal $(a_0, \ldots, a_m) \subseteq R$, in which a_i is the leading coefficient of f_i.

R is noetherian, then the chain formed by $(a_0, \ldots, a_m)$ stablizes. Say $a_{m+1} \in (a_0, \ldots, a_m)$, let $a_{m+1} = r_0 a_0 + \ldots + r_m a_m$, consider

$$f^* = f_{m+1} - \sum_{i=0}^{m} (r_i f_i(x)) x^{\deg f_{m+1} - \deg f_i},$$

then $f^* \in I \backslash (f_0, \ldots, f_m)$ since the rest of the terms are linear combinations of elements in $(f_0, \ldots, f_m)$. If we write $f_k = a_k x^{d_k} +$ lower terms, then

$$\begin{aligned} f^* &= (a_{m+1} x^{d_{m+1}} + \text{lower terms}) - \textstyle\sum_{i=0}^{m} r_i ((a_i x^{d_i} + \text{lower terms})) x^{\deg d_{m+1} - \deg d_i} \\ &= a_{m+1} x^{d_{m+1}} - \textstyle\sum_{i=0}^{m} r_i a_i x^{d_{m+1}} + \text{lower terms} \\ &= \text{lower terms}. \end{aligned}$$

this gives us that $\deg f^* < \deg f_{m+1}$, therefore $f^* \in (f_0, \ldots, f_m)$, yielding a contradiction. ■

With Zorn's Lemma, 6.46, 6.48, 6.53 can be proved.

Definition 2.67 X is a ***partially ordered*** set if there is a relation $x \leqslant y$ onr X that is

- Reflexive,
- Antisymmetric ($x \leqslant y, y \leqslant x \Rightarrow x = y$), and
- Transitive.

Definition 2.68 A partially ordered set X is a ***chain*** if for all $x, y \in X$, either $x \leqslant y$ or $y \leqslant x$.

Axiom 2.69 (Zorn's Lemma) If X is a non-empty partially ordered set in which every chain has an upper bound then X has a maximal element.

Remark. The standard way of applying Zorn's Lemma to a set $\mathcal{A}$ is to construct a family $\mathcal{F}$ with desired property, then show that any chain $\mathcal{C}$ in $\mathcal{F}$ has an upper bound M (for example, if the partial order is inclusion, the union of all sets in $\mathcal{C}$ is the upper bound) and that M is in $\mathcal{F}$ hence in $\mathcal{C}$. Zorn's Lemma then says that $\mathcal{F}$ contains a maximal such with the desired property.

Definition 2.70 A poset if ***well-ordered*** if every nonempty subset S of X contains a smallest element.

Theorem 2.71 The following are equivalent:

(1) Zorn's Lemma.

(2) The well ordering principle: Every set X has some well-ordering of its elements.

(3) The axiom of choice.

(4) Hausdorff maximal principle.

10/08/08

Proposition 2.72 (6.46) In a commutative ring R with $1 \neq 0$, every ideal is contained in a maximal ideal.

PROOF. Let $\mathcal{F} = \{I : I' \supseteq I\}$ be the set of proper R-ideals that contain I. The set $\mathcal{F}$ is partially ordered w.r.t. inclusion. $\mathcal{F}$ has a maximal element if every chain in $\mathcal{F}$ has an upper bound (Zorn's Lemma). Let C be a chain of ideals in $\mathcal{F}$, define $I^* = \bigcup_{I \in C} I$, then clearly $I^* \supsetneq I$ and I^* is an upper bound for C. Moreover, $I^* \in F \Leftrightarrow I^*$ is a proper R-ideal. Indeed, I is proper, for if $1 \in I^*$ then $1 \in I$ for some I; but the ideals in C are proper. Contradiction. Let $M \in F$ be maximal, then M is a maximal R-ideal. Suppose $I \subseteq M \subsetneq J \subseteq R$, then $J \in F$, contradiction. ■

Definition 2.73 Let V be a vector space V over some field k, and let $Y \subseteq V$ be a (possibly infinite) subset.

(1) Y is ***linearly independent*** if every finite subset of Y is linearly independent.

(2) Y ***spans*** V is each $v \in V$ is a linear combination of finitely many elements of Y. We write $V = \langle Y \rangle$ when V is spanned by Y.

(3) A ***basis*** of a vector space V is a linearly independent subset that spans V.

Example 2.74 $V = k[x]$ as a vector space over k has a basis $Y = \{1, x, x^2, \ldots\}$.

Proposition 2.75 (6.48) Let V be a vector space over k, then V has a basis and every linearly independent subset $B \subseteq V$ is contained in a basis for V.

PROOF. Let $X = \{B' : B \subseteq B'\}$, the family of all the linearly independent subsets of V that contain B. The family X is nonempty, since $B \in X$. We want to show that every chain $C \subseteq X$ has an upper bound. Let $C = \{B_j : j \in J\}$ be a chain of X and let $B^* = \bigcup_{j \in J} B_j$. Then $B_j \subseteq B^*$ for all $j \in J$ and B^* is an upper bound for C if B^* is linearly independent.
Assume B^* is not linearly independent, say $B^* \supseteq \{y_1, y_2, \ldots, y_m\}$ with $y1, y_2, \ldots, y_m$ linearly dependent. Then there are B_{j_i}'s such that $y_i \in B_{j_i}, i = 1, 2, \ldots, m$. We have $\bigcup_{i=1}^m B_{j_i} \supseteq \{y_1, y_2, \ldots, y_m\}$. There must be some $j' \in \{j_1, j_2, \ldots, j_m\}$ s.t. $B_{j'} \supseteq \{y_1, y_2, \ldots, y_m\}$ (since we are working in a chain with the relationship being inclusion). Contradicting that $B_{j'}$'s are all linearly independent.
We have shown that every chain $C \subseteq X$ has an upper bound, by Zorn's Lemma, X has a maximal element M. By definition of X, M is linearly independent. M also spans V; for if not, then there exists $a \in V \backslash \langle M \rangle$ and $B \subseteq M \subsetneq \langle M, a \rangle$. That is M plus a is a larger linearly independent subset of V that contains B, contradicting the maximality of M. ■

Lemma 2.76 (6.52) Let R be a commutative ring and let $\mathcal{F}$ be the family of all those ideals in R that is not finitely generated. If $\mathcal{F} \neq \varnothing$, then $\mathcal{F}$ has a maximal element.

PROOF. We show that every chain C in $\mathcal{F}$ has an upper bound in $\mathcal{F}$. Let $I^* = \bigcup_{I \in C} I$, then I^* is an upper bound for C if I^* is not f.g.. Suppose $I^* = (a_1, a_2, \ldots, a_m), a_i \in I_i$ is f.g., as before, there exits $I_0 \in C$ s.t. $(a_1, a_2, \ldots, a_m) \subseteq I_0$. But then $I^* \subseteq I_0 \subseteq I^*$ and I_0 is f.g., contradiction. I^* is an upper bound. The rest follows Zorn's Lemma. ■

Theorem 2.77 (I. S. Cohen, 6.53 in the text) A commutative ring R is noetherian if and only if every prime ideal in R is finitely generated.

PROOF. We need to show the "if" part only. Let $\mathcal{F}$ be the family of ideals that is not f.g., we obtain a contradiction from $\mathcal{F} \neq \varnothing$. By previous lemma, there exists maximal $M \in \mathcal{F}$ that is not f.g., we show that M is a prime ideal. Suppose not, then there exist $a, b \notin M, ab \in M$. Then $M + Ra \supsetneq M, M + Rb \supsetneq M$ and $M+Ra, M+Rb$ are f.g., by the maximality of M. But $(M+Ra)(M+Rb) = M$ is then f.g., contradiction. ■

3 Fields

10/13/08

Definition 3.1 A ***field*** is a commutative ring in which $1 \neq 0$ and every nonzero element is a unit. A ***subfield*** of a field K is a subring k of K that is also a field.

Definition 3.2 For a given field K with a subfield k, we call K an ***extension field*** of field k and K/k a ***field extension*** or an extension of fields.
An extension field K of a field k is a ***finite extension*** of k if K is a finite-dimensional ***vector space*** over k. The dimension of k, denoted by $[K : k]$, is called the ***degree*** of K/k.

Remark. This is saying that for any field extension K/k, we may treat elements of K as vectors and elements of k as scalars.

Example 3.3 Dimension of field extensions.

(1) $\mathbb{R}/\mathbb{Q}$. $\mathbb{R}$ is of infinite dimension over $\mathbb{Q}$.

(2) $\mathbb{Q}(i)/\mathbb{Q} : \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}, i^2 = -1\}$. $\mathbb{Q}(i)$ is of finite dimension over $\mathbb{Q}$.

Theorem 3.4 If R is a commutative ring, and I is an R-ideal, then R/I can be made a ring with multiplicative operation $(a + I)(b + I) = (ab + I)$.

PROOF. SKETCH: The underlying abelian groups of R and I give R/I as a quotient group under addition; we only need to verify that R/I is a monoid under the given multiplication, which is straightforward. ■

R/I is called the ***quotient ring*** of R ***modulo*** I.

Theorem 3.5 For any homomorphism $f : R \to A$ of rings, $R/\ker f \cong \mathrm{im} f$.

PROOF. To prove we need to show that we have a homomorphism and it is bijective. If we forget about the multiplication, $R/\ker f \cong \mathrm{im} f$ is an isomorphism of groups. It then suffices to verify that the map is compatible with multiplication. ■

Remark. In any homomorphism between a ring and a field $R \to K$, the image is a subring of K and therefore must be a domain (straightforward to verify). If we have a homomorphism between two fields $F \to K$, it is more special since the kernel is an ideal in F but there are only two ideals, $\{0\}, F$ in F.

Definition 3.6 For a field k, let k_0 be the intersection of all the subfields of k, then k_0 is itself a subfield, called the ***prime field*** of k.

Example 3.7 $k = \mathbb{R}, k_0 = \mathbb{Q}$. Any subfield of R must contain 1; then it must contain $\mathbb{Z}$ with addition; then it must contain all $\mathbb{Q}$ since very nonzero element is a unit in a field.

Proposition 3.8 For a field k, the prime field k_0 is either $k_0 = \mathbb{Q}$ or $k_0 = \mathbb{F}_p (\cong \mathbb{Z}/p\mathbb{Z})$ where p is a prime number.

PROOF. Consider the ring homomorphism

$$f : \mathbb{Z} \to k,$$

which is the mapping

$$f : n \mapsto n1_k.$$

then ker $f \subseteq \mathbb{Z}$ and ker $f = (m)$ for some $m \in \mathbb{Z}$. The later is true because $\mathbb{Z}$ is PID. We have two cases:

- **case** $m = 0$: f is injective, therefore, k contains all the integers. For k to be a field, it then contains the fraction ring of $\mathbb{Z}$, which gives us $\mathbb{Q}$. We then have $k_0 = \mathbb{Q}$.
- **case** $m \neq 0$: We have that $f' : \mathbb{Z}/m\mathbb{Z} \to k$ is an injective mapping. Since k is a field, imf' is a domain (cancellation law certainly holds for any subring of a field; therefore any subring of a field must be a domain). $m\mathbb{Z}$ is then a prime ideal in $\mathbb{Z}$. Let prime $p = m$, we then have $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is isomorphic a subfield $P = \{0, 1_k, 21_k, \ldots, (p-1)1_k\}$ (21_k is 2 multiplies 1_k) of k. Now any subfield of k must contain 1_k and therefore all of P. P is then the prime field of k.

■

If $k_0 = \mathbb{Q}$, we say k is a field of ***characteristic 0***; if $k_0 = \mathbb{F}_p$, k is a field of ***characteristic*** p. The later case is sometimes also called ***positive characteristics***, ***finite characteristic***, or ***nonzero characteristic***.

Proposition 3.9 If k is finite field, then $|k| = p^n$ for a prime p and $n > 0$.

