Advanced Algebra I

Sep. 22, 2006 (Fri.)

1. Set Theory

We recall some set theory that will be frequently used in the sequel or that is not covered in the basic college course. However, we will keep this chapter as minimum as possible.

We assume the notion of "set" and some basic operation of sets without bothering their definition.

1.1. **Zorn's Lemma.**

Definition 1.1.1. *A set S is said to be* **partially ordered** *if there is a relation $\leq$ such that*

(1) *(reflexive) $x \leq x$*
(2) *(anti-symmetric) if $x \leq y$ and $y \leq x$, then $x = y$.*
(3) *(transitive) if $x \leq y$ and $y \leq z$ then $x \leq z$.*

We usually call a partially ordered set to be a POSET.

Definition 1.1.2. *A pair of elements in an POSET is said to be* **comparable** *if either $x \leq y$ or $y \leq x$. A set is said to be* **totally ordered** *(or linearly ordered) if every pair is comparable.*

We also need the following definition:

Definition 1.1.3. *A maximal element of an poset S is an element $m \in S$ such that if $m \leq x$ then $m = x$.*

Foe a given subset $T \subset S$, an upper bound of T is an element $b \in S$ such that $x \leq b$ for all $x \in T$.

One has the following

Theorem 1.1.4 (Zorn's lemma)**.** *Let S be a non-empty poset. If every non-empty totally ordered subset (usually called a "chain") has an upper bound, then there exists a maximal element in S.*

Zorn's Lemma could be taken as an axiom of set theory. It can be proved to be equivalent with the Axiom of Choice. It's also equivalent to the Well-ordering Principle. We simply give the statement of these. The reader can find the proof in most of the books on set theory.

An ordered set is said to be well-ordered if it is totally ordered and every non-empty subset B has a least element, i.e. an element $a \in B$ such that $a \leq x$ for all $x \in B$.

Theorem 1.1.5 (Well-ordered Principle)**.** *Every non-empty set can be well-ordered.*

One might wondering that $(\mathbb{Q}, \leq)$ equipped with the usual ordering is not well-ordered. So the statement says that there is another ordering which make the set $\mathbb{Q}$ well-ordered.

Example 1.1.6. *Let R be a non-zero commutative ring. One can prove that there exists a maximal ideal by using Zorn's lemma. The proof goes as following: Let $S = \{I \lhd R | I \neq R\}$ equipped with the $\subset$ as the partial ordering. $S \neq \emptyset$ because $0 \in S$. For a chain $\{I_j\}_{j \in J}$, one has a upper bound $I = \cup I_j$. Then we have a maximal element in S by Zorn's lemma. One can easily show that the maximal element corresponds to a maximal ideal.*

1.2. **cardinality.** In order to compare the "size of sets", we introduce the cardinality.

Definition 1.2.1. *Two sets A, B are said to have the same cardinality if there is a bijection between them, denoted $|A| = |B|$.*
And we say $|A| \leq |B|$ if there is a injection from A to B.

It's easy to see that the cardinality has the properties that $|A| \leq |A|$ and if $|A| \leq |B|, |B| \leq |C|$, then $|A| \leq |C|$. So It's likely that the "cardinality are partially ordered" or even totally ordered.

Lemma 1.2.2. *Given two set A, B, either $|A| \leq |B|$ or $|B| \leq |A|$.*

Sketch. Consider

$$S = \{(C, f) | C \subset A, f : C \to B \text{ is an injection}\}.$$

Apply Zorn's lemma to S, one has an maximal element (D, g), then one claim that either $D = A$ or $im(g) = B$.
We leave it as an exercise for the readers. □

Theorem 1.2.3 (Schroeder-Bernstein)**.** *If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.*

Sketch. Let $f : A \to B$ (resp. $g : B \to A$) be the given injections respectively. One needs to construct a bijection by using f and g.

Some parts of A use f and some parts not. So we consider the partition

$$A_1 := \{a \in A | a \text{ has parentless ancestor in } A\},$$
$$A_2 := \{a \in A | a \text{ has parentless ancestor in } B\},$$
$$A_3 := \{a \in A | a \text{ has infinite ancestor}\}.$$

And so does B.

Then we claim that f restricted to A_1, A_3 are bijections to B_1, B_3. And g restricted to B_2, B_3 are bijections to A_2, A_3. So the desired bijection can be constructed. □

We need some more properties of cardinality. If $|A| = |\{1, .., n\}|$, then we write $|A| = n$. And if $|A| = |\mathbb{N}|$ then we write $|A| = \aleph_0$.

Proposition 1.2.4. *If A is infinite, then $\aleph_0 \leq |A|$.*

Sketch. By Axiom of Choice. □

Definition 1.2.5.

$$|A| + |B| := |A \amalg B|,$$

$$|A| \cdot |B| := |A \times B|.$$

We have the following properties:

Proposition 1.2.6.

(1) *If $|A|$ is infinite and $|B|$ is finite, then $|A + B| = |A|$.*
(2) *If $|B| \leq |A|$ and $|A|$ is infinite, then $|A + B| = |A|$.*
(3) *If $|B| \leq |A|$ and $|A|$ is infinite, then $|A \times B| = |A|$.*

Proof. For (1), take a countable subset A_0 in A by Proposition 1.2.4. One sees that $|A_0| = |A_0| + |B|$ by shifting the index by $|B|$. Then we have

$$|A| = |A - A_0| + |A_0| = |A - A_0| + |A_0| + |B| = |A| + |B|.$$

For (2), it's enough to see that $|A + A| \leq |A|$ since clearly

$$|A| \leq |A + B| \leq |A + A|.$$

Pick an maximal subset $X \subset A$ having the property that $|X+X| \leq |X|$ by Zorn's Lemma. One claim that $A - X$ is finite, and then we are done by (1).

To see the claim, if $A - X$ is infinite, then there is a countable subset $A_0 \subset A - X$. One can construct an injective function $A \amalg X \amalg A \amalg X \to A \amalg X$ which contradicts to the maximality of X.

For (3), it suffices to show that $|A \times A| = |A|$. We sketch the proof. Let

$$S = \{(B, f) | B \text{ is an infinite subset of } A, f : B \to B \times B \text{ an bijection}\}.$$

S is non-empty because S contains an infinite countable subset. S can be equipped with natural partial ordering and by Zorn's Lemma, there exists a maximal element, say (M, g).

Let C be the complement of M in A. If $|C| \leq |M|$, then by (2), $|A| = |M|$. Hence there is a bijection $h : A \to M$. It follows that there is a bijection $A \xrightarrow{h} M \xrightarrow{G} M \times M \xrightarrow{(h^{-1}, h^{-1})} A \times A$.

Finally, if $|C| \geq |M|$, then there is a subset $M_1 \in C$ such that $|M_1| = |M|$. Let $M' = M \cup M_1$. One can construct a bijection from $M' \to M' \times M'$. This contradicts to the maximality of M. Hence we are done. □

Sep. 22, 2006 (Fri.)

2. Group Theory

The concept of groups is a very fundamental one in Mathematics. It arise as automorphism of certain sets. For example, some geometry can be described as the groups acting on the geometric objects.

In the first section, we are going to recall some definition and basic properties of groups in general. In the second section, we introduce the acting of groups. The groups action can find many applications in geometry, algebra, and the theory of groups itself. In the third section, we are would like to take care of various aspects of reducing or factoring groups into simple ones.

2.1. **Basic group theory.**

Definition 2.1.1. *A group G is a set together with a binary operation $\circ : G \times G \to G$ satisfying:*

1. *there is an $e \in G$ such that $e \circ g = g \circ e = g$ for all $g \in G$.*
2. *for all $g \in G$, there is an $g^{-1} \in G$ such that $g \circ g^{-1} = g^{-1} \circ g = e$*
3. *for all $g_1, g_2, g_3 \in G$, we have $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.*

A group is said to be **abelian** *if $x \circ y = y \circ x$ for all $x, y \in G$.*

For simplicity, we will denote xy for $x \circ y$.

A subset $H \subset G$ is a **subgroup** if H is a group by using the binary operation of G, denoted $H < G$.

A **group homomorphism** $f : G \to H$ is a function between groups that respects the structure of groups. That is, a function satisfying $f(xy) = f(x)f(y)$.
The **kernel** of f, denote $\ker(f)$, is defined to be $\{x \in G | f(x) = e_H\}$.