PROOF. Assume $p \mid |k|$ and $q \mid |k|$ for distinct primes p, q, then by Cauchy's for abelian group, there are elements a, b in k with order p and q, respectively (a, b is of some prime order so they are not the 0 element). a is of order p so $0_k = ap = ap1_k$. Simiarly, $bq1_k = 0_k$. Since k is a field, then k is an integral domain, therefore, $a(p1_k) = 0$ and $a \neq 0 \Rightarrow p1_k = 0$; $p1_k = q1_k = 0$. But $(p, q) = 1 \Rightarrow \exists r, s, s.t.\ sp + tq = 1$. But $1_k = sp1_k + tq1_k = 0_k$, contradiction. ■

Proposition 3.10 Let k be a field and let $I = (p(x)) \subseteq k[x]$. Then $k[x]/I$ is a field if and only if $p(x)$ is irreducible in $k[x]$.

PROOF.

"⇒" Suppose $k[x]/I$ is a field. If $p(x)$ is not irreducible, then $p(x) = g(x)h(x)$ with $\deg(g) < \deg(p)$ and $\deg(h) < \deg(p)$. We must have that $g(x) + I \neq I$, otherwise $g(x) \in I \Rightarrow p(x) | g(x) \Rightarrow \deg(p) \leqslant \deg(g)$. Same holds for $h(x)$. Now $(g(x) + I)(h(x) + I) = (g(x)h(x) + I) = (p(x) + I) = 0 + I$. But $k[x]/I$ is a field then an integral domain, in which the product of nonzero elements is nonzero. Contradiction.

"⇐" Suppose $p(x)$ is irreducible, we show that $k[x]/I$ is a field by verifying that the definition is satisfied.

(1) $1 \neq 0$. $I = (p(x))$ is a proper ideal and $1 \notin I$ for if not, then $p(x)$ must be a unit and then not irreducible. Therefore, $1 + I \neq 0 + I$.

(2) Every nonzero element is a unit. For the above choice of $f(x)$, $p(x) \nmid f(x)$, otherwise $f(x) \in (p(x))$ and $f(x) + I = I$. Since $p(x)$ is irreducible, $f(x) \nmid p(x)$ by definition. Therefore p, f are relatively prime and there are polynomials s, t with $sf + tp = 1$. Now $1 + I = s(x)f(x) + t(x)p(x) + I = s(x)f(x) + I = (s(x) + I)(f(x) + I)$, and we have found the inverse of $f(x) + I$.

■

PROOF. [Second proof] We may use Proposition 2.34. That is, R/I is a field if and only if I is maximal.

"⇒" We have that R/I is a field then $(p(x))$ is maximal and then prime. We want to show that $p(x)$ is irreducible. For any $g(x), h(x)$ s.t. $p(x) = g(x)h(x)$, obviously $(p(x)) \subseteq (g(x)), (p(x)) \subseteq (h(x))$. $(p(x))$ is prime, then $g(x)h(x) \subseteq (p(x))$ hence $g(x) \in (p(x))$ or $h(x) \in (p(x))$. We then have $(g(x)) \subseteq (p(x))$ or $(h(x)) \subseteq (p(x))$. Therefore one of g, h is a unit, and $p(x)$ is irreducible.

"⇐" We want to show that $(p(x))$ irreducible then $(p(x))$ is maximal. For any $f(x) \notin (p(x))$, $f(x) = q(x)p(x) + r(x)$, where $\deg(r(x)) < \deg(p(x))$. Therefore $(p(x), r(x)) = 1$ and $(p(x), f(x)) = R$. Since $f(x)$ is arbitrary, $(p(x))$ is maximal.

■

Example 3.11 $k = \mathbb{Q}, k[x] = \mathbb{Q}(x)$, choose $p(x) = x^2 + 1$, $p(x)$ is irreducible. Let $I = (p(x))$, then $\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}(i)$ by $f(x) + I \mapsto f(i)$.

10/15/08

Proposition 3.12 (3.117) Let k be a field and let $p(x) \in k[x]$ be irreducible polynomial of degree d; $I = (p(x))$. Let $K = k[x]/I$, and write $\beta = x + I$.

(a) K is a field with a subfield $k' = \{a + I : a \in k\}$ s.t. $k' \cong k$.

(b) β is a root of $p(x)$.

(c) If β is a root of $g(x) \in k[x]$ then $p(x)|g(x)$.

(d) $p(x)$ is the unique monic irreducible polynomial in $k[x]$ s.t. β is a root of $p(x)$.

(e) K is a vector space over k of dim $= [K : k] = d$ with basis $1, \beta, \beta^2, \ldots, \beta^{d-1}$.

PROOF.

(a) K is a field by previous proposition. Define the map $\phi : k \to K$ s.t. for $a \in k$, $a \mapsto a + I$. The map is injective by Cor 3.53 in the textbook(we first verify that ϕ defines a homomorphism of rings, then we have that $\ker \phi$ is an ideal in k. But k is a field, the only ideals in k is zero ideal or k itself. Since $1 \mapsto 1 + I \neq 0 + I$, not everything maps to $0 + I$, therefore the kernel is not k; hence it is $\{0\}$ and we have an injection.); the kernel is then trivial. Therefore, by first isomorphism theorem of rings, $k \cong k/\{0\} \cong k'$. ϕ is an isomorphism from $k \to k'$.

(b) We may write $p(x) = \sum_{i=0}^{d} a_i x^i$. We evaluate $p(\beta)$ as

$$\begin{aligned} p(\beta) &= p(x + I) = a_0 + a_1(x + I) + \ldots + a_d(x + I)^d \\ &= a_0 + a_1(x + I) + a_2(x^2 + I) + \ldots + a_d(x^d + I) \\ &= a_0 + a_1 x + \ldots + a_d x^d + I \\ &= p(x) + I = I. \end{aligned}$$

Therefore, β is a root of $p(x)$.

(c) If $p(x) \nmid g(x)$, $p(x)$ irreducible $\Rightarrow \gcd(p(x), g(x)) = 1$ and exist $s(x), t(x)$ s.t. $1 = sp + gt$. Since β is the root of both $g(x)$ and $p(x)$, $s(\beta)p(\beta) + t(\beta)g(\beta) = 0$. Contradiction. Therefore, $p(x) \mid g(x)$.
Alternatively (more clearly), follow proof in (b), $0+I = g(\beta) = g(x)+I$. $g(x) \in (p(x))$, hence $p(x) \mid g(x)$.

(d) By (c), if there is another monic irreducible $g(x)$ with β as a root, then $p(x) \mid g(x)$ and $g(x) \mid p(x)$. Thus $g(x) = cp(x)$ for some constant c. Since both $p(x)$ and $g(x)$ are monic, the leading coefficient are both 1, which implies $c = 1$. Thus $p(x) = g(x)$ and $p(x)$ is unique.

(e) We first show that every $f(x)$ in $k[x]$ is a linear combination of β^i's. Every elements of $K = k[x]/I$ has the form $f(x) + I$. We may write $f(x) = q(x)p(x) + r(x)$ with $\deg(r(x)) < \deg p(x) = d$. Then

$$\begin{aligned} f(x) + I &= r(x) + I \\ &= r_0 + r_1 x + r_2 x^2 + \ldots + r_{d-1} x^{d-1} + I \\ &= r_0 + r_1(x + I) + r_2(x^2 + I) + \ldots + r_{d-1}(x^{d-1} + I) \\ &= r_0 + r_1(x + I) + r_2(x + I)^2 + \ldots + r_{d-1}(x + I)^{d-1} \\ &= r_0 + r_1\beta + r_2\beta^2 + \ldots + r_{d-1}\beta^{d-1}. \end{aligned}$$

We have shown that every $f(x)$ can be represented as a linear combination of β^i with $i < d$. We now show that the basis is linearly independent. Suppose this is not true; then there exist $c_0, c_1, \ldots, c_{d-1}$ that are not all zeros such that $\sum_{i=0}^{d-1} c_i\beta^i = 0$. Let $g(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{d-1}x^{d-1}$, then $0 + I = \sum_{i=0}^{d-1} c_i\beta^i + I = g(x) + I$, therefore $g(x) \in I$ and $p(x) \mid g(x)$. But $\deg(g(x)) < d = \deg(p(x))$; therefore $g(x) = 0$ and every c_i must be 0. Contradiction.

■

Definition 3.13 Let K/k be an extension of fields. $\alpha \in K$ is ***algebraic*** over k if there is some nonzero polynomial $f(x) \in k[x]$ having α as a root; otherwise, α is ***transcendental*** over k, An extension K/k is ***algebraic*** if every $\alpha \in K$ is algebraic over k.

Example 3.14 Algebraic and transcendental elements and algebraic field.

(1) $\sqrt{3} \in \mathbb{R}/\mathbb{Q}$ is algebraic over $\mathbb{Q}$; since it is a root of $f(x) = x^2 - 3$.

(2) $\pi \in \mathbb{R}/\mathbb{Q}$ is transcendental over $\mathbb{Q}$ (proof is not trivial).

(3) $K = \mathrm{Frac}(k[x])$, then K/k if a field extension. $x \in K/k$, is transcendental over k.

Example 3.15 $\sqrt{5} - \sqrt{3} \in \mathbb{R}$, is a root of $f(x) = (x - \sqrt{5} - \sqrt{3})(x - \sqrt{5} + \sqrt{3})(x - \sqrt{5} + \sqrt{3})(x + \sqrt{5} + \sqrt{3}) = x^4 - 16x^2 + 4$.

Definition 3.16 If K/k is an extension and $\alpha \in K$, then $k(\alpha)$ is the intersecion of all those subfields of k that contain k and α; we call $k(\alpha)$ the subfield of K obtained by ***adjoining*** α to k.

Example 3.17 $\mathbb{Q}(\sqrt{3}) = \mathbb{Q} + \mathbb{Q}\sqrt{3}$ is the smallest subfield of $\mathbb{R}/\mathbb{Q}$ that contains $\sqrt{3}$.

Proposition 3.18 If K/k is a finite field extension, then K/k is an algebraic extension.

PROOF. For a finite K/k, K is a vector space of some dimension n over k. Then for any $\alpha \in K$, the list of $n+1$ vectors $1, \alpha, \alpha^2, \ldots, \alpha^n$ must be linearly dependent. Then there are $a_0, a_1, \ldots a_n$, not all 0, such that $\sum a_i \alpha^i = 0$. Then α is a root of $f(x) = \sum a_i x^i$. ■

Remark. This suggest that for $\alpha \in K$, $p(x) = \text{irr}(\alpha, k)$ cannot have degree higher than $[K : k]$. This is true because $1, \alpha, \alpha^2, \ldots, \alpha^n$ are dependent; then we can obtain a $f(x)$ as in above proof with α as a root. $f(x) \leqslant n$; but $p(x) \mid f(x)$ by the definition of $p(x)$. Hence $\deg(p) \leqslant n$.

Example 3.19 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ with possible basis $\{1, \sqrt{2}\}$. Any element of the form $\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is algebraic over $\mathbb{Q}$ s.t. $\deg \text{irr}(\alpha, \mathbb{Q}) \leqslant 2$.

Theorem 3.20 (3.120) Let K/k be an extension of fields and let $\alpha \in K$ be algebraic over k.

(a) There exists a unique monic irreducible polynomial $p(x) \in k[x]$ having α as a root. Moreoever, if $I = (p(x))$, then $k[x]/I \cong k(\alpha)$ given by $f(x) + I \mapsto f(\alpha)$.

(b) If α' is another root of $p(x)$, then $k(\alpha) \cong k(\alpha')$.

PROOF.

(a) For algebraic $\alpha \in K$, consider the homomorphism of rings

$$\begin{aligned} \varphi : \quad & k[x] \to K \\ & f(x) \mapsto f(\alpha) \end{aligned}$$

The kernel of φ is a principle ideal (any ideal $I \in k[x]$ is a principle one, otherwise $\exists p(x), q(x) \in I, p \nmid q$ and $q \nmid p$, then there are some s, t s.t. $sp + tq = 1 \Rightarrow (p, q) = R$, I cannot be proper); we may let $\ker \varphi = (h(x))$ for some $h(x) \in k[x]$. Then $k[x]/(h(x)) \cong \text{im}\varphi \subseteq K$. $\text{im}\varphi$ is a subring of K and thus a domain; this gives that $h(x)$ is irreducible, and we can get $p(x)$ monic irreducible and $(p(x)) = (h(x))$. Finally, $\text{im}\varphi = k(\alpha)$, since $\text{im}\varphi$ is a subfield of K (since $k[x]/(h(x))$ is a field since $h(x)$ is irreducible) containing k (if we let $f(x) = c \in k$) and α (if we let $f(x) = x$); it is the smallest since every such subfield must contain all the polynomials of α. We then get $k[x]/I \cong k(\alpha)$. Uniqueness follows Proposition 3.12(d).

(b) The two isomorphisms, $k[x]/I \cong k(\alpha)$ and $k[x]/I \cong k(\alpha')$ induces a third: $k(\alpha) \cong k(\alpha')$.

■

Definition 3.21 For given K/k, $\alpha \in K$ algebraic over k, let $\text{irr}(\alpha, k) \in k[x]$ be the unique monic irreducible polynomial in $k[x]$ that has α as a root. $\text{irr}(\alpha, k)$ is called the minimal polynomial of α over k.

Example 3.22 $\text{irr}(\sqrt{5} - \sqrt{3}, \mathbb{Q}) = x^4 - 16x^2 + 4$.

Theorem 3.23 Let k be a field and let $f(x) \in k[x]$ be a nonzero polynomial. Then there exists a field K containing k as a subfield and with $f(x)$ a product of linear factors in $K[x]$.

PROOF. We prove via induction on the $\deg(f)$.

- ($\deg(f) = 1$). If $\deg(f) = 1$, $f(x)$ is already in linear factor form; $K = k$ then suffices.

- ($\deg(f) > 1$). If $\deg(f) > 1$, write $f(x) = p(x)g(x)$ in which $p(x)$ is irreducible. By Proposition 3.12(a), $F = k[x]/(p(x))$ is a field containing k and a root of $p(x)$ (a root in F is $z = x + I$, $I = (p(x))$). Hence, in $F[x]$, we have $p(x) = (x - z)h(x)$ and $f(x) = (x - z)h(x)g(x)$. Induction hypothesis then gives us a field K containing F in which $h(x)g(x)$, and hence $f(x)$, is a product of linear factors in $K[x]$.

■

10/17/08

Theorem 3.24 (3.121) Let $k \subseteq E \subseteq K$ be fields s.t. K/E and E/k are both finite. Then K/k is finite and

$$[K : k] = [K : E][E : k].$$

PROOF. We first show that every element of K can be expressed as linear combination with a basis of size $[K : E][E : k]$ over k, then we show that the basis is linearly independent.

(1) Let the basis of $[K : E]$ be $\beta_1, \beta_2, \ldots, \beta_m$ and that of $[E : k]$ be $\alpha_1, \alpha_2, \ldots, \alpha_n$. Then we may write any element $x \in K$ as $x = \sum_{i=0}^{m} c_i\beta_i$. For each c_i, we may write it using basis over k as $c_i = \sum_{j=0}^{n} d_{ij}\alpha_j$. Then $x = \sum_{i,j} d_{ij}\beta_i\alpha_j$ and $X = \{\beta_i\alpha_j\}$ spans K over k.

(2) To see that X is linearly independent, we see that for any linear combination of all basis elements in X to be 0, since β_i's are linearly independent, $\sum d_{ij}\alpha_j$ must all be zero. This in turn requires that all d_{ij}'s are zero.

■

Definition 3.25 Let $k \subseteq K$ be fields, let $f(x) \in k[x]$. Then $f(x)$ ***splits over*** K if

$$f(x) = a(x - z_1)(x - z_2)\ldots(x - z_n),$$

where $z_1, z_2, \ldots, z_n$ are in K and $a \in k$ is nonzero. For a given field k and given polynomial $f(x) \in k[x]$, E/k is a ***splitting field*** of $f(x)$ over k if $f(x)$ splits over E but not over any proper subfield of E.

Corollary 3.26 (3.124) Let k be a field, and let $f(x) \in k[x]$. Then a splitting field of $f(x)$ over k exists.

PROOF. By Kronecher's theorem, there is a field extension K/k such hat $f(x)$ splits in $K[x]$; say, $f(x) = a(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$. Then the subfield $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a splitting field of $f(x)$ over k. ■

Proposition 3.27 (3.126) Let p be a prime, and let k be a field. If $f(x) = x^p - c \in k[x]$, then either $f(x)$ is irreducible in $k[x]$ or c has a p-th root, say, α, in k. Therefore, if k contains the p-th roots of unity, then $k(\alpha)$ is a splitting field of $f(x)$.

PROOF. Suppose that $f(x)$ is not irreducible over k, then $f(x) = g(x)h(x), 1 \leqslant d = \deg g < p$. Let $(1, \omega, \omega^2, \ldots, \omega^{p-1}$ be the set of p-th roots of unity. We have

$$\begin{cases} f(x) &= (x - \alpha)(x - \alpha\omega)\ldots(x - \alpha\omega^{p-1}) \\ f(x) &= g(x)h(x) \end{cases}$$

Let b be the constant term of $g(x)$ be b, $\pm b = \alpha^d\omega$, in which ω is again a p-th root of unity ($\omega^p = 1$). Then

$$(\pm b)^p = (\alpha^d\omega)^p = \alpha^{dp} = c^d.$$

p is prime and $d < p$, therefore p, d are relative primes; $\gcd(d, p) = 1$ and we have $1 = sd + tp$ with s, t integers. We get

$$c = c^{sd+tp} = c^{sd}c^{dp} = (\pm b)^{ps}c^{tp} = [(\pm b)^s c^t]^p.$$

Therefore, c has a p-th root in k as $(\pm b)^s c^t$. If $\omega \in k$, $E = k(\alpha)$ is a splitting field of $f(x)$. ■

Theorem 3.28 (Galois, 3.127 in the text) Let p be a prime and $n > 0$. Then there exists a field of size p^n.

PROOF. Let $q = p^n, k = \mathbb{F}_p, g(x) = x^q - x \in k[x]$. By Kronecker's theorem, there exists K/k s.t. $g(x)$ splits over K. Let $E \subseteq K$ be the subset

$$E = \{\alpha \in K : g(\alpha) = 0\},$$

we claim that E is a field of size $q = p^n$. To see this, we first show that $g(x)$ has no multiple roots. For a multiple root α, $(x - \alpha) \mid g(x)$ and $(x - \alpha) \mid g'(x)$; but $g'(x) = qx^{q-1} - 1 = -1$ (we get -1 by $\mod p$ since we work with $\mathbb{F}_p$). Therefore, all the roots are distinct, and $|E| = q = p^n$.
We are then left to verify that E is a subfield of K. We have:

- $1 \in E$ since 1 is a root of $x^q - x$.
- For $a, b \in E$, $(ab)^q = a^q b^q = ab$ (since $a^q - a = 0 \Rightarrow a = a^q$). We thus have $ab \in E$.
- For $a, b \in E$, $(a + b)^q = a^q + \ldots + b^q = a^q + b^q = a + b \in E$. All cross terms $\binom{q}{k}a^k b^{q-k}$ are zeros because $p \mid \binom{q}{k}$; therefore $\binom{q}{k}a^k b^{q-k} \equiv 0 \mod p$.
- Inverse. $a \in E$, $a^{q-1} = 1$, then $a^{q-2}a = 1 \Rightarrow a^{-1} = a^{q-2}$.

therefore, E is a field of size p^n. ■

10/20/08

Corollary 3.29 (3.128)For given p and $n > 0$, there exists an irreducible polynomial $g(x) \in \mathbb{F}_p[x]$ of degree n.

PROOF. Let $E/\mathbb{F}_p$ be a field extension with $q = p^n$ elements, then $E^* = E\backslash\{0\}$ is a group of size $q - 1$. Moreover, this group is cyclic by Lemma 2.20. Then $E^* = \langle\alpha\rangle$ for some α of multiplicative order $q - 1$. $E = \mathbb{F}_p(\alpha)$ since on one hand $\mathbb{F}_p(\alpha) \subseteq E$; on the other $\mathbb{F}_p(\alpha)$ contains α and then every nonzero elements of E. Let $p(x) = \text{irr}(\alpha, \mathbb{F}_p)$, degree $d = [\mathbb{F}_p[x]/(f(x)) : \mathbb{F}_p]$ (Proposition 3.12(e)). But $\mathbb{F}_p[x]/(p(x)) \cong \mathbb{F}_p(\alpha) = E$ by Theorem 3.20 in the text. Therefore $d = [E : \mathbb{F}_p] = n$; $f(x)$ is an irreducible polynomial of degree n. ■

Lemma 3.30 (3.130) Let $f(x) \in k[x]$, where k is a field, and let E be a splitting field of $f(x)$ over k. Let $\varphi : k \to k'$ be an isomorphism of fields, let $\varphi^* : k[x] \to k'[x]$ be the isomorphism

$$g(x) = a_0 + a_1x + \ldots + a_nx^n \mapsto g^*(x) = \varphi(a_0) + \varphi(a_1)x + \ldots + \varphi(a_n)x^n,$$

that is, φ^* is an extension of φ to $k[x]$. Let E' be a splitting field of $f^*(x)$ over k'. Then there is an isomorphism $\Phi : E \to E'$ extending φ.

PROOF. We prove via induction on the degree of $d = [E : k]$.

($d = 1$). $f(x) \in k[x]$ has all roots in k, then $f(x)$ is product of linear polynomials, $f^*(x) = \varphi(f(x))$ is also product of linear polynomials in k'; then $E' = k'$ is a splitting field of $f^*(x)$.

($d > 1$). Let $z \notin k$ be a root of $f(x)$ in E, and let $p(x) = \text{irr}(z, k)$ be the minimal irreducible polynomial with z as a root. $\deg(p) > 1$ since $z \notin k$. Then $k[x]/(p(x)) \cong k(z) \subseteq E$ and $[k(z) : k] = \deg(p)$. Given $\varphi : k \cong k'$, $p^*(x) = \varphi(p(x))$ is again a minimal irreducible polynomial in $k'[x]$ (if one of p, p^* can be factorized, then φ, being an isomorphism, would indicate that the other is as well). Let z' be a root of $p^*(x)$, then φ extends to an isomorphism $\widetilde{\varphi}$ of $k(z) \to k'(z')$ by Theorem 3.20 (before applying Theorem 3.20, we note that $\varphi : k \to k'$ extends naturally to an isomorphism $\varphi' : k[x] \cong k'[x], f(x) \mapsto f^*(x)$; φ' then induces an isomorphism $\varphi'' : k[x]/(p(x)) \cong k'[x]/(p^*(x))$, $f(x) + I \mapsto f^*(x) + I^*$. Then $k(z) \cong k[x]/(p(x)) \cong k'[x]/(p^*(x)) \cong k'(z')$).
Then E is again a splitting field of $f(x) \in k(z)[x]$ since all roots of $f(x)$ are still in E. Similarly E' a splitting field of $f^*(x) \in k'(z')[x]$. But now $[E : k(z)] < [E : k]$, so we may apply inductive hypothesis that $\widetilde{\varphi}$ extends to some Φ that is an isomorphism between E and E'; then φ also extends to Φ.

■

Theorem 3.31 Any two splitting fields E and E' for $f(x)$ over k are isomorphic.

PROOF. This is the case when $k = k'$ in previous lemma. ■

Corollary 3.32 (E. H. Moore, 3.132 in the text) Any two finite fields having exactly p^n elements are isomorphic. Alternatively, a field of size $q = p^n$ is unique up to isomorphism.