A subgroup $H < G$ is said to be **normal** if $gHg^{-1} = H$ for all $g \in G$, denoted $H \lhd G$. Given a subgroup $H < G$, we note G/H the set of left cosets, i.e. $G/H = \{gH | g \in G\}$. When $H \lhd G$ is normal, then G/H has induced group structure given by $xH \circ yH := xyH$. This is called the quotient group.

We remark that a subgroup is normal if and only if it is the kernel of some homomorphism. The following lemma is useful

Lemma 2.1.2. *Let $f : G \to H$ be a group homomorphism. Let N be a normal subgroup of G contained in* $\ker(f)$*, then there is an induced homomorphism $\bar{f} : G/N \to H$.*

Proof. Define $\bar{f} : G/N \to H$ by $\bar{f}(gN) = f(g)$. Then it's routine to verify it's well-defined and it's a group homomorphism. □

Regarding group homomorphisms, there are some useful facts:

Theorem 2.1.3 (First isomorphism theorem). *Let $f : G \to H$ be a group homomorphism, then there is an induced isomorphism $\bar{f} : G/\ker(f) \cong im(f)$.*
In particular, if f is surjective, then $\bar{f} : G/\ker(f) \cong H$.

Proof. Define $\bar{f} : G/\ker(f) \to H$ by $\bar{f}(g\ker(f)) = f(g)$. Then it's routine to verify it's well-defined and it's a injective group homomorphism. □

Example 2.1.4. *Let G be the set of all maps $T_{a,b} : \mathbb{R} \to \mathbb{R}$ such that $T_{a,b}(x) = ax + b$ with $a \neq 0$. Then G is a group under composition.*
There are two natural subgroups:
$A := \{T_{a,0}\} \cong \mathbb{R}^*$, the multiplication group.
$N := \{T_{1,b}\} \cong \mathbb{R}$, the translation group.
There is a group homomorphism $f : G \to \mathbb{R}^*$ by $f(T_{a,b}) = a$. Its kernel is N, which is a normal subgroup of G. So we have $G/N \cong A$.
Moreover, $G = NA = AN$ and $N \cap A = \{e\}$. So in fact G is the **semidirect product** *of A and N.*

Theorem 2.1.5 (Second isomorphism theorem). *Let H, K be subgroups of G. Then we have group isomorphism*

$$H/(H \cap K) \cong HK/K,$$

when
1. $H < N_G(K)$ or especially,
2. $K \lhd G$.

Sketch. Recall that $N_G(K) := \{x \in G | xKx^{-1} = K\}$ denotes the normalizer of K in G. It is the maximal subgroup of G in which K is normal. In particular $K \lhd N_G(K)$. So $K \lhd G$ if and only if $G = N_G(K)$.

Also one can check that if $H < N_G(K)$, then $HK = KH < N_G(K)$ is a subgroup of G. Moreover, $K \lhd HK$.

On the other hand, if $H < N_G(K)$, then $H \cap K \lhd H$. Thus both sides are groups.

Finally, we consider $f : H \to HK/K$ by $f(h) = hK$. It's easy to check that f is surjective with kernel $H \cap K$. By first isomorphism theorem, we proved (1). And (2) is just a special case of (1). □

Given a surjective homomorphism $f : G \to H$, by First isomorphism theorem, $H \cong G/N$ where $N = \ker(f)$ is a normal subgroup. It's natural to study the group structures between them. It's easy to see that there is a map

$$\{K < G/N\} \xrightarrow{f^{-1}} \{L < G | N < L\}.$$

In fact, this map is bijective. Moreover, it sends normal subgroups to normal subgroups.

Theorem 2.1.6 (Third isomorphism theorem)**.** *Given $N \lhd G$ and $K \lhd G$ containing N. Then $K/N \lhd G/N$. Moreover, $(G/N)/(K/N) \cong G/K$.*

Sketch. It's easy to check that $K/N \lhd G/N$ by definition.
In fact, we consider $f : G \to G/K$. Since $N \lhd G$ and N is contained in $\ker(F) = K$, by Lemma 2.1.2, we have an induced map $\bar{f} : G/N \to G/K$ which is clearly surjective. One checks that $\ker(\bar{g}) = K/N$ and we are done by Themreom 2.1.3. □

2.2. **cyclic groups.**
Among all groups, perhaps simplest ones are cyclic groups. Let G be a group. We say that G is cyclic if there is an element $x \in G$ such that every element $g \in G$ can be written as x^n for some $n \in \mathbb{Z}$.

It's clear that $\mathbb{Z}$ under addition is a cyclic group. By the definition, given a cyclic group G, there is a surjective map $f : \mathbb{Z} \to G$, by $n \mapsto x^n$. This is indeed a group homomorphism. Therefore, by Theorem 2.1.3, $G \cong \mathbb{Z}/\ker(f)$.

The reader should find no difficulty showing that subgroups of $\mathbb{Z}$ is either $\{0\}$ or of the form $n\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, every subgroup is normal.

Turning back to the discussion of cyclic groups. There are two cases:
1. $\ker(f) = 0$. Then $G \cong \mathbb{Z}$. This is called an infinite cyclic group.
2. $\ker(f) = n\mathbb{Z}$. Then $G \cong \mathbb{Z}/n\mathbb{Z}$. This is called a cyclic group of order n, denoted $\mathbb{Z}_n$.

There list some properties and leave the proof for the readers.

Proposition 2.2.1. *Let G be a cyclic group.*
1. Every subgroup is cyclic.
2. Homomorphic image of G is cyclic.
3. If G is a cyclic group of order n, for all $d|n$ there exist a subgroup of order d.
4. If G is a cyclic group of order n with a generator x, then the set of generators consist of $\{x^t | (t, n) = 1\}$.

Sep. 29, 2006 (Fri.)

2.3. **group action.**

Group action is one of the most fundamental concept in group theory. There are many situations that group actions appear naturally. The purpose of this section is to develop basic language of group action and apply this to the study of abstract groups.

We will first define the group action and illustrate some previous known theorem as examples.

Definition 2.3.1. *We say a group G acts on a set S, or S is a G-set, if there is function $\alpha : G \times S \to S$, usually denoted $\alpha(g,x) = gx$, compatible with group structure, i.e. satisfying:*

(1) *let $e \in G$ be the idetity, then $ex = x$ for all $x \in S$.*
(2) *$g(hx) = (gh)x$ for all $g,h \in G$, $x \in S$.*

By the definition, it's clear to see that if $y = gx$, then $x = g^{-1}y$. Because $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$.

Moreover, one can see that given a group action $\alpha : G \times S \to S$ is equivalent to have a group homomorphism $\tilde{\alpha} : G \to A(S)$, where $A(S)$ denote the group of bijections on S.

Exercise 2.3.2. *There is a bijection between $\{$group action of G on $S\}$ with $\{$group homomorphism $G \to A(S)\}$.*

Example 2.3.3 (Cayley's Theorem)**.**

Let G be a finite group of $|G| = n$. Then there is an injective homomorphism $G \to S_n$.

To see this, we consider G acts on G via the group operation, i.e. $G \times G \to G$. Thus we have a homomorphism $\varphi : G \to A(G)$.

It's clear that $A(G) = S_n$. It's easy to see that φ is injective. □

This give an example of "permutation representation". That is, represent a group into permutation groups. We gave another example:

Example 2.3.4.

Let $\mathbb{F}_2$ be the field of 2 elements. We would like to see that $GL(2,\mathbb{F}_2) \cong S_3$.

We consider V the 2 dimensional vector space over $\mathbb{F}_2$. There are 3 non-zero vector in V, denoted, $W := \{v_1 := e_1, v_2 := e_2, v_3 := e_1 + e_2\}$. It's clear that $GL(2,\mathbb{F}_2)$ acts on W. Thus we have a representation $GL(2,\mathbb{F}_2) \to A(W) \cong S_3$. One can check that this is indeed an isomorphism. □

We now introduce two important notions:

Definition 2.3.5. *Suppose G acts on S. For $x \in S$, the* **orbit** *of x is defined as*

$$\mathcal{O}_x := \{gx | g \in G\}.$$

And the **stabilizer** *of x is defined as*

$$G_x := \{g \in G | gx = x\}.$$

It's immediate to check the following:

Lemma 2.3.6. *Given a group G acting on S. For $x, y \in S$, we have:*
1. $G_x < G$.
2. either $\mathcal{O}_x = \mathcal{O}_y$ or $\mathcal{O}_x \cap \mathcal{O}_y = \emptyset$.
3. if $y = gx$, then $G_y = gG_xg^{-1}$.