PROOF. Let E be a field of size $q = p^n$, then $E^* = E \backslash \{0\}$ is a cyclic group of order $q - 1$ and $\alpha^{q-1} = 1$ for all $\alpha \in E^*$; $\alpha^q - \alpha = 0$ for all $\alpha \in E$. Thus, E of size p^n is a splitting field for $g(x) = x^q - x$ over $\mathbb{F}_p$ (since $x^q - x \in \mathbb{F}_p[x]$) and therefore, E is a unique up to isomorphism. ■

Extra: The number of irreducible polynomials of given degree is encoded by a Zeta function. The classical Riemann Zeta function is $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, s \in \mathbb{C}$. **[see text/notes for now, may be added later]**

10/22/08

Definition 3.33 Let E/k be a filed extension. An ***automorphism*** σ of E is an isomorphism $\sigma : E \to E$. σ ***fixes*** k if $\sigma(a) = a$ for all $a \in k$.

Proposition 3.34 (4.1) Let k be subfield of a field K, let

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

and let $E = k(z_0, z_1, \ldots, z_n) \subseteq K$ be a splitting field for f over k. If σ is an automorphism of E fixing k, then σ permutes the roots.

PROOF. Suppose α is a root of $f(x)$, from

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,$$

we obtain that

$$\begin{aligned} 0 = \sigma(f(\alpha)) &= \sigma(\alpha)^n + \sigma(a_{n-1}\alpha^{n-1}) + \ldots + \sigma(a_1(\alpha)) + \sigma(a_0) \\ &= \sigma(\alpha^n) + a_{n-1}\sigma(\alpha)^{n-1} + \ldots + a_1\sigma(\alpha) + a_0 \\ &= f(\sigma(\alpha)), \end{aligned}$$

since $\sigma(a_i) = a_i$ by the assumption that σ fixes k. Therefore $\sigma(\alpha)$ is also a root of $f(x)$. On the other hand, since $\sigma : E \to E$ is isomorphism and the number of roots are finite, σ is a bijection between $\{z_i\}$ and itself, therefore permuting the roots. ■

Definition 3.35 Let E/k be a field extension. The ***Galois group*** of E over k, $\mathrm{Gal}(E/k)$, is the set of all automorphisms of E that fixes k. Let $f(x) \in k[x]$ has splitting field E over k, the ***Galois group*** of f over k is $\mathrm{Gal}(E/k)$.

Lemma 3.36 (4.2 in the test) Let $E = k(z_1, z_2, \ldots z_n)$ and let $\sigma \in \mathrm{Gal}(E/k)$ be such that $\sigma(z_i) = z_i$ for $i = 1, 2, \ldots, n$, then $\sigma = \mathrm{id}_E$.

PROOF. We prove via induction on n.

(1) $(n = 1)$. $E = k(z_1)$, let $\alpha \in E$, then $\alpha = \frac{f(z_1)}{g(z_1)}$ for $f, g \in k[z], g(z_1) \neq 0$. Then $\sigma(\alpha) = \frac{\sigma(f(z_1))}{\sigma(g(z_1))} = \frac{f(z_1)}{g(z_1)} = \alpha$.

(2) $(n > 1)$. Let $K = k(z_1, z_2, \ldots, z_{n-1})$, if σ fixes $z_1, z_2, \ldots, z_n$ then σ fixes K by induction hypothesis; σ fixes E after we apply (n=1) case again.

■

Theorem 3.37 (4.3) For $f(x) \in k[x]$, $\deg f = n$. The Galois group $\mathrm{Gal}(E/k)$ is isomorphic to a subgroup of S_n.

PROOF. Let $X = \{z_1, z_2, \ldots, z_n\}$. Define

$$\varphi : \mathrm{Gal}(E/k) \to \mathrm{Symm}(X),$$

by $\varphi : \sigma \mapsto \sigma|X$. $\sigma|X$ is the restriction of σ to X. We need to verify that φ gives an injective homomorphism.

- $\varphi(\sigma\tau)(z_i) = (\sigma\tau)(z_i) = \sigma(\tau(z_i)) = \sigma((\varphi(\tau))(z_i)) = ((\varphi(\sigma)\varphi(\tau))(z_i))$. Therefore φ is a homomorphism.
- The kernel of φ fixes $z_i \in X$; by previous lemma, σ is the identity element. Since there is a single element in the kernel, the map is injective.

We then have an injective homomorphism from $\mathrm{Gal}(E/k)$ to $\mathrm{Symm}(X)$, but $\mathrm{Symm}(X)$ is a subgroup of S_n (since some elements of X may be multiple roots). We are done. ■

Lemma 3.38 (4.4) If k is a field of characteristic $k = 0$, then an irreducible polynomial $f(x) \in k[z]$ has no repeated roots.

PROOF. Let $f(x) \in k[x], f(x) \neq 0$ be irreducible. We may assume that $\deg f > 1$, which implies $f'(x) \neq 0$ since $k = 0$ (that is, we don't need to consider the modulo stuff). $f(x)$ has a repeated root if and only if $\gcd(f, f') \neq 1$. But $f(x)$ irreducible, so $f' \nmid f$, $\gcd(f, f') = 1$. ■

Definition 3.39 Let E/k be algebraic. An ***irreducible polynomial*** $f(x) \in k[x]$ is ***separable*** if it has no repeated roots. An ***arbitrary polynomial*** $f(x) \in k[x]$ is ***separable*** if its irreducible factors are separable. An ***element*** $\alpha \in E$ is ***separable over*** k if $\text{irr}(\alpha, k)$ is separable. E/k is ***separable*** if α is separable over k for every $\alpha \in E$.

Example 3.40 Let $k = \mathbb{F}_p(t) = \text{Frac}(\mathbb{F}_p[t])$, let $f(x) = x^p - t$. Claim: $f(x)$ is irreducible over k and is not separable. Let α be any root of $f(x)$ s.t. $\alpha^p = t$. Then $f(x) = x^p - t = x^p - \alpha^p = (x - \alpha)^p$. Therefore $f(x)$ has repeated roots and is inseparable. To show that $f(x)$ is irreducible, by proposition 3.27, $f(x)$ is either irreducible in k or it contains a root in k; suppose it contains a root $\alpha \in k$. Say $\alpha = \frac{g(t)}{h(t)}$, then $\alpha^p(h(t))^p = (g(t))^p \Rightarrow t(h(t))^p = (g(t))^p$, the leading powers of t at two sides cannot match, contradiction.

10/24/2008

Theorem 3.41 (4.7) Let E/k be a splitting field for $f(x) \in k[x]$, $f(x)$ separable in E/k.

(1) for $\varphi : k \cong k'$ and for a splitting field E' for $f^* = \varphi(f)$, φ extends to exactly $[E : k]$ isomorphisms $\Phi : E \to E'$.

(2) $|\text{Gal}(E/k)| = [E : k]$.

PROOF. Sketch of ideas: It works similarly as Lemma 3.30. Here the induction is on $[E : k]$. For induction step, we again pick a $p(x)$ irreducible, and it has degree d with d non-repeating roots. For α as a root of $p(x)$, for each α' as a root of $p^*(x)$, there is an extension of isomorphism from $k \cong k'$ to isomorphism $k(\alpha) \cong k'(\alpha')$. There are exactly d of these. Then we can apply induction hypothesis over $k(\alpha)[x]$ to get that there are $[E : k(\alpha)]$ isomorphisms between E, E' extending $\widetilde{\varphi}$. We then obtain the result.
Note that here we don't need to consider other roots of $p(x)$ since we are basically trying to construct E from one side and find corresponding isomorphisms on the other side. For this reason, using $k(\alpha)$ or $k(\beta)$ are the same; but we don't need to use both to construct E. ■

Corollary 3.42 (4.9) If moreover $f(x)$ is irreducible, then $n = \deg(f) \mid |\text{Gal}(E/k)|$.

PROOF. $n = \deg(f) = [k(\alpha) : k]$ and $[E : k(\alpha)][k(\alpha) : k] = [E : k]$. ■

Theorem 3.43 (4.12) Let $k = \mathbb{F}_p, E = \mathbb{F}_{p^n}$, where E is the splitting field of $g(x) = x^q - x$ over $\mathbb{F}_p$ for $q = p^n$. Then $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n with generator:

$$\text{Frob} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, u \mapsto u^p$$

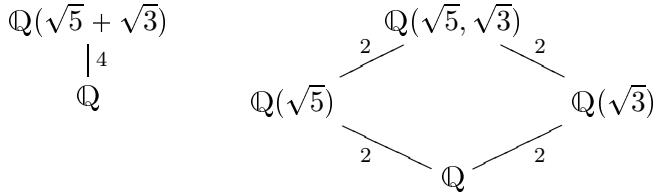
PROOF. We know that $|\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$ by Theorem 3.41. Therefore, we only need to verify that Frob is an automorphism of $\mathbb{F}_{p^n}$ that fixes $\mathbb{F}_p$, and that Frob is of order n. Let $q = p^n$, and let $G = \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Since $\mathbb{F}_q$ has characteristic p, we have $\text{Frob}(a+b) = (a+b)^p = a^p + b^p = \text{Frob}(a) + \text{Frob}(b), \text{Frob}(ab) = (ab)^p = a^p b^p = \text{Frob}(a)\text{Frob}(b)$, and Frob is homomorphism of fields (a field under ring homomorphism maps to a field, since $1 \to 1$ and for any $f(a), \exists b, ab = 1 \Rightarrow f(a)f(b) = 1$). As a homomorphism from a field, Frob is injective (since kernel is an ideal in $\mathbb{F}_q$; a field only has itself or $\{0\}$ as ideals. Since 1 is mapped to 1, the whole field is not the kernel.), $\mathbb{F}_q$ is finite, Frob is bijective and then an automorphism.
Frob fixes $\mathbb{F}_p$ since for $a \in \mathbb{F}_p$, $a^p \equiv a \mod p$ (Fermat's little theorem). The order of Frob is n since $u^{p^n} = u$ for all u. If smaller n' can satisfy $u^{p^{n'}} = p$ for all roots of $u^{p^n} = u$, then $u^{p^{n'}} = p$ has too many roots. ■

Example 3.44 $\mathbb{F}_4/\mathbb{F}_2$ is the splitting field of $x^4 - x = x(x+1)(x^2+x+1) = x(x+1)(x+\alpha)(x+\alpha^2)$. We have

	$\overbrace{\text{Gal}(\mathbb{F}_4/\mathbb{F}_2)}$	
u	id(u)	Frob(u)
0	0	0
1	1	1
α	α	α^2
α^2	α^2	α

Example 3.45 $F(x) = x^4 - 16x^2 + 4 = \text{irr}(\sqrt{5} + \sqrt{3}, \mathbb{Q}) \in \mathbb{Q}[x]$,

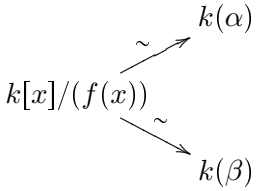


$\mathbb{Q}(\sqrt{5}+\sqrt{3}) = \mathbb{Q}(\sqrt{5},\sqrt{3})$ is a splitting field for $f(x)$ over $\mathbb{Q}$,

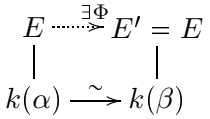
$$\begin{aligned}\text{Gal}(\mathbb{Q}(\sqrt{5},\sqrt{3})/\mathbb{Q}) &= \{(\sqrt{5}\mapsto\sqrt{5}, \sqrt{3}\mapsto\sqrt{3}), (\sqrt{5}\mapsto-\sqrt{5}, \sqrt{3}\mapsto\sqrt{3}),\\ &\quad (\sqrt{5}\mapsto\sqrt{5}, \sqrt{3}\mapsto-\sqrt{3}), (\sqrt{5}\mapsto-\sqrt{5}, \sqrt{3}\mapsto-\sqrt{3})\}\end{aligned}$$

Proposition 3.46 (4.13) Let k be a field and let E/k be a splitting field for $f(x) \in k[x]$ s.t. $f(x)$ has no repeated roots. Then $f(x)$ is irreducible if and only if $\text{Gal}(E/k)$ acts transitively on the roots of $f(x)$.

PROOF. ($\Rightarrow$). Let $f(x)$ be irreducible and let α, β be roots of $f(x)$. Since



there exists $\varphi : k(\alpha) \cong k(\beta)$; then



φ extends to an automorphism $\Phi : E \to E$ s.t. Φ fixes k and $\Phi(\alpha) = \beta$.
($\Leftarrow$). Let $f(x) = q_1(x)q_2(x)\dots q_t(x)$ for irreducible polynomial $q_1, \dots, q_t$. Let $q_1(\alpha), q_2(\beta) = 0$. By assumption, there exists $\sigma : E \to E, \sigma \in \mathrm{Gal}(E/k)$. s.t. $\sigma(\alpha) = \beta$. But then $q_1(\beta) = 0$ and β is a multiple root (it appears in both q_1, q_2), contradiction. ■

Alternative proof of Corollary 3.42: Proof. $G = \mathrm{Gal}(E/k)$ acts transitively on X as the set of roots of f, where $|X| = n = \deg f$. Then $|G| = |G_x||X| \Rightarrow n \mid |G|$. ■

Example 3.47 Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, $f(x)$ is irreducible (by Eisenstein). What is the splitting field of $f(x)$ over $\mathbb{Q}$? $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2} + \sqrt[3]{4})$, let $x = \sqrt[3]{2}u$, $x^3 - 2 = 2(u-1)(u^2+u+1)$. We have

$$\begin{array}{c} E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) \\ \Big| 2 \\ \mathbb{Q}(\sqrt[3]{2}) \\ \Big| 3 \\ \mathbb{Q} \end{array}$$

hence $[E : \mathbb{Q}] = 6$, which is maximal for f of degree 3. In general, for $\deg f = n, \mathrm{Gal}(E/k) \subseteq S_n$; in our case $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$.

10/27/2008

Definition 3.48 A ***pure extension*** of type m is an extension $k(u)/k, u^m \in k$ for some $m \geqslant 1$. An extension K/k is a ***radical extension*** if there is a tower of fields

$$k = K_0 \subseteq K_1 \subseteq \dots \subseteq K_t,$$

in which each K_{i+1}/K_i is a pure extension.

Definition 3.49 Let $f(x) \in k[x]$ have splitting field E/k. We say $f(x)$ is ***solvable by radicals*** if there is a radical extension

$$k = K_0 \subseteq K_1 \subseteq \dots \subseteq K_t,$$

with $E \subseteq K_t$.

Proposition 3.50 Ever irreducible cubic

$$f(x) = x^3 + bx^2 + cx + d \in k[x]$$

is solvable by radicals.

Proof. [sketched] Apply change of variable twice, first time let $x = x - \frac{b}{3}$, then $x = g + h$. This yields the equation

$$g^3 + h^3 + (3gh + q)x + r = 0$$

. Obviously, solutions of g, h to

$$\begin{cases} g^3 + h^3 = -r \\ gh = -\frac{1}{3}q \end{cases}$$

will also be solutions to the original equation when we add up g and h. It turns out that three solutions are obtained this way; since a cubic has only three roots, these are all the solutions. ■

Remark. The material that will be covered in the next several lectures will lead to theorem 4.26 and 4.53 in the text. 4.26 says that if $f(x)$ is solvable by radicals then $\mathrm{Gal}(E/k)$ is solvable for characteristic $k = 0$. 4.52 makes 4.26 stronger by showing the other ways around is also true (if and only if). We can thend draw conclusions that cubics and quartics are solvable by radicals since for $f(x) \in k[x]$, $\mathrm{Gal}(E/k) \subseteq S_3$(cubics) or S_4(quartics). Since S_3, S_4 are both solvable, cubics and quartics are solvable by radicals.

Theorem 3.51 (4.16) Let $k \subseteq B \subseteq E$ s.t. B/k is a splitting field for $f(x) \in k[x]$. E/k is a splitting field for $g(x) \in k[x]$. Then $\mathrm{Gal}(E/B) \lhd \mathrm{Gal}(E/k)$ and $\mathrm{Gal}(E/k)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/k)$.

Proof. Let $B = k(z_1, \ldots, z_n)$, let $\sigma \in \mathrm{Gal}(E/k)$, then σ permutes the roots of f by the proof used in Proposition 3.34. In particular, $\sigma(B) = B$. Define $\rho : \mathrm{Gal}(E/k) \to \mathrm{Gal}(B/k)$ by $\sigma \mapsto \sigma|_B$. We then claim that ρ is a homomorphism with $\ker \rho = \mathrm{Gal}(E/B)$, and ρ is surjective. ρ is a homomorphism can be obtained similarly as that in Theorem 3.37. We also have $\ker \rho = \mathrm{Gal}(E/B)$ since the kernel is exactly these permutations in E that fixes B. It follows that $\mathrm{Gal}(E/B)$ is a normal subgroup of $\mathrm{Gal}(G/k)$. ρ is surjective by Lemma 3.30: if $\tau \in \mathrm{Gal}(B/k)$, then there is $\sigma \in Gal(E/k)$ extending τ. The first isomorphism theorem then gives the result. ■

Definition 3.52 A ***character*** of a group G in a field K is a group homomorphism $\chi : G \to K^*$(K^* is the multiplicative group of K with 0 removed).

Remark. Since a field K with zero removed is a multiplicative group (denote this as K^*), then $\sigma \in \mathrm{Aut}(K)$ restricted to K^* (denoted as $\sigma|_{K^*}$) is then a character in K.

Lemma 3.53 (E.Artin) A set of distinct characters $\{\chi_1, \ldots, \chi_n\}$ is independent. That is, if $a_1, \ldots, a_n$ are such that

$$(*) \qquad a_1\chi_1(g) + a_2\chi_2(g) + \ldots + a_n\chi_n(g) = 0,$$

for all $g \in G$, then $a_1 = a_2 = \ldots = a_n = 0$.

Proof. Proof by descent. Assuming that a relation $(*)$ exists with nonzero coefficient, we show that there exists a relation with fewer nonzero coefficients. Clearly, at least two coefficients in $(*)$ are nonzero. Say $a_1, a_2 \neq 0$. Let $h \in G$ be s.t. $\chi_1(h) \neq \chi_2(h)$, then

$$a_1\chi_1(gh) + \ldots + a_n\chi_n(gh) = 0 \Leftrightarrow a_1\chi_1(h)\chi_1(g) + \ldots + a_n\chi_n(g)\chi_n(h) = 0.$$

Subtract $(*)\chi_1(h)$ from the second equation yields

$$a_2(\chi_2(h) - \chi_1(h))\chi_2(g) + \ldots + a_n(\chi_n(h) - \chi_1(h))\chi_n(g) = 0,$$

let $a_1' = a_2(\chi_2(h) - \chi_1(h)), \ldots$, we obtain a smaller set of χ_i's that are dependent. ■

Corollary 3.54 (Dedekind) Let $G = K^*$ and let $\{\sigma_1, \ldots, \sigma_n\}$ be distinct field automorphism, then $\{\sigma_1, \ldots, \sigma_n\}$ are independent.

PROOF. Apply previous lemma. ■

10/29/2008

Lemma 3.55 (4.17)

(1) Let $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a finite extension of fields. Then there is a finite extension E/k s.t. E/k is a splitting field for some $f(x) \in k[x]$(Such an extension E/k of smallest degree is called the ***normal closure*** of K/k). Moreover, if each α_i is separable over k, then $f(x)$ can be chosen to be a separable polynomial.

(2) If K is a radical extension of k then a normal closure E/k is also a radical extension.

PROOF.

(1) Theorem 3.20 gives us $p_i(x) = \text{irr}(\alpha_i, k)$ has α_i as a root for each α_i. Let $f(x) = p_1(x) \ldots p_n(x)$, we have E that is a splitting field of $f(x)$ containing K. If α_i is separable over k then from definition $f(x)$, as a product of irreducible polynomials that are separable, is itself separable.

(2) We can write the radical extension K as $k_0 = k \subseteq k_1 = k(u_1) \subseteq k_2 = k(u_1, u_2) \subseteq \ldots \subseteq k_t = k(u_1, u_2, \ldots, u_t) = K$ s.t. k_{i+1}/k_i is a pure extension ($u_{i+1}^{m_{i+1}} \in k_i$). We may let

$$G = \text{Gal}(E/k) = \{\sigma_1 = \text{id}, \sigma_2, \ldots, \sigma_r\}.$$

Let $B_0 = k$. We construct a tower

$$B_0 = k \subseteq k(u_1 = \sigma_1(u_1)) \subseteq k(u_1, \sigma_2(u_1)) \subseteq \ldots \subseteq k(u_1, \sigma_2(u_1), \ldots, \sigma_r(u_1)) = B_1.$$

Any σ_j, being an automorphism then a homomorphism (that is, $\sigma_j(ab) = \sigma_j(a)\sigma_j(b)$), gives $\sigma_j(u_1)^{m_1} = \sigma_j(u_1^{m_1})$. Since $u_1^{m_1} \in k$ and σ_j fixes k, $\sigma_j(u_1)^{m_1} \in k = B_0$. Thus B_1/B_0 is a radical extension. Similarly we may define

$$B_{i+1} = B_i(u_{i+1}, \sigma_2(u_{i+1}), \ldots, \sigma_r(u_{i+1})),$$

It is straightforward to see that B_{i+1}/B_i is a radical extension. Since $E = B_t$, we have that E is also a radical extension.

■

Lemma 3.56 (4.18) Let K/k be a radical extension, say $k = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_t = K$. Assume that moreover $[K_{i+1} : K_i] = p_i$ is prime, and let that k contains p_i-th roots of unity for $i = 1, 2, \ldots, t$. If K/k is a splitting field then there exits a sequence of subgroups

$$\text{Gal}(K/k) = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_t = \{e\}$$

s.t. $G_{i+1} \lhd G_i$ and $[G_i : G_{i+1}] = p_i$. In other words, $G = \text{Gal}(K/k)$ is solvable.

PROOF. For each i, let $G_i = \mathrm{Gal}(K/K_i)$. Since elements of $G_i = \mathrm{Gal}(K/K_i)$ are automorphisms of K that fixes K_i, they certainly contain all elements that fixes K_{i+1}, thus having $G_{i+1} = \mathrm{Gal}(K/K_{i+1})$ as a subgroup, therefore we have the subgroup relationship

$$\mathrm{Gal}(K/k) = G_0 \geqslant G_1 \geqslant G_2 \geqslant \ldots \geqslant G_t = \{1\}.$$

Since $K_1 = k(u)$ with $u^{p_1} \in k$, and k contains the p_1th roots of unity, K_1 is the splitting field for $f(x) = x^{p_1} - u^{p_1}$. Obviously, K is also a splitting field for $f(x)$. Theorem 3.51 then applies to say that $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/K_1) \cong \mathrm{Gal}(K_1/k)$ and $G_1 = \mathrm{Gal}(K/K_1)$ is normal in $G_0 = \mathrm{Gal}(K/k)$. Since $|\mathrm{Gal}(K_1/k)| = [K_1 : k] = p_1$ by Lemma 3.55, $G_0/G_1 \cong \mathbb{Z}/p_1\mathbb{Z}$ is cyclic of oder p_1. Repeating this for all i then yields the result. ■

Theorem 3.57 Construction of a polynomial not solvable by radicals.
Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p s.t. $f(x)$ has precisely two complex roots. Then the splitting field $E/\mathbb{Q}$ of $f(x)$ has groups $\mathrm{Gal}(E/\mathbb{Q}) \cong S_p$.

10/31/2008

Items to cover today:

- Construct $f(x) = x^p + \ldots \in \mathbb{Q}[x]$, with Galois group S_p.
- Compare normal extension versus splitting field extension (same).
- Remove condition in Lemma 3.56.