Proposition 2.3.7.

$$|G| = |\mathcal{O}_x| \cdot |G_x|.$$

Sketch. For given $y \in \mathcal{O}_x$, we consider $S_y := \{g \in G | gx = y\}$. Then

$$G = \cup_{y \in \mathcal{O}_x} S_y,$$

which is a disjoint union.

Furthermore, for each $y \in \mathcal{O}_x$, we can write $y = gx$. Then one has $S_y = gG_x$. In particular $|S_y| = |G_x|$. We fix a g_y such that $y = g_yx$ once and for all. We may define a bijection $G \to \mathcal{O}_x \times G_x$ as sets by $g \mapsto (gx, g(g_{gx})^{-1})$. Thus

$$|G| = |\mathcal{O}_x| \cdot |G_x|.$$

□

Corollary 2.3.8 (Lagrange's Theorem)**.** *Let $H < G$ be a subgroup. Then $|G| = |G/H| \cdot |H|$.*

Proof. We take $S = G/H$ with the action $G \times G/H \to G/H$ via $\alpha(g, xH) = gxH$. For $H \in S$, the stabilizer is H, and the orbit is G/H. Thus we have

$$|G| = |G/H| \cdot |H|,$$

which is the Lagrange's theorem. □

Another way of counting is to consider the decomposition of S into disjoint union of orbits. Note that if $\mathcal{O}_x = \mathcal{O}_y$ if and only if $y \in \mathcal{O}_x$. Thus for convenience, we pick a representative in each orbit and let I be a set of representatives of orbits. We have a disjoint union:

$$S = \cup_{x \in I} \mathcal{O}_x.$$

In particular,

$$|S| = \sum_{x \in I} |\mathcal{O}_x|.$$

This simple minded equation actually give various nice application. We have the following natural applications.

Example 2.3.9 (translation)**.**

Let G be a group. One can consider the action $G \times G \to G$ by $\alpha(g, x) = gx$. Such action is called translation. More generally, let $H < G$ be a subgroup. Then one has translation $H \times G \to G$ by $(h, x) \mapsto hx$. In this setting, $\mathcal{O}_x = Hx$. And the set of orbits is G/H, the right cosets of H in G. Then

$$|S| = \sum_{x \in I} |\mathcal{O}_x| = |G/H| \cdot |H|$$

gives Lagrange theorem again. □

Example 2.3.10 (conjugation)**.**

Let G be a group. One can consider the action $G \times G \to G$ by $\alpha(g, x) = gxg^{-1}$. Such action is called conjugation. For a $x \in G$, $G_x = C(x)$, the centralizer of x in G. And $\mathcal{O}_x = \{gxg^{-1} | g \in G\}$ the conjugacy classes of x in G. So in general, we have

$$|G| = \sum_{\text{conj. classes}} |C|,$$

which is the **class equation**.

Now assume that G is finite. The class equation now reads:

$$|G| = \sum_{x \in I} |G|/|C(x)|,$$

where I denotes a representative of conjugacy classes.

And $\mathcal{O}_x = \{x\}$ if and only if $x \in Z(G)$, the center of G. So, for G finite, the class equation now gives

$$|G| = |Z(G)| + \sum_{x \in I, x \notin Z(G)} |G|/|C(x)|.$$

Which is the usual form of class equation. □

The class equation is very useful if the group is a finite p-group. We recall some definition

Definition 2.3.11. *If p is a prime, then a* p**-group** *is a group in which every element has order a power of p.*
By a finite p-group, we mean a group G with $|G| = p^n$ for some $n > 0$.

Consider now G is a finite p group acting on S. Let

$$S_0 := \{x \in S | gx = x, \forall g \in G\}.$$

Then the class equation can be written as

$$|S| = |S_0| + \sum_{x \in I, x \notin S_0} |\mathcal{O}_x|.$$

One has the following

Lemma 2.3.12. *Let G be a finite p-group. Keep the notation as above, then*

$$|S| \equiv |S_0| \quad (mod\, p).$$

Proof. If $x \notin S_0$, then $1 \neq |\mathcal{O}_x| = p^k$ because $|G| = |\mathcal{O}_x| \cdot |G_x|$. □

By consider the conjugation $G \times G \to G$, one sees that

Corollary 2.3.13. *If G is a finite p-group, then G has non-trivial center.*

By using the similar technique, one can also prove the important Cauchy's theorem

Theorem 2.3.14 (Cauchy)**.** *Let G be a finite group such that $p \mid |G|$. Then there is an element in G of order p.*

sketch. We keep the notation as in Lemma 2.3.12. Let

$$S := \{(a_1, ..., a_p) | a_i \in G, \prod a_i = e\}.$$

And consider a group action $\mathbb{Z}_p \times S \to S$ by $(1, (a_1, .., a_p)) \mapsto (a_p, a_1, ..., a_{p-1})$. One claims that $S_0 = \{(a, a, ..., a) | a \in G, a^p = e\}$.

By the Lemma, one has $|S| \equiv |S_0| \pmod p$. It follows that $p \mid |S_0|$. In particular, $|S_0| > 1$, hence there is $(a, ..., a) \in S_0$ with $a \neq e$. One sees that $o(a) = p$. □

Corollary 2.3.15. *A finite group G is a p-group if and only it is a finite p-group.*

2.4. **Sylow's theorems.** We are now ready to prove Sylow theorems. The first theorem regards the existence of p-subgroups in a given group. The second theorem deals with relation between p-subgroups. In particular, all Sylow p-subgroups are conjugate. The third theorem counts the number of Sylow p-subgroups.

Theorem 2.4.1 (First Sylow theorem)**.** *Let G be a finite group of order $p^n m$ (where $(p, m) = 1$). Then there are subgroups of order p^i for all $0 \leq i \leq n$.*

Furthermore, for each subgroup H_i of order p^i, there is a subgroup H_{i+1} of order p^{i+1} such that $H_i \lhd H_{i+1}$ for $0 \leq i \leq n-1$.

In particular, there exists a subgroup of order p^n, which is maximal possible, called Sylow p-subgroup. We recall the useful lemma which will be used frequently.

Lemma 2.4.2. *Let G be a finite p-group. Then*

$$|S| \equiv |S_0| \quad (mod\, p).$$

proof of the theorem. We will find subgroup of order p^i inductively. By Cauchy's theorem, there is a subgroup of order p. Suppose that H is a subgroup of order p^i. Consider the group action that H acts on

$S = G/H$ by translation, i.e. $H \times G/H \to G/H$ by $h(xH) := hxH$. One shows that $xH \in S_0$ if and only if $xH = hxH$ for all $h \in H$ if and only if $x \in N_G(H)$. Thus $|S_0| = |N_G(H)/H|$.

If $i < n$, then

$$|S_0| \cong |S| = p^{n-i}m \equiv 0 \pmod{p}.$$

By Cauchy's theorem, the group $N_G(H)/H$ contains a subgroup of order p. The subgroup is of the form H_1/H, hence $|H_1| = p^{i+1}$. Moreover, $H \lhd H_1$. □

Example 2.4.3. *If G is a finite p-group of order p^n, then one has a series of subgroups $\{e\} = H_0 < H_1 < ... < H_n = G$ such that $|H_i| = p^i$ and $H_i \lhd H_{i+1}, H_{i+1}/H_i \cong \mathbb{Z}_p$. In particular, G is solvable.*

Definition 2.4.4. *A subgroup P of G is a Sylow p-subgroup if P is a maximal p-subgroup of G.*

If G is finite of order $p^n m$ then a subgroup P is a Sylow p-subgroup if and only if $|P| = p^n$ by the proof of the first theorem.

Theorem 2.4.5 (Second Sylow theorem)**.** *Let G be a finite group of order $p^n m$. If H is a p-subgroup of G, and P is any Sylow p-subgroup of G, then there exists $x \in G$ such that $xHx^{-1} < P$.*

Proof. Let $S = G/P$ be the set of left cosets and H acts on S by translation. Thus by Lemma 2.3.12, one has $|S_0| \equiv |S| = m(\text{mod } p)$. Therefore, $S_0 \neq \emptyset$. One has

$$xP \in S_0 \Leftrightarrow hxP = xP \quad \forall h \in H \Leftrightarrow x^{-1}Hx < P.$$

This completes the proof. □

An immedaitely but important consequence is that any two Sylow p-subgroups are conjugate.

Theorem 2.4.6 (Third Sylow theorem)**.** *Let G be a finite group of order $p^n m$. The number of Sylow p-subgroups divides $|G|$ and is of the form $kp + 1$.*

Proof. Let S be the conjugate class of a Sylow p-subgroup P (this is the same as the set of all Sylow p-subgroups). We consider the action that G acts on S by conjugation, then the action is transitive, i.e. for any $x, y \in S$, there exists $g \in G$ such that $y = gx$. In particular $\mathcal{O}_x = S$. Hence $|S| \mid |G|$ for $|G| = |G_x| \cdot |\mathcal{O}_x|$.

Furthermore, we consider the action $P \times S \to S$ by conjugation. Then

$$Q \in S_0 \Leftrightarrow xQx^{-1} = Q \quad \forall x \in P \Leftrightarrow P < N_G(Q).$$

Both P, Q are Sylow p-subgroup of $N_G(Q)$ and therefore conjugate in $N_G(Q)$. However, $Q \lhd N_G(Q)$, Q has no conjugate other than itself. Thus one concludes that $P = Q$. In particular, $S_0 = \{P\}$. By Lemma 2.3.12, one has $|S| = 1 + kp$. □

Example 2.4.7.

Group of order 200 must have normal Sylow subgroups. Hence it's not simple. To see this, let $r_p :=$ number of Sylow p-subgroups. Then $r_5 = 1$. So if P is a Sylow 5-subgroup. Since gPg^{-1} is also a Sylow subgroup, it follows that $gPg^{-1} = P$ for all $g \in G$. Thus $P \lhd G$. □

Example 2.4.8.

There is no simple group of order 36. To see this, we consider P a Sylow 3-subgroup. Then $r_3 = 1$ or 4. In case that $r_3 = 4$, let S be the set of Sylow 3-subgroups. We have a group action $G \times S \to S$ by conjugation. Thus we have a group homomorphism $\varphi : G \to A(S) \cong S_4$. Comparing the cardinality of groups, one sees that φ must have non-trivial kernel. Hence G is not simple. □

2.5. **groups of small order.** We can use the technique developed in the previous sections to study group of small order in more detail.

First of all, as a direct consequence of Cauchy's theorem,

Proposition 2.5.1. *Let p be a prime. A group of order p is cyclic.*

Example 2.5.2.

Classify groups of order $2p$.

If $p = 2$, then this is well-known. So we may assume that $p > 2$. First of all there is a subgroup $H < G$ of order p, generated by x, by Cauchy's theorem. By Sylow's third theorem, we have $r_p = 1$, hence H is normal. Similarly, there is an element of order 2, say y. By normality of H, we have $yxy^{-1} = x^k$ for some k. Since

$$x = y^2xy^{-2} = yx^ky^{-1} = x^{k^2},$$

it follows that $k^2 \equiv 1(\mod p)$. Hence $k \equiv 1$ or $\equiv -1$.

Case 1. $k \equiv 1$, then $xy = yx$. It follows that G is abelian. By chinese Remainder Theorem, G is cyclic.

Case 2. $k \equiv -1$, then $xy = yx^{-1}$. These kind of group is called **dihedral groups**, denoted D_{2p}. □

Example 2.5.3.

Let p, q be primes. If $|G| = pq$, then its structure can be determined similarly.

We assume that $p > q$. Then there are $x, y \in G$ of order p, q respectively. Moreover, $H :=< x > \lhd G$. We have $yxy^{-1} = x^k$ for some k. Since

$$x = y^qxy^{-q} = yx^ky^{-1} = x^{k^q},$$

it follows that $k^q \equiv 1(\mod p)$. Now the situation depends on the structure of $\mathbb{Z}_p^*$. Recall that $\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$ is cyclic.

Case 1. $q \nmid p-1$, then $k^q \equiv 1(\mod p)$ implies that $k \equiv 1$. Hence $xy = yx$. It follows that G is abelian. By chinese Remainder Theorem,

G is cyclic.
Case 2. $q \mid p-1$, then $k^q \equiv 1(\mod p)$ has q solutions, $k \equiv a, a^2, ..., a^{q-1}, a^q \equiv 1$. If we pick $k \equiv a$, then we determined a group G_1 which is generated by x_1, y_1 with $y_1 x_1 y_1^{-1} = x_1^a$. If we pick $k \equiv a^2$, then we determined a group G_2 which is generated by x_2, y_2 with $y_2 x_2 y_2^{-1} = x_2^{a^2}$. Note that the map $\varphi : G_2 \to G_1$ by $\varphi(y_2) = y_1^2, \varphi(x_2) = x_1$ gives an isomorphism. Therefore, for different solution $k \equiv a, a^2, ..., a^{q-1}$, they determined the same group. □

There is a useful construction to produce groups from simple ones called **semi-direct product** which we now introduce. Given two groups G, H and a homomorphism $\theta : H \longrightarrow \mathrm{Aut}(G)$. Let $G \times_\theta H$ be the set $G \times H$ with the binary operation $(g, h)(g', h') = (g(\theta(h)(g')), hh')$. One can verify that this produce a group.

For example, in the case 2 of above example, we have $G = \mathbb{Z}_p, H = \mathbb{Z}_q$ and we consider $\theta : \mathbb{Z}_q \longrightarrow \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^*$ by $\theta(1) = a$. Then we obtained $\mathbb{Z}_p \times_\theta \mathbb{Z}_q$. Such group is called a **metacyclic groups**.

Proposition 2.5.4. *Let p be a primes. If $|G| = p^2$, then G is abelian.*

We will discuss the structure of finite ableina groups later. In principle, their structure are pretty easy.

sketch. By class equation, one sees that $Z(G)$ is non-trivial.
Case 1. if $|Z(G)| = p^2$, then G is abelian.
Case 2. if $|Z(G)| = p$, then $G/Z(G)$ is a group of order p , hence cyclic. We pick $x \in G$ such that $G/Z(G)$ is generated by $xZ(G)$. We also pick $y \in G$ such that $Z(G)$ is generated by y. It's easy to check that G is generated by x, y. Note that $xy = yx$, it follows that G is abelian. □

Using above properties, one can classified groups of order ≤ 15 completely unless for order 8 and 12. In fact groups of order 8 are either abelian or D_8 or Q_8. Where Q_8 is the quaterion group defined by $\{i, j, k, -i, -j, -k, 1, -1 | i^2 = j^2 = k^2 = -1, ijk = -1\}$.

Easy example of non-abelian groups of order 12 includes A_4, D_{12}. In fact there is one more, $T =< a, b | a^6 = b^4 = 1, b^2 = a^3 = (ab)^2 >$.

Theorem 2.5.5. *every non-abelian group G of order 12 is isomorphic to A_4, D_{12} or T.*

sketch. Let P be a Sylow 3-subgroup. We first consider the action $G \times G/P \to G/P$ by translation. It gives rise to a homomorphism $\varphi : G \to A(G/P) \cong S_4$. It's clear that $\ker(\varphi) < P$.
Case 1. $\ker(\varphi) = \{e\}$, then $G \cong A_4$.
Case 2. $\ker(\varphi) = P$. Then we need to wok harder. So now, $P \lhd G$ and P is the unique Sylow 3-subgroup. Let $P = \{x, x^2, x^3 = e\}$, then x, x^2 are the only element in G of order 3.

Let K be a Sylow 2-subgroup, then K is either V_4 or $\mathbb{Z}_4$.
Case 2.i. If $K \cong V_4$, by computing the relation between generators,

one can show that $G \cong D_{12}$.
Case 2.ii. If $K \cong \mathbb{Z}_4$, by computing the relation between generators, one can show that $G \cong T$.

□

Groups of order p^n, $n \geq 3$ could be very complicated. Here just give two more examples.

Example 2.5.6.

Let $G < GL(2, \mathbb{C})$ be the group generated by $A = \begin{pmatrix} 0 & \omega \\ \omega & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, where ω is a primitive 2^{n-1}th root of unity for $n \geq 3$. Then G is a group of order 2^n. □

Example 2.5.7.

Let $G < GL(3, \mathbb{C})$ be the group generated by $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, where ω is a primitive 3th root of unity. Then G is a group of order 27. □

Oct. 13, 2006 (Fri.)

2.6. **symmetry of the plane.** A map from plane itself is called a **rigid motion**, or an **isometry**, if it is distance-preserving. Let S be a subset of the plane. Then the subgroups of rigid motions preserving S is called the **symmetry of** S. It's well-known that:

Example 2.6.1.