Theorem 3.58 ***Construction of*** $f(x) = x^p + \ldots \in \mathbb{Q}[x]$***, with Galois group*** S_p**.** Let $f(x) = x^p + \ldots \in \mathbb{Q}[x]$ be an irreducible polynomial with precisely two complex roots. Then the splitting field $E/\mathbb{Q}$ of $f(x)$ has group $\mathrm{Gal}(E/\mathbb{Q}) \cong S_p$.

PROOF. We want to construct $S_p = \langle (12), (12\ldots p) \rangle$. Let α be a root of $f(x)$, then $p = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $p \mid [E : \mathbb{Q}]$. For a splitting field $E/\mathbb{Q}$, $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]$. Hence, $\mathrm{Gal}(E/\mathbb{Q})$ contains an element of order p. Since $\mathrm{Gal}(E/\mathbb{Q}) \subseteq S_p$, $\mathrm{Gal}(E/\mathbb{Q})$ contains an element $\sigma = (i_1, i_2, \ldots, i_p)$. Let $\tau \in \mathrm{Gal}(E/\mathbb{Q})$ corresponds to complex conjugation, then $\tau = (j_1, j_2)$ (there exists τ since complex conjugation only affects the two complex roots and fixes everything else). wlog, we may assume $\tau = (12)$ and $\sigma = (12\ldots p)$ (by taking a suitable power of $\sigma = (i_1, i_2, \ldots, i_p)$). ■

Definition 3.59 An extension is ***normal*** if for every $\alpha \in E$, α algebraic over k, the polynomial $p(x) = \mathrm{irr}(\alpha, k)$ splits in E.

Theorem 3.60 A finite extension E/k is normal if and only if E is the splitting field of some polynomial $f(x) \in k[x]$.

PROOF. ($\Rightarrow$) Assume $E = k(\alpha_1, \ldots, \alpha_n)$, E is the splitting field of $f(x) = \prod_{i=1}^{n} \mathrm{irr}(\alpha_i, k)$.
($\Leftarrow$) let E/k be the splitting field for $f(x) \in k[x]$, let $\alpha \in E$, let $g(x) = \mathrm{irr}(\alpha, k)$. We have $E = E(\alpha)$. Let α' be another root of $g(x)$. Then we have that $k(\alpha) \cong k(\alpha')$ with isomorphism φ. We then have that $f(x) \in k(\alpha)[x]$ have $E(\alpha)$ as the splitting field since all of $f(x)$'s roots are in E. Similarly, $f(x) \in k(\alpha')[x]$ has $E(\alpha')$ as

the splitting field. By Lemma 3.30, φ extends to an isomorphism between $E(\alpha), E(\alpha')$. But $E = E(\alpha)$ and $E \subseteq E(\alpha')$, therefore $E = E(\alpha')$. ■

Remark. Lemma 3.56 has two conditions that will be removed: 1. k contains the pth roots of unity whenever $p \mid [K : k]$, 2. K/k is a splitting field. Next lemma removes the second condition.

Lemma 3.61 (4.20) Let k be a field and let $f(x) \in k[x]$ be solvable by radicals: There is a radical extension $k = K_0 \subseteq K_1 \subset \ldots K_t$ with K_t containing a splitting field E of $f(x)$. If each K_{i+1}/K_i is a pure extension of prime type p_i, and if k contains all the p_i-th roots of unity, then the Galois group $\mathrm{Gal}(E/k)$ is a quotient of a solvable group.

PROOF. We work with the normal closure of K/k, say L. By Lemma 3.55, L/k is a splitting field extension and a radical extension. Then Lemma 3.56 gives us that $\mathrm{Gal}(L/k)$ is solvable. Since L/k, E/k are both splitting field extensions, by Theorem 3.51, $\mathrm{Gal}(E/k) \cong \mathrm{Gal}(L/k)/\mathrm{Gal}(L/E)$ is again solvable (quotient group of a solvable group is again solvable by 4.21). ■

11/03/08

Remark. Summary of 4.17 - 4.20
Let $f(x) \in k[x]$ be solvable by radicals. Then there exists a tower

$$\begin{array}{ll} L & \text{normal closure of} K/k \\ | & \\ K & \text{radical extension over} k \\ | & \\ E & \text{splitting field of} f(x) \text{over} k \\ | & \\ k & \end{array}$$

Assume moreover that k contains the p-th roots of unity whenever $p \mid [K : k]$.
Combining the following with Lemma 3.55 (4.17),

- L/k is splitting field over k;
- L/k is radical;
- $p \mid [L : k] \Rightarrow p \mid [K : k]$.

Lemma 3.56 (4.18) says that if $E = K = L$, then $\mathrm{Gal}(E/k)$ is solvable.
Lemma 3.61 (4.20) says that if $E \subseteq K \subseteq L$, then $\mathrm{Gal}(E/k)$ is a quotient group of $\mathrm{Gal}(L/k)$ and then is solvable.

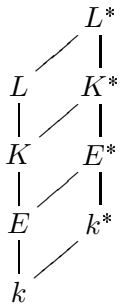
Lemma 3.62 Let k^*/k be a splitting field for $g(x) = x^m - 1 \in k[x]$, then k^*/k is abelian.

PROOF. Let $\sigma, \tau \in \mathrm{Gal}(k^*/k)$, say $\sigma(\omega) = \omega^a, \tau(\omega) = \omega^b$, where ω is a primitive mth root of unity, then $(\sigma\tau)(\omega) = (\omega^b)^a = (\tau\sigma)(\omega)$. ■

Example 3.63 Special case when $k = \mathbb{Q}, k^* = \mathbb{Q}(\omega)$.
$(\mathbb{Z}/m\mathbb{Z})^* \cong \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ with $(a \mod m) \mapsto (\sigma : \omega \mapsto \omega^a)$.
For $m = 15$, $[\mathbb{Q}(\omega) : \mathbb{Q}] = |(\mathbb{Z}/15\mathbb{Z})^*| = 8$, $(\mathbb{Z}/15\mathbb{Z})^* \cong (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Abelian but not cyclic.

Theorem 3.64 (4.26) Let $f(x) \in k[x]$ be solvable by radicals and let E/k be the splitting field of $f(x)$ over k. Then $\mathrm{Gal}(E/k)$ is solvable.

PROOF. The idea is to construct another tower



by letting k^*/k be the splitting field of $x^m - 1 \in k[x]$ where m is large enough s.t. $p \mid m$ whenever $p \mid [K : k]$. Then k^* contains all the pth roots of unity that we need to apply Lemma 3.61. We then have that $\mathrm{Gal}(E^*/k^*)$ is solvable. Now look at the tower $k - k^* - E^*$, since $E^*/k, k^*/k$ are splitting field extensions (and k^*/k solvable by construction), by Theorem 3.51, $\mathrm{Gal}(E^*/k^*)$ is normal in $\mathrm{Gal}(E^*/k)$ with quotient group isomorphic to $\mathrm{Gal}(k^*/k)$; therefore $\mathrm{Gal}(E^*/k)$ is also solvable. Finally for the tower $k - E - E^*$, $E^*/k, E/k$ are splitting field extensions, we then apply Theorem 3.51 again to get that $\mathrm{Gal}(E/k) \cong \mathrm{Gal}(E^*/k)/\mathrm{Gal}(E^*/E)$ and therefore solvable as a quotient group. ■

Remark. Now the ***Fundamental Theorem of Galois Theory*** starts.

Definition 3.65 For a field E and for a subfield $H \subseteq \mathrm{Aut}(E)$, define the ***fixed field*** of H as

$$E^H = \{a \in E : \sigma(a) = a, \forall \sigma \in H\},$$

that is, the part of E that is fixed by H.

Remark. If $H = \mathrm{Gal}(E/k) \subseteq \mathrm{Aut}(E)$, then $E^H \supseteq k$; this is true because any $\sigma \in \mathrm{Gal}(E/k)$ fixes k; therefore at least k is in the fixed field E^H.

Example 3.66 The inclusion $E^H \supseteq k$ can be strict. Let $E = \mathbb{Q}(\sqrt[3]{2}$. If $\sigma \in G = \mathrm{Gal}(E/\mathbb{Q})$, then σ must fix $\mathbb{Q}$, and so it permutes the roots of $f(x) = x^3 - 2$. But the other two roots of $f(x)$ are not real, so that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. It now follows that σ is the identity and $E^G = E$.

Proposition 3.67 (4.28) If E is a field, then the function $H \mapsto E^H$ is order reversing: if $H \leqslant L \leqslant \mathrm{Aut}(E)$, then $E^L \subseteq E^H$.

PROOF. $a \in E$ fixed by L must be fixed by H, but not necessarily the other way around. ■

Definition 3.68 A rational function $\frac{g(x_1,x_2,\ldots,x_n)}{h(x_1,x_2,\ldots,x_n)} \in k[x]$ is a symmetric function if it is fixed by S_n.

Proposition 3.69 (4.30) A list $\sigma_1, \ldots, \sigma_n$ of distinct characters from $E^* \to E^*$ is independent over E.

Lemma 3.70 (4.31) If $G = \{\sigma_1, \ldots, \sigma_n\} \subseteq \mathrm{Aut}(E)$ is a set of distinct automorphisms then $[E : E^G] \geqslant n$.

PROOF. Suppose $[E : E^G] = r < n$, since E is an extension field of E^G, we may assume it has a basis $\alpha_1, \ldots, \alpha_r$. Then the system of equations

$$\begin{aligned}
&\sigma_1(\alpha_1)x_1 + \sigma_2(\alpha_1)x_2 + \ldots + \sigma_n(\alpha_1)x_n = 0\\
&\sigma_1(\alpha_2)x_1 + \sigma_2(\alpha_2)x_2 + \ldots + \sigma_n(\alpha_2)x_n = 0\\
&\ldots\\
&\sigma_1(\alpha_r)x_1 + \sigma_2(\alpha_r)x_2 + \ldots + \sigma_n(\alpha_r)x_n = 0,
\end{aligned}$$

has a nontrivial solution $c_1, \ldots, c_n$, since $n > r$. Then for any $\beta \in E$,

$$\beta = b_1\alpha_1 + \ldots + b_r\alpha_r$$

then if we multiply b_i with the ith row of the system and note that $b_i = \sigma_j(b_i)$ for any σ_j (since σ_j fixes E^G), we have

$$\begin{aligned}
&\sigma_1(b_1\alpha_1)c_1 + \sigma_2(b_1\alpha_1)c_2 + \ldots + \sigma_n(b_1\alpha_1)c_n = 0\\
&\sigma_1(b_2\alpha_2)c_1 + \sigma_2(b_2\alpha_2)c_2 + \ldots + \sigma_n(b_2\alpha_2)c_n = 0\\
&\ldots\\
&\sigma_1(b_r\alpha_r)c_1 + \sigma_2(b_r\alpha_r)c_2 + \ldots + \sigma_n(b_r\alpha_r)c_n = 0,
\end{aligned}$$

summing up all the rows then gives us

$$\sigma_1(\beta)c_1 + \sigma_2(\beta)c_2 + \ldots + \sigma_n(\beta)c_n = 0$$

which contradicts the independence of the characters $\sigma_1, \ldots, \sigma_n$. ■

11/05/08

Proposition 3.71 (4.32) If $G \subseteq \mathrm{Aut}(E)$ is a finite subgroup, then $[E : E^G] = |G|$.

PROOF. From Lemma 3.70 we have $[E : E^G] \geqslant n$; therefore we need to show $[E : E^G] \leqslant n = |G|$. Let $G = \{\sigma_1 = \mathrm{id}, \ldots, \sigma_n\}$ and let $\alpha_1, \ldots, \alpha_m$, be independent over E^G, the system

$$\begin{aligned}
&\sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \ldots + \sigma_1(\alpha_m)x_m = 0\\
&\sigma_2(\alpha_1)x_1 + \sigma_2(\alpha_2)x_2 + \ldots + \sigma_2(\alpha_m)x_m = 0\\
&\ldots\\
&\sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \ldots + \sigma_n(\alpha_m)x_m = 0,
\end{aligned}$$

we claim that it has no nontrivial solution. Therefore, $n \geqslant m$ and we are done.
Assume that $x = (x_1, \ldots, x_m)$ is a nontrivial solution to $A^T x = 0$, we may assume that

- Not all $x_1, \ldots, x_m \in E^G$. Otherwise, since $\sigma_1 = \mathrm{id} \Rightarrow \sigma_1(\alpha_i) = \alpha_i$, the first row of the system gives us that $x_1\alpha_1 + \ldots + x_m\alpha_m = 0$. But $\alpha_1, \ldots, \alpha_m$ are independent over E^G.
- X has maximum number of zeros among all nontrivial solutions.