Let S be the regular n-gon centered at the origin. Then the symmetry of S id the group D_{2n}. □

In order to build this is a more solid foundation, we need to work a little bit more.

A list of rigid motions consists of:
1. Orientation-preserving motions:
a. Translation.
b. Rotation.
2. Orientation-reversing motions:
a. Reflection.
b. Glide reflection, i.e. reflecting about a line l and then translating by a non-zero vector a parallel to l.

Theorem 2.6.2. *The above list is complete.*

Sketch. We first fix some notations:
t_a: translation by a vector a.
ρ_θ: rotation by an angle θ about the origin.
r: reflection about the x-axis.

Step 1. Orientation preserving motions that fix the origin are $\{\rho_\theta\}$.
Step 2. Let m ne an orientation preserving motion. If $m(o) = a$, then $t_{-a}m = \rho_\theta$ for some θ. by Step 1. Thus $m = t_a\rho_\theta$.
Step 3. If m is not a translation, i.e. $\theta \neq 0$, then m is a rotation about a point p. To see this, first show that m has a fixed point, denoted p, if $\theta \neq 0$. A point on the plane can be written as $p + x$,

$$m(p+x) = t_a\rho_\theta(p+x) = \rho_\theta(p+x)+a = \rho_\theta(p)+\rho_\theta(x)+a = p+\rho_\theta(x).$$

Step 4. Orientation reversing motions that fix the origin are $\{\rho_\theta r\}$. For given such m, it's clear that rm preserves the orientation and fixes the origin. So $rm = \rho_\theta$ for some θ. Thus $m = r\rho_\theta = \rho_{-\theta}r$. Also note that $\rho_\theta r$ is the reflection about l, denoted r_l, which is the line obtained by rotating x-axis by $\frac{1}{2}\theta$.
Step 5. Let m be an orientation reversing motion. Then $m(o) = a$ for some a. Thus $t_{-a}m$ is an orientation reversing motion that fixes origin, hence $t_{-a}m = r_l$. Therefore, $m = t_a r_l$ which is a glide reflection. □

Indeed, let $O(2,\mathbb{R})$ be the subgroup of motions that fix the origin. Then $O(2,\mathbb{R})$ is generated by $\{\rho_\theta, r\}$. Let M be the groups of plane rigid motions, then there is a group action $M \times \mathbb{R}^2 \to \mathbb{R}^2$. The orbit of o is the whole $\mathbb{R}^2$ and the stabilizer of o is $O(2, \mathbb{R})$.

For readers who want to know more about symmetry, we refer [Artin], Chapter 5.

2.7. **abelian groups.** In this section, we are going to study a simple but important category of groups, the abelian groups.

Given an abelian group G, we usually use $+$ to denote the operation. We say that G can be generated by $X \subset G$, denoted $G =< X >$, if every element of G can be written as $\sum n_i x_i$ for some $n_i \in \mathbb{Z}$ and $x_i \in X$. Note that $n_i \neq 0$ for all but finitely many i.

A **basis** of an abelian group G is a *linearly independent* generating subset X. That is for distinct $x_1, ..., x_k \in X$, $\sum n_i x_i = 0$ implies that n_i for all i.

An abelian group with a basis is called a **free abelian group**. And the rank, denoted $rk(F)$, is $|X|$.

It's easy to prove that an abelian group is free if and only if it's a direct sum of $\mathbb{Z}$.

On the other hand, given a set X, we can always construct a free abelian group on the set X by consider the set

$$F := \{\sum n_x x | x \in X, n_x \in \mathbb{Z}, n_x = 0 \text{ for all but finitely many } x\}.$$

The group operation on F is nothing but $\sum n_x x + \sum m_x x := \sum (n_x + m_x)x$. It's clear that X is a basis of F in this construction.

Example 2.7.1.

This construction appeared, for example, in algebraic topology. The groups of 1-chains is the free abelian group on the set of simplicial 1-chains. □

Example 2.7.2.

Let X be a Riemann surface, then the group of divisors, $Div(X)$, is the free abelian group on the set X. □

It has the following universal property:

Proposition 2.7.3. *Let F be a free abelian group with basis X. For any function $f : X \to G$ to an abelian group G. There exist a unique homomorphism $\varphi : F \to G$ extending f.*

Proof. Let $\varphi(\sum n_x x) = \sum n_x f(x)$, then verify it. □

Corollary 2.7.4. *Every abelian group is a quotient of a free abelian group.*

Proof. Let$G$ be an abelian group. Let F be the free abelian group on the set G. Consider $f : G \to G$ the identity map. Then we are done. □

Example 2.7.5.

$\mathbb{Q}$ can be describe as following. Let $X = \{x_1, ..., x_n, ...\}$ and F the free abelian group on the set X. Take $f : X \to \mathbb{Q}$ by $f(x_i) = \frac{1}{i}$. Then $\mathbb{Q}$ is a quotient of F. □

We are now ready to state develop to main theorem of this section. We need the following:

Lemma 2.7.6. *If $\{x_1, ..., x_n\}$ is a basis of F, then $\{x_1, ..., x_{j-1}, x_j + ax_i, x_{j+1}, ..., x_n\}$ is also a basis of F for $i \neq j$ and $a \in \mathbb{Z}$.*

Theorem 2.7.7. *Let F be a free abelian group of rank n and G is a non-zero subgroup of F, then there exists a basis $\{x_1, ..., x_n\}$ of F, an integer r $(1 \leq r \leq n)$ and positive integer $d_1, ..., d_r$ such that $d_1|d_2|...|d_r$ and G is free abelian group with basis $\{d_1x_1, ..., d_rx_r\}$.*

Sketch. If $n = 1$, this is easy.

By induction, we assume that the theorem is true for all abelian groups of rank $\leq n - 1$. Let

$$S := \{s \in \mathbb{Z} | sy_1 + ...k_ny_n \in G, \text{ for some basis of } F\ , y_1, ..., y_n\}.$$

Let d_1 be the smallest positive integer in S. By changing basis, we may have $\{x_1, y_2, ..., y_n\}$ basis of F and $d_1x_1 \in G$.

Let $H =< y_2, ..., y_n >$. It's clear that $F = H \oplus \mathbb{Z}x_1$. We claim that $G = (H \cap G) \oplus \mathbb{Z}d_1x_1$.

Apply induction hypothesis to $G \cap H < H$, then we are done. □

Corollary 2.7.8 (fundamental theorem of finitely generated abelian groups)**.** *Let G be a finitely generated abelian group. Then there exist an integer r and positive integers $d_1|d_2|...|d_t$ such that*

$$G \cong \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_t} \oplus \mathbb{Z}^r.$$

Proof. Let X be a finite generating set of G. And let F be the free abelian group on the set X. Then there is a surjective homomorphism $F \to G$. Apply Theorem 2.7.7 to ker $< F$. □

Now we restrict ourselves to finite abelian groups. Let G be a finite abelian group, by Corollary 2.7.8,

$$G \cong \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_t}.$$

These $d_1, ..., d_t$ are called **invariant factors**. We consider the factorization of d_i into prime factors, then we have for all i,

$$d_i = p_1^{a_{i,1}}...p_k^{a_{i,k}}.$$

By Chinese Remainder Theorem, we have for all i,

$$\mathbb{Z}_{d_i} \cong \mathbb{Z}_{p_1^{a_{i,1}}} \oplus ... \oplus \mathbb{Z}_{p_k^{a_{i,k}}}.$$

Therefore,

$$G \cong \oplus_{j=1}^k (\oplus_{i=1}^t \mathbb{Z}_{p_j^{a_{i,j}}}).$$

It's clear that $\oplus_{i=1}^{t}\mathbb{Z}_{p_j^{a_{i,j}}}$ is the Sylow p_j-subgroup. And these $p_j^{a_{i,j}}$ are called **elementary divisors**.

Example 2.7.9.

Let $G = \mathbb{Z}_{100} \oplus \mathbb{Z}_{40}$. By Chinese Remainder Theorem, $\mathbb{Z}_{100} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_{25}$ and $\mathbb{Z}_{40} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_5$. Thus

$$G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25} \cong \mathbb{Z}_{20} \oplus \mathbb{Z}_{200}.$$

So invariant factors are $20, 200$ and elementary divisors are $4, 8, 5, 25$. □

Example 2.7.10.

Let $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$. Then invariant factors are (m, n), $[m, n]$, the gcd and lcm of m, n. □

Oct. 20, 2006 (Fri.)

Let G be an abelian group, there there is a natural important homomorphism $m : G \to G$ by $m(x) := mx$ for $m \in \mathbb{N}$. The image is denoted mG and kernel is denoted $G[m]$. Let $G(p) = \{u \in G | o(u) = p^n \text{ for some } n \geq 0\}$. One can show that $G(p)$ is the Sylow p-subgroup of G. And G is a direct sum of Sylow subgroups. Thus it remains to study finite abelian p-groups. The only non-trivial part of classical theory is showing that a finite abelian p-group is a direct sum of cyclic p-groups.

We also remark that for a given finitely generated abelian group G, the rank, invariant factors, and elementary divisors are unique. To see this, we proceed as following steps:

1. if $\mathbb{Z}^n \cong \mathbb{Z}^m$, then $n = m$.

To see this, let $G \cong \mathbb{Z}^n \cong \mathbb{Z}^m$. We consider $G/2G \cong \mathbb{Z}_2^n \cong \mathbb{Z}_2^m$. Thus $n = m$.

2. let $G_{tor} := \{u \in G | mu = 0 \text{ for some } m\}$. It's clear that $G_{tor} < G$.

3. If

$$G_1 = \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_t} \oplus \mathbb{Z}^r,$$
$$\cong G_2 = \mathbb{Z}_{d'_1} \oplus ... \oplus \mathbb{Z}_{d'_{t'}} \oplus \mathbb{Z}^{r'}$$

Then clearly, $G_{1tor} \cong G_{2tor}$ and also $G_1/G_{1tor} = \mathbb{Z}^r \cong G_2/G_{2tor} = \mathbb{Z}^{r'}$. Hence in particular $r = r'$.

4. It remains to show that $t = t'$ and $d_i = d'_i$.

To see this, it's equivalent to show the uniqueness of elementary divisors of finite abelian groups. So now we assume that G is finite abelian group. Also note that if $G_1 \cong G_2$, then $G_1(p) \cong G_2(p)$. Thus we may even assume that G is a finite abelian p-group.

Suppose now that

$$G_1 := \mathbb{Z}_{p^{a_1}} \oplus ... \oplus \mathbb{Z}_{p^{a_t}}$$
$$\cong G_2 := \mathbb{Z}_{p^{b_1}} \oplus ... \oplus \mathbb{Z}_{p^{b_s}},$$

with $a_1 \leq a_2 \leq ... \leq a_t, b_1 \leq b_2 \leq ... \leq b_s$.

Then we have $pG_1 \cong pG_2$ and $G_1/pG_1 \cong G_2/pG_2$. Note that $G_1/pG_1 \cong \mathbb{Z}_p^{c_1}$, with $c_1 = \{i | a_i > 1\}$. It follows that $c_1(G_1) = c_1(G_2)$. Similarly, we can define $c_k := \{i | a_i > k\}$ and $c_k(G_1) = c_k(G_2)$.

Moreover, $G_1[p] \cong \mathbb{Z}_p^t \cong G_2[p] \cong \mathbb{Z}_p^s$. Hence $t = s$.

Since $t, c_1(G_1), c_2(G_1)...$ determine $a_1, ..., a_t$ uniquely and $s, c_1(G_2), c_2(G_2)...$ determine $b_1, ..., b_s$ uniquely. It follows that $t = s$ and $a_i = b_i$ for all i.

2.8. **Nilpotent groups, solvable groups.** Given a group G, if G has a normal subgroup N, then we have a quotient group G/N. One can expect that knowing N and G/N would give some information on G. In this section, we are going to introduce the general technique of this idea.

Let G be a group. If G has no non-trivial normal subgroup, then G is said to be **simple**.

In general, there are two natural way to produce normal subgroups. The first one is the the center $Z(G)$. It is a normal subgroup of G. And we have the canonical projection $G \to G/Z(G)$. Let $C_2(G)$ be the inverse image of $Z(G/Z(G))$ in G. By the correspondence theorem, $Z(G/Z(G))$ is a normal subgroup of $G/Z(G)$ hence $C_2(G)$ is a normal subgroup of G. And then let $C_3(G)$ to be the inverse image of $Z(G/C_2(G))$. By doing this inductively, one has an ascending chain of normal subgroups

$$\{e\} < C_1(G) := Z(G) < C_2(G) < ...$$

Notice that by the construction, each $C_i(G) \lhd G$ and $C_{i+1}(G)/C_i(G)$ is abelian.

Definition 2.8.1. *G is nilpotent if $C_n(G) = G$ for some n.*

Proposition 2.8.2. *A finite p-group is nilpotent.*

Proof. We use the fact that a finite p-group has non-trivial center. Thus one has $C_i \gneqq C_{i+1}$. The group G has finite order thus the ascending chain must terminates, say at C_n. If $C_n \neq G$, then G/C_n has non-trivial center. One has $C_n \gneqq C_{n+1}$ which is impossible. Hence $C_n = G$. □

Theorem 2.8.3. *If H, K are nilpotent, so is $H \times K$.*

Proof. The key observation is that $Z(H \times K) = Z(H) \times Z(K)$. Then inductively, one proves that $C_i(H \times K) = C_i(H) \times C_i(K)$. If $C_n(H) = H, C_m(K) = K$ then $C_l(H \times K)$ for $l = max(m, n)$. □

Lemma 2.8.4. *Let G be a nilpotent group and $H \lneqq G$ be a proper subgroup. Then $H \lneqq N_G(H)$.*

Proof. Let $C_0(G) = \{e\}$. Let k be the largest index such that $C_k(G) < H$. Then $C_{k+1}(G) \not< H$. Pick $a \in C_{k+1} - H$, then for every $h \in H$, we have $C_k ha = C_k h C_k a = C_k a C_k h = C_k ah$ for $C_{k+1}/C_k = Z(G/C_k(G))$. Thus $aha^{-1} \in C_k h \subset H$ for all $h \in H$. That is $a \in N_G(H) - H$. □

Then we are ready to prove the following:

Theorem 2.8.5. *A finite group is nilpotent if and only if it's a direct product of Sylow p-subgroups.*

Proof. By the previous two results, it's clear that a direct product of Sylow p-subgroups is nilpotent.

Conversely, if G is nilpotent, then we will prove that every Sylow p-subgroup is a normal subgroup of G. By checking the decomposition criterion, one has the required decomposition.

It remains to show that if P is Sylow p-subgroup, then $P \lhd G$. To this end, it suffices to prove that $N_G(P) = G$. By applying this Claim to $N_G(P)$, then it says that $N_G(P)$ can't be a proper subgroup of G since $N_G(N_G(P)) = N_G(P)$. Thus it follows that $N_G(P) = G$. □

Example 2.8.6.

Let $G = D_{12} = \{x^i y^j | x^6 = y^2 = e, xy = yx^5\}$. One of it's Sylow 2-subgroup is $\{e, x^3, y, x^3 y\}$ isomorphic to V_4 and it's Sylow 3-subgroup is $\{e, x^2, x^4\} \cong \mathbb{Z}_3$.

However $Z(G) = \{e, x^3\}$ and $G/Z(G) \cong D_6 \cong S_3$ and $Z(S_3) = \{e\}$. Thus G is not nilpotent. And therefore, $D_{12} \ncong V_4 \times \mathbb{Z}_3$. □

We have seen that we have a series of subgroup by taking centers. Another natural construction is to take commutators.

Definition 2.8.7. *Let G be a group. The commutator of G, denoted G' is the subgroup generated by the subset $\{aba^{-1}b^{-1} | a, b \in G\}$.*

Roughly speaking, the subgroup G' measures the non-commutativity of a group. More precisely, $G' = \{e\}$, if and only G is abelian. The smaller G', the more commutative it is.

Proposition 2.8.8. *We have:*
1. $G' \lhd G$,
2. and G/G' is ableian.
3. if $N \lhd G$, then G/N is abelian if and only if $G' < N$.

Proof. 1.) for all $g \in G$, $g(aba^{-1}b^{-1})g^{-1} \in G'$, hence $gG'g < G'$. So $G' \lhd G$.
2.) $aG'bG' = abG' = ab(b^{-1}a^{-1}ba)G' = baG' = bG'aG'$.
3.) Consider $\pi : G \to G/N$. If G/N is abelian, then $\pi(aba^{-1}b^{-1}) = e$, hence $G' < N$. Conversely, if $G' < N$, we have a surjective homomorphism $G/G' \to G/N$. G/G' is abelian, hence so is it homomorphic image G/N. □

Definition 2.8.9. *We can define the the commutator inductively, i.e. $G^{(2)} := (G')'$, etc. The $G^{(i)}$ is called the i-th derived subgroup of G. It's clear that $G > G' > G^{(2)} > ....$*

A group is solvable is $G^{(n)} = \{e\}$ for some n.