We may then arrange x as

$$x = (x_1 \notin E^G, x_2, \ldots, x_r = 1, x_{r+1} = 0, \ldots, x_m = 0),$$

in which $x_1, \ldots, x_r$ are not zero and the rest are zeros. Since $x_r = 1$, we have

$$\sigma_j(\alpha_1)x_1 + \ldots + \sigma_j(\alpha_r) = 0.$$

Since $x_1 \notin E^G$, some σ_k does not fix it, $\sigma_k(x_1) \neq x_1$, applying σ_k to above equation,

$$(\sigma_k\sigma_j)(\alpha_1)\sigma_k(x_1) + \ldots + (\sigma_k\sigma_j)(\alpha_r) = 0$$

since $\sigma_k\sigma_j$ is just another element in $\sigma_1, \ldots, \sigma_n$, we may let it be σ_i for some i. Then the equation becomes

$$\sigma_i(\alpha_1)\sigma_k(x_1) + \ldots + \sigma_i(\alpha_r) = 0.$$

Subtracting this from the ith equation of the linear system, we have

$$\sigma_i(\alpha_1)(\sigma_k(x_1) - x_1) + \ldots + \sigma_i(\alpha_{r-1})(\sigma_k(x_{r-1}) - x_{r-1}) = 0.$$

Since $(\sigma_k(x_1) - x_1) \neq 0$, we obtain a nontrivial solution with more zeros (each j corresponds to a unique i so we again get the system), contradiction. ■

Theorem 3.72 (4.33) If $G, H \leqslant \mathrm{Aut}(E)$ are two finite subgroups s.t. $E^G = E^H$, then $G = H$ (in other words, function $\gamma : H \mapsto E^H$ is injective).

PROOF. If we can prove that for $\sigma \in \mathrm{Aut}(E), G \subseteq \mathrm{Aut}(E), \sigma$ fixes $E^G \Leftrightarrow \sigma \in G$, then $\sigma \in H \Leftrightarrow \sigma$ fixes $E^H \Leftrightarrow \sigma$ fixes $E^G \Leftrightarrow \sigma \in G$. Now for the proof, we have two directions:

($\Leftarrow$) Trivial inclusion.

($\Rightarrow$) Suppose σ fixes $E^G, \sigma \notin G$. We have $E^G \subseteq E^{G\cup\{\sigma\}}$ since all of E^G are fixed by $G \cup \{\sigma\}$. On the other hand, Proposition 3.67 gives $E^G \supseteq E^{G\cup\{\sigma\}}$, therefore $E^G = E^{G\cup\{\sigma\}}$. But then $n = |G| = [E : E^G] = [E : E^{G\cup\{\sigma\}}] = |G \cup \{\sigma\}| = n + 1$ by Proposition 3.71, contradiction.

■

11/07/2008

Theorem 3.73 (4.34) Let E/k be a finite extension of fields with group $G = \mathrm{Gal}(E/k)$. The following are equivalent

(1) E/k is a splitting field for some separable $f(x) \in k[x]$.

(2) $k = E^G$.

(3) E/k is a normal extension.

PROOF. We have (1) $\Leftrightarrow$ (3) by Theorem 3.60, therefore we prove (1) $\Leftrightarrow$ (2).

((1) $\Rightarrow$ (2)). E/k is a splitting field, then by Theorem 3.41, $|G| = [E : k]$. By Proposition 3.71, $|G| = [E : E^G]$. Therefore $[E : k] = [E : E^G]$. But $k \subseteq E^G$ since k is fixed by all elements of G; $[E : k] = [E : E^G][E^G : k]$. We then have $[E^G : k] = 1$ then $k = E^G$.

((2) $\Rightarrow$ (1)). Let $\alpha \in E, \alpha \notin k$, for all $\sigma \in G$, let $\alpha_1, \ldots, \alpha_n$ be the distinct elements of $\sigma(\alpha)$. Then let $f(x) = \prod_{i=1}^{n}(x - \alpha_i) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$. Now any coefficient of $f(x)$ is invariant under any $\tau \in G$ since $f^*(x) = x^n + \tau(a_{n-1})x^{n-1} + \ldots + \tau(a_0) = \prod_{i=1}^{n}(x - \tau(\alpha_i)) = f(x)$. That is, all coefficients a_i's of $f(x)$ are in E and are fixed by G; $a_i \in E^G$ then $f(x) \in E^G[x]$. Since $E^G = k$ by assumption, $f(x) \in k[x]$. Then we have that E/k is a splitting field for $f(x)$. $f(x)$ has no repeated roots therefore any irreducible factor of $f(x)$ is separable, making $f(x)$ also separable.

■

Definition 3.74 A finite extension is a ***Galois extension*** if it is normal and separable.

Corollary 3.75 (4.36) If E/k is Galois and B is an intermediate field, then E/B is Galois.

PROOF. E/k is a splitting field of $f(x) \in k[x]$, then E/B is also a splitting field of $f(x) \in B[x]$. ■

Theorem 3.76 (4.43) Let E/k be a finite Galois extension with group $G = \mathrm{Gal}(E/k)$.

(1) The function $\gamma : H \mapsto E^H$ is an order invesring bijection between subgroups of G and intermediate fields of E/k with inverse $\sigma : B \mapsto \mathrm{Gal}(E/B)$.

(2) Let B be an intermediate field, then B/k is Galois if and only if $H = \mathrm{Gal}(E/B) \lhd G$.

PROOF.

(1) γ is injective by Theorem 3.72. We prove surjectiveness by showing that every intermediate field B is of form $B = E^H$ for some subgroup $H \leqslant G$. For the tower $k - B - E$, let $H = \mathrm{Gal}(E/B)$, E is a splitting field of some $f(x) \in k[x] \subseteq B[x]$; then Theorem 3.73(2) gives us that $B = E^H$.

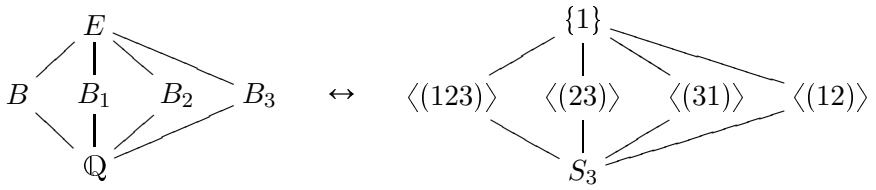
(2) ($\Rightarrow$) B/k Galois then is a splitting field extension. Then $\mathrm{Gal}(E/B)$ is normal in $\mathrm{Gal}(E/k)$. ($\Leftarrow$) Assume that $H \lhd G$, then $B = E^H = \{a \in E : \eta(a) = a, \forall \eta \in H\}$. For any $\sigma \in G, \eta \in H, a \in E^H$, since $H \lhd G$, $\sigma\eta'\sigma^{-1} = \eta \in H$; $\eta\sigma = \sigma\eta' \Rightarrow \eta(\sigma(a)) = \eta\sigma a\sigma^{-1}\eta^{-1} = \sigma\eta' a\eta'^{-1}\sigma^{-1} = \sigma a\sigma^{-1} = \sigma(a)$. Since η is arbitrary, $\sigma(a)$ is fixed by H, so $\sigma(a) \in B$. This gives that for any $\alpha \in B, p(x) = \mathrm{irr}(\alpha, k)$, if we denote another root of $p(x)$ as β, then some $\sigma \in G$ gives $\sigma(\alpha) = \beta$. But $\sigma(\alpha) \in B$, hence all roots of $p(x)$ is in B, making B/k a normal splitting field. B/k is then Galois.

■

11/10/2008

Example 3.77 Let $E = \mathbb{Q}(\sqrt[3]{2}, \omega), \omega^2 + \omega + 1 = 0$. Determine all subfields $B \subseteq E$.

$k = \mathbb{Q}, G = \mathrm{Gal}(E/k) \cong S_3$. This is true since G is isomorphic to a subset of S_3 since E is the splitting field of $x^3 - 2$; $[E : k] > 3$, but the largest proper subfield of S_3 is A_3 with 3 elements; hence $E \cong S_3$. $S_3 = \{(1), (12), (23), (13), (123), (132)\}$ has four subgroups, so we should have four subfields B, B_1, B_2, B_3 with the correspondence:



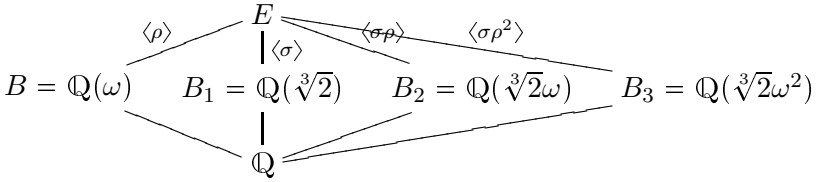
Action of $G = S_3$ on E, let $x^3 - 2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3), \alpha_1 = \sqrt[3]{2}, \alpha_2 = \omega\sqrt[3]{2}, \alpha_3 = \omega^2\sqrt[3]{2}$. Choose generators ρ and σ for $\mathrm{Gal}(E/\mathbb{Q})$ as:

$$\begin{array}{ll} \rho(\sqrt[3]{2}) = \omega\sqrt[3]{2} & \rho(\omega) = \omega \\ \sigma(\sqrt[3]{2}) = \sqrt[3]{2} & \sigma(\omega) = \omega^2 \end{array}$$

We see that G is then isomorphic to S_3 with mapping

1	ρ	ρ^2	σ	$\sigma\rho$	$\sigma\rho^2$
(1)	(123)	(132)	(23)	(13)	(12)

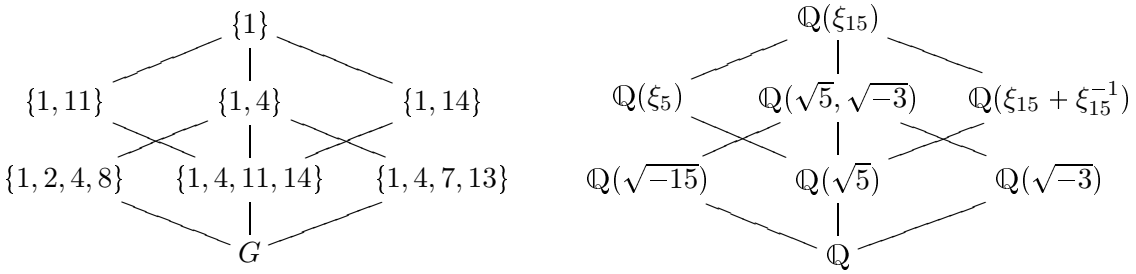
We then have



11/12/2008

Example 3.78 $\mathbb{Q}(\xi_{15})/\mathbb{Q}, \xi_{15}$ is the 15th root of unity. Find all intermediate fields.

$\mathrm{Gal}(\mathbb{Q}(\xi_{15})/\mathbb{Q}) \cong (\mathbb{Z}/15\mathbb{Z})^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$, hence $[\mathbb{Q}(\xi_{15}) : \mathbb{Q}] = 8$. We have



[see notes for additional detail]

Theorem 3.79 (4.46) Let E/k be finite extension of fields, there exists $\alpha \in E$ s.t. $E = k(\alpha)$ if and only if there are finitely many fields B s.t. $k \subseteq B \subseteq E$.

PROOF. (case k is finite). E is also finite, and E/k is generated by a generator α for the multiplicative group $E^* = \langle \alpha \rangle$.

(case k is infinite). We have two directions

($\Leftarrow$). Assume that E/k has finitely many intermediate fields. Let $k \subseteq k(\alpha_1, \alpha_2) \subseteq E$ for $\alpha_1, \alpha_2 \in E$, we show that there exits $\alpha \in E$ s.t. $k(\alpha_1, \alpha_2) = k(\alpha)$. Consider the extensions $k \subseteq k(\alpha_1 + c\alpha_2) \subseteq k(\alpha_1, \alpha_2), c \in k$. Since there are only finitely many intermediate $k(\alpha_1 + c\alpha_2)$ by assumption, there exist $c \neq c'$ s.t. $k(\alpha_1 + c\alpha_2) = k(\alpha_1 + c'\alpha_2)$, but then $k(\alpha_1 + c\alpha_2) = k(\alpha_1 + c\alpha_2, \alpha_1 + c'\alpha_2) = k(\alpha_1, \alpha_2)$.

($\Rightarrow$). Assume that $E = k(\alpha)$ for some $\alpha \in E$, if E/k is Galois, then there are finitely many intermediate fields (by Fundamental Theorem of Galois Theory), each intermediate field corresponds to a subgroup $H \subseteq \mathrm{Gal}(E/k)$.
If E/k is not Galois, then let L/k be a normal closure for E/k (such normal closure always exists when E/k is a finite extension). Then L/k has finitely many intermediate fields; hence E/k has finitely many intermediate fields.

■

Remark. There is a second proof of the ($\Rightarrow$) direction above in the note.

Theorem 3.80 (4.47) If E/k is a finite separable extension then $E = k(\alpha)$ for some $\alpha \in E$. In particular, when characteristic $k = 0$, every finite extension E/k can be written as $E = k(\alpha)$ for some $\alpha \in E$.

PROOF. Let L/k be the normal closure of E/k, if $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$, then we can take L the splitting field of $f(x) = \prod_{i=1}^{n} \mathrm{irr}(\alpha_i, k)$. Then L/k is finite Galois, hence has finitely many intermediate extensions; therefore, E/k has finitely many subextensions and by Theorem 3.79, $E = k(\alpha)$ for some $\alpha \in E$. ■

11/14/2008

Theorem 3.81 (4.50, Hilbert's Theorem 90) Let E/k be a finite Galois extension with $G = \mathrm{Gal}(E/k)$ a cyclic group of order n. Say $G = \langle \sigma \rangle$, let norm $N : E^* \to E^*$ defined by $N(u) = \prod_{\tau \in G} \tau(u)$. Then $N(u) = 1$ if and only if $u = \frac{v}{\sigma(v)}$, for some $v \in E^*$.

PROOF. Let

$$\begin{array}{ll} N : E^* \to E^* & D : E^* \to E^* \\ N(u) = \displaystyle\prod_{\tau \in G} \tau(u) & D(v) = \frac{v}{\sigma(v)} \end{array}$$

the claim is then equivalent to the statement

$$\ker N = \mathrm{im} D$$

(N and D are both homomorphisms w.r.t. multiplication)

($\Leftarrow$) Assume $u = \frac{v}{\sigma(v)} \in \mathrm{im} D$,

$$N(u) = \frac{\prod_{\tau \in G} \tau(v)}{\prod_{\tau \in G} \tau(\sigma(v))} = \frac{\prod_{\tau \in G} \tau(v)}{\prod_{\tau \in G} \tau(v)} = 1$$

($\Rightarrow$) Assume $N(u) = 1$, since $E^* = \langle\sigma\rangle$, let

$$a_0 = u, a_1 = u \cdot \sigma(u), \ldots, a_{n-1} = u \cdot \sigma(u) \ldots \sigma^{n-1}(u) = N(u) = 1, a_i \in E$$

For any $\alpha \in E$, $\sigma(a_i\sigma^i(\alpha)) = \frac{a_{i+1}}{u}\sigma^{i+1}(\alpha) = \frac{a_{i+1}\sigma^{i+1}(\alpha)}{u}$, for $i = 0, \ldots, n-1 \quad \textit{modulo} \quad n$. Let $\beta = \sum_{i=0}^{n-1} a_i\sigma^i(\alpha)$, then $\sigma(\beta) = \frac{\beta}{u}$ and $u = \frac{\beta}{\sigma(\beta)}$, provided that $\beta \neq 0$.

The automorphisms $1, \sigma, \ldots, \sigma^{n-1}$ are independent over E. Thus, $a_0 + a_1\sigma + \ldots + a_{n-1}\sigma^{n-1} \neq 0$ and there exists α, s.t. $\beta = \sum_{i=0}^{n-1} a_i\sigma^i(\alpha) \neq 0$. ■

Remark. Properties of norm $N(u)$.

(i) If $u \in E^*$, then $N(u) \in k^*$ since $N(u)$ is fixed by G: $\forall\tau \in G, \tau(N(u)) = N(u)$.

(ii) $N(uv) = N(u)N(v)$ (the multiplication in E^* is commutative since E is a field), so $N : E^* \to k^*$ is a homomorphism.

(iii) If $a \in k$, then $N(a) = a^n$, where $n = [E : k]$.

(iv) If $\sigma \in G$ and $u \in E^*$, then $N(\sigma(u)) = N(u)$.

Remark. Additional information is given on ***complex*** and ***Hilbert 90*** briefly in the notes.

Corollary 3.82 (4.51) Let E/k be a Galois extension of degree $[E : k] = p$, p a prime, s.t. k contains the pth roots of unity. Then E/k is a pure extension, $E = k(z), z^p \in k$.

PROOF. Let ω be a primitive pth root, $\omega \in k$,

$$N(\omega) = \prod_{\tau\in G} \tau(\omega) = \omega \ldots \omega = \omega^p = 1$$

here $\tau(\omega) = \omega$, since $\omega \in k, \tau \in G$ fixes ω.

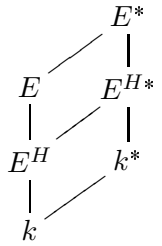
Thus (by Theorem 3.81), $\omega = \frac{z}{\sigma(z)}$ for some $z \in E$. But then, $1 = \omega^p = \frac{z^p}{(\sigma(z))^p} \Rightarrow (\sigma(z))^p = \sigma(z^p) = z^p \Rightarrow z^p \in k$.

For z above, $z \notin k$, otherwise $\sigma(z) = z \Rightarrow \omega = 1$. Lastly, $E = k(z)$ since $[E : k] = p$ prime, there are no intermediate fields in between. ■

Theorem 3.83 (4.53) Let k be a field with characteristic $k = 0$. Let E/k be Galois with $G = \mathrm{Gal}(E/k)$ a solvable group, then E can be embedded in a radical extension of k (therefore, the Galois group of a polynomial $f(x) \in k[x]$, characteristic $k = 0$ is solvable $\Leftrightarrow$ f is solvable by radicals).

PROOF. Let E/k be Galois, $G = \mathrm{Gal}(E/k)$. a solvable group. From the composition series of G, we see that there exists $H \lhd G$ of index $[G : H] = p$. Let $k^* = k(w)$ be an extension of k that contains pth roots of unity. E/E^H is Galois of degree $[E : E^H] < [E : k]$. $H = \mathrm{Gal}(E/E^H) \lhd G$ is solvable. We may use induction to get that there exists a radical extension $E^H \subseteq R_1 \subseteq \ldots \subseteq R_t$ s.t. $E \subseteq R_t$.

Consider E^H/k, if $k^* = k$, then $k \subseteq E^H$ is a pure extension of degree p by Theorem 3.82 and we are done. If not, we build a tower



Let E/k be a splitting field for some $f(x) \in k[x]$, then E^*/k is a splitting field for $f(x)(x^p - 1)$. Since p is prime, E^*/k is Galois. But then E^*/k^* is Galois with group $G^* = \mathrm{Gal}(E^*/k^*)$. Let α_i be roots of $f(x)$,

$$E^* = k^*(\alpha_1, \ldots, \alpha_n)$$
$$E = k(\alpha_1, \ldots, \alpha_n)$$

The restriction map $\rho : \mathrm{Gal}(E^*/k^*) \to \mathrm{Gal}(E/k)$ is well defined group homomorphism. ρ is injective since $\rho(\varphi) = \mathrm{id}_E \Leftrightarrow \varphi$ fixes $\alpha_1, \ldots, \alpha_n \Leftrightarrow \varphi = \mathrm{id}_{E^*}$. Thus G^* is isomorphic to a subgroup of G. In particular, G^* is solvable. As before, E^* can be embedded in a radical extension of k^*. That is, exists $k^* \subseteq T_{1*} \subseteq \ldots \subseteq T_s^*$ s.t. $E^* \subseteq T_S^*$ (thus $E \subseteq T_s^*$). Add $k \subseteq k^* = k(\omega)$ gives us a radical extension that starts at k. ■

Remark. Some isolated topics will now be covered that is in the curriculum but not that cohorent with other materials.

11/19/2008 - 11/21/2008

Remark. Quartics and resolvent polynomial were discussed. In particular, methods were given as how to tell the Galois group of an irreducible quartic. See notes for detail.

12/01/2008

Remark. Algebraic closure will now be dicussed. In particular, it will be shown that $\mathbb{C}$ is algebraically closed.

Definition 3.84 A field k is algebraically closed if every nonsonstant $f(x) \in k[x]$ has a root in k. An algebraic closure $\overline{k}$ of a field k is an algebraic extension $\overline{k}/k$ such that $\overline{k}$ is algebraically closed.

Proposition 3.85 Every polynormial $f(x) \in \mathbb{R}(x)$ of odd degree has a root in $\mathbb{R}$.

Corollary 3.86 There exists no extension $E/\mathbb{R}$ of odd degree larger than 1.

Proposition 3.87 Every polynomial $f(x) \in \mathbb{C}[x]$ of degree two has a root in $\mathbb{C}$.

Theorem 3.88 [Fundamental Theorem of Algebra] Every nonconstant $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.

12/03/2008 - 12/05/2008

Remark. We will prove that every field k has a unique (up to isomorphism) algebraic closure $\overline{k}$.

Proposition 3.89 (6.54) Let K/k be an extension of fields

(1) For $z \in K$, z is algebraic over k if and only if $k(z)/k$ is finite.

(2) For $z_1, \ldots, z_n \in K$, $z_1, \ldots, z_n$ are algebraic over $k \Leftrightarrow k(z_1, \ldots, z_n)/k$ is finite.

(3) For $y, z \in K$, K/k algebraic, $y + z, yz, y^{-1} (y \neq 0)$ are all algebraic over k.

(4) $K_{alg} = \{z \in K : z \text{ algebraic over } k\}$ is a subfield of K.

Proposition 3.90 (6.56)

(1) $k \subseteq K \subseteq E$, $E/K, K/k$ algebraic, then E/k algebraic.

(2) Let $k_0 \subseteq k_1 \subseteq \ldots k_n \subseteq \ldots$ be a tower of fields such that k_{n+1}/k_n is algebraic for all $n \geqslant 0$. Then $\widetilde{k} = \cup_{n \geqslant 0} k_n$ is a field and algebraic over k_0.

(3) Let $K = k(A)$ be obtained from k by adjoining α for all $\alpha \in A$. If all α's are algebraic over k, then K is algebraic over k.

Lemma 3.91 (6.57) Let k be a field and let $k[T]$ be the ring of polynomials in the variables $\{t : t \in T\}$. If $t_1, \ldots, t_n \in T$ are distinct and if $f_i(t_i) \in k[t_i] \subseteq k[T]$ is a nonconstant plynomial for $i = 1, \ldots, n$, then $I = (f_1(t_1), \ldots, f_n(t_n))$ is a proper ideal in $k[T]$.

Theorem 3.92 (6.58) Given a field k, there exits an algebraic closure $\overline{k}$ of k.

Lemma 3.93 (6.61) Let $\overline{k}/k$ be an algebraic closure for k and let F/k be an algebraic extension. Then there exists an embedding $f : F \to \overline{k}$.