Example 2.8.10.

Take $G = S_4$. The commutator is the smallest subgroup that G/G' is abelian. Since the only non-trivial normal subgroups of S_4 are V, A_4. It's clear that $G' = A_4$ (Or one can prove this by hand). Similarly, one finds that $G^{(2)} = A_4' = V$, and $G^{(3)} = \{e\}$. Hence S_4 is solvable. □

Another useful description of solvable groups is the groups with *solvable series.*

Definition 2.8.11. *A groups G has a subnormal series if there is a series of subgroups of G*

$$G = H_0 > H_1 > H_2 > ... > H_n,$$

such that $H_i \lhd H_{i-1}$ for all $1 \leq i \leq n$.

A subnormal series is a solvable series if $H_n = \{e\}$ and H_{i-1}/H_i is abelian for all $1 \leq i \leq n$.

A subnormal series is a normal series if all H_i are normal subgroups of G.

Theorem 2.8.12. *A group is solvable if and only it has a solvable series.*

Proof. It's clear that $G > G' > ...G^{(n)} = \{e\}$ is a solvable series. It suffices to prove that a group with a solvable series is solvable. Suppose now that G has a sovable series $\{e\} = H_n < ... < H_0 = G$. First observe that $G' < H_1$ since G/H_1 is abelian. We claim that $G^{(i)} < H_i$ for all i inductively. Which can be proved by the observation that the intersection of the series $\{e\} = H_n < ... < H_0 = G$ with $G^{(i)}$ gives a solvable series of $G^{(i)}$. □

Example 2.8.13.

A finite p-group has a solvable series, hence is solvable.

Moreover, a nilpotent group is solvable. To see this, let G be a nilpotent group. Then there exist a series

$$\{e\} < C_1(G) := Z(G) < C_2(G) < ... < C_n(G) = G.$$

Notice that $C_{i+1}(G)/C_i(G) = Z(G/C_i(G))$ is abelian. Therefore this is a solvable series. □

Oct. 27, 2006 (Fri.)

Proposition 2.8.14. *Let H be a subgroup of a solvable group G, then H is solvable.*

Let N be a normal subgroup of G. Then G is solvable if and only if both N and G/N are solvable.

Sketch. G has a solvable series, intersecting the series with H gives a solvable series of H.

If $N \lhd G$, then we have $\pi : G \to G/N$. Projecting the solvable series of G to G/N gives a solvable series of G/N.

Finally, if N and G/N are solvable, they have solvable series respectively. Apply π^{-1} to the solvable series of G/N gives a series from N to G. Combine this series with the serious of H gives a solvable series of G. □

Example 2.8.15.

We will prove in the coming subsection that A_5 is not solvable, hence so is S_n for $n \geq 5$. □

2.9. **normal and subnormal series.** We turning back to series a little bit more. A subnormal series is called a composition series if every quotient is a simple group.

Definition 2.9.1. *For a subnormal series, $\{e\} = H_n < ... < H_0 = G$, the factors of the series are the quotient groups H_{i-1}/H_i and the length is the number of non-trivial factors. A refinement is a series obtained by finite steps of one-step refinement which is $\{e\} = H_n < . < K < .. < H_0 = G$.*

Definition 2.9.2. *Two series are said to be equivalent if there is a one-to-one correspondence between the non-trivial factors. And the corresponding factors groups are isomorphism.*

It's clear that this defines an equivalent relation on subnormal series.

The main theorems are

Theorem 2.9.3 (Schreier)**.** *Any two subnormal (resp. normal) series of a group G have a subnormal (resp. normal) refinement that are equivalent.*

An immediate corollary is the famous Jordan-Hölder theorem.

Theorem 2.9.4 (Jordan-Hölder)**.** *Any two composition series of a group are equivalent.*

The main technique is the Zassenhaus Lemma, or sometimes called butterfly Lemma.

Lemma 2.9.5 (Zassenhaus)**.** *Let $A^* \lhd A$ and $B^* \lhd B$ be subgroups of G. Then*

(1) $A^*(A \cap B^*) \lhd A^*(A \cap B)$.
(2) $B^*(A \cap B) \lhd B^*(A \cap B)$.
(3) $A^*(A \cap B)/A^*(A \cap B^*) \cong B^*(A \cap B)/B^*(A^* \cap B)$.

Sketch. It's clear that $A \cap B^* = (A \cap B) \cap B^* \lhd A \cap B$. And similarly, $A^* \cap B \lhd A \cap B$. Let $D = (A \cap B^*)(A^* \cap B) \lhd A \cap B$. One can have a well-defined homomorphism $f : A^*(A \cap B) \to A \cap B/D$ with kernel $A^*(A \cap B^*)$. And similarly for the other homomorphism. □

proof of Schreier's theorem. Let $\{e\} = G_{n+1} < ... < G_0 = G$ and $\{e\} = H_{m+1} < ... < H_0 = G$ be two subnormal series. Let $G(i,j) := G_{i+1}(G_i \cap H_j)$ (resp. $H(i,j) := H_{j+1}(G_i \cap H_j)$). Then one has a refinement

$$G = G(0,0) > G(0,1) > ... > G(0,m) > G(1,0) > ... > G(n,m),$$

$$G = H(0,0) > H(1,0) > ... > H(n,0) > H(0,1) > ... > H(n,m).$$

By applying Zaseenhaus Lemma to $G_{i+1}, G_i, H_{j+1}, H_j$, one has

$$G(i,j)/G(i,j+1) \cong H(i,j)/H(i+1,j).$$

□

2.10. **simplicity of A_5.** An element in S_n is said to be have cycle structure $(m_1, .., m_r)$ with $m_1 \geq m_2 \geq ... \geq m_r$, $m_1 + ... + m_r = n$ if its cycle decomposition is of length $m_1, ..., m_r$ respectively. For example, $(1,2)(3,4) \in S_4$ has cycle structure $(2,2)$ and $(1,2) \in S_4$ has cycle structure $(2,1,1)$.

Remark 2.10.1. *There is a one-to-one correspondence between cycle structures of S_n and partition of the integer n.*

A key observation is that any two elements are conjugate to each other if and only if they have the same cycle structure. Let's call the set of all elements of cycle structure $(m_1, ..., m_r)$ the cycle class of $(m_1, ...m_r)$. A consequence of this fact is that a subgroup $N < S_n$ is normal if and only if N is union of cycle classes.

Let's put it another way, given a group G, we can always consider the group action $G \times G \to G$ by conjugation. The conjugate classes are the orbits. A subgroup $H < G$ is normal if and only if it is union of orbits. If $G = S_n$, then orbits are cycle classes.

Example 2.10.2. *In S_4, V is the union of class $(1,1,1,1)$ and $(2,2)$. A_4 is the union of V and the class $(3,1)$.*

The purpose of this subsection is to show that A_5 is a simple non-abelian group, hence a non-solvable group.

Theorem 2.10.3. *A_5 is a simple non-abelian group.*

Proof. One note that in S_5, possible cycle structures are $(5), (4,1)$,$(3,1,1)$,$(3,2), (2,2,1), (2,1,1,1), (1,1,1,1,1)$ with $24, 30, 20, 20, 15, 10, 1$ elements in each class. While A_5 is the union of classes of $(5), (3,1,1), (2,2,1), (1,1,1,1,1)$.

We consider the actions of conjugation $\alpha : S_5 \times A_5 \to A_5$ and its restriction $\beta : A_5 \times A_5 \to A_5$. For $\sigma \in A_5$, let $\mathcal{O}_{\alpha,\sigma}$ be the orbit of the α and $\mathcal{O}_{\beta,\sigma}$ be the orbit of the β. And let $G_{\alpha,\sigma}, G_{\beta,\sigma}$ be the stabilizer.

It's clear that $G_{\alpha,\sigma} = C_{S_5}(\sigma)$ and $G_{\beta,\sigma} = C_{A_5}(\sigma) = C_{S_5}(\sigma) \cap A_5$. Thus we have either $|G_{\beta,\sigma}| = \frac{1}{2}|G_{\alpha,\sigma}|$ or $|G_{\beta,\sigma}| = |G_{\alpha,\sigma}|$. Hence $|\mathcal{O}_{\beta,\sigma}| = |\mathcal{O}_{\alpha,\sigma}|$ or $|\mathcal{O}_{\beta,\sigma}| = \frac{1}{2}|\mathcal{O}_{\alpha,\sigma}|$.

case 1. If σ has cycle structure (5), then $|\mathcal{O}_{\alpha,\sigma}| = 24, |G_{\alpha,\sigma}| = 5$. It follows that $|G_{\beta,\sigma}| = 5$ and hence $|\mathcal{O}_{\beta,\sigma}| = 12$.

case 2. If σ has cycle structure $(3,1,1)$, then $|\mathcal{O}_{\alpha,\sigma}| = 20, |G_{\alpha,\sigma}| = 6$. However, one notice that there is an element $\tau \in C_{S_5}(\sigma) - C_{A_5}(\sigma)$ (e.g. $(45)(123) = (123)(45)$). Hence $|G_{\beta,\sigma}| \neq |G_{\alpha,\sigma}|$ and must be $\frac{1}{2}|G_{\alpha,\sigma}| = 3$. Therefore $|\mathcal{O}_{\beta,\sigma}| = 20$.

case 3. If σ has cycle structure $(2,2,1)$,then $|\mathcal{O}_{\alpha,\sigma}| = 15, |G_{\alpha,\sigma}| = 8$. It follows that $|\mathcal{O}_{\beta,\sigma}| = 15$.

Combining all this, if $H < A_5$ is a normal subgroup, then $|H| = 1 + 12r_1 + 20r_2 + 15r_3$, where r_i are integers. Moreover $|H| \mid |A_5| = 60$, which is impossible unless $|H| = 1$ or 60. □

2.11. **simple linear groups.** We have seen that A_5 is a simple group. Another important source of simple groups is via the linear groups.

We first introduce some notions. Let V be a m-dimensional vector space over a field K. Then the **general linear group** $GL(V)$ is the group of all non-singular linear transformations on V. If we choose a basis $\{e_1, ..., e_m\}$ of V, then a non-singular linear transformation can be represented as a non-singular matrix in $GL(m, K)$. If K is a field of q elements (thus unique up to isomorphism, which we will see later), then we may write $GL(m, q)$ instead.

Proposition 2.11.1. $|GL(m,q)| = (q^m - 1)(q^m - q)...(q^m - q^{m-1})$.

Proof. Let $\{e_1, ..., e_m\}$ be a basis and A a $m \times m$ matrix. A is non-singular if and only $\{Ae_1, ..., Ae_m\}$ is again a basis. Or equivalently, $\{Ae_1, ..., Ae_m\}$ is linearly independent. Ae_1 can have anything but zero, thus there are $q^m - 1$ choices. And then Ae_2 can be anything independent of Ae_1, thus there are $q^m - q$ choices. Inductively, we get the formula. □

A matrix (or linear transformation) is called **unimodular** if determinant is 1. Let $SL(V)$, (resp. $SL(m, K)$) be the subgroups of unimodular matrices. An *elementary transvection* $B_{ij}(\lambda)$ is a matrix which is 1 along diagonal, λ as its ij entry, and 0 elsewhere. A **transvection** is a matrix B such that is similar (which is conjugate in group theory) to some $B_{ij}(\lambda)$. Note that $B_{ij}(\lambda)^{-1} = B_{ij}(-\lambda)$.

Lemma 2.11.2. *If $A \in GL(m, K)$ with $\det A = \mu$, then $A = UD(\mu)$, where U is a product of elementary transvections and $D = diag(1, ..., 1, \mu)$.*

Sketch. Performing elementary row operations by multiplying elementary transvections on the left. One sees that it reaches a matrix of type $D(\mu)$.

For example, we look at first column. Assume that $a_{21} \neq 0$. Then multiply $B_{12}(a_{21}^{-1}(1 - a_{11}))$, one gets a matrix A' with $A'_{11} = 1$. Then multiply $B_{21}(-a_{21})$, the one gets a matrix A'' with $A''_{11} = 1, A''_{21} = 0$. □

Proposition 2.11.3. *We have:*
1. $GL(m, K)$ is a semi-direct product of $SL(m, K)$ by K^*.
2. $SL(m, K)$ is generated by elementary transvections.

Proof. 1. Consider $\det : GL(m, K) \to K^*$. It's clear that this is a group homomorphism with kernel $SL(m, K)$. Hence $SL(m, K) \lhd GL(m, K)$. On the other hand, $\Delta := \{D(\mu)|\mu \in K^*\} < GL(m, K)$ and $\Delta \cong K^*$. One can verify that $GL(m, K) = SL(m, K)\Delta$ by the abbove Lemma. And it's clear that $SL(m, K) \cap \Delta = \{e\}$. Thus, we are done.
2. This follows immediately from above Lemma. □

We now introduce more notations. Let $Z(m, K)$ (resp. $Z(V)$) be the center of $GL(m, K)$. Then it's easy to see that $Z(m, K)$ is nothing but scalar matrices. Let $SZ(m, K) = Z(m, K) \cap SL(m, K)$, the group of unimodular scalar matrices. One can also verify that $Z(SL(m, K)) = SZ(m, K)$.

In order to compute the cardinality of $SZ(m, K)$, we recall the following fact:

Proposition 2.11.4. *Let K be a field.*
1. $x^n = 1$ has at most n solutions in K.
2. Every finite subgroup of K^* is cyclic. In particular, if K is finite, then K^* is cyclic.

As a result, if K is a finite field of q elements, then $x^m = 1$ has exactly $(q - 1, m)$ solutions. Thus $SZ(m, q) = (q - 1, m)$.

Let $PGL(V) := GL(V)/Z(V)$ and $PSL(V) := SL(V)/SZ(V)$. Then we have

$$|PGL(m, q)| = |SL(m, q)| = (q^m - 1)(q^m - q)...(q^m - q^{m-1})/(q - 1),$$

$$|PSL(m, q)| = (q^m - 1)(q^m - q)...(q^m - q^{m-1})/d(q - 1),$$

where $d = (q - 1, m)$.

We now give some more example of finite simple groups.

Theorem 2.11.5. *The group $PSL(2, q)$ are simple if and only if $q > 3$.*

Proof. If $q = 2, 3$, then $|PSL(2, 2)| = 6, |PSL(2, 3)| = 12$. Hence they are not simple.

Assume now that $q \geq 4$. Let $N \lhd PSL(2,q)$ and $H \lhd SL(2,q)$ be its preimage. It is enough to show that if $SZ(m,q) \lneq H < SL(m,q)$, then $H = SL(m,q)$.
1. For any matrix $A \in H - SZ(m,q)$. Then its rational canonical form is either $\begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}$ or $\begin{bmatrix} 0 & -1 \\ 1 & \beta \end{bmatrix}$.
2. In either case, H contains a matrix of the form $\begin{bmatrix} \alpha & 0 \\ \beta & \alpha^{-1} \end{bmatrix}$ with $\alpha \neq \pm 1$.

To see this, it remains to consider A in the second case. We assume $A = \begin{bmatrix} 0 & -1 \\ 1 & \beta \end{bmatrix}$. Then $TAT^{-1}A^{-1} = \begin{bmatrix} \alpha^{-2} & 0 \\ \beta(\alpha^2 - 1) & \alpha^2 \end{bmatrix} \in H$ for $T = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}$. We can pick α so that $\alpha^2 \neq \pm 1$ (unless $q = 5$, this case need some extra care).
3. Let $B = B_{21}(1)$, $A = \begin{bmatrix} \alpha & 0 \\ \beta & \alpha^{-1} \end{bmatrix}$ with $\alpha \neq \pm 1$. Then H contains $BAB^{-1}A^{-1} = B_{21}(1 - \alpha^{-2})$, an elementary tranvection with $1 - \alpha^{-2} \neq 0$.
4. If H contains $B_{21}(\mu)$, then $UB_{21}(\mu)U^{-1} = B_{12}(-\mu)$ for $U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.
5. It remains to show that H contains $B_{12}(\nu)$ for all $\nu \in K$ since $SL(m,q)$ is generated by transvections.

To see this, note that

$$\begin{bmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{bmatrix} \begin{bmatrix} 1 & \mu \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{bmatrix}^{-1} = \begin{bmatrix} 1 & \mu\alpha^2 \\ 0 & 1 \end{bmatrix}.$$

Let $G = \{0\} \cup \{\mu \in K | B_{12}(\mu) \in H\}$. It's clear that G is an additive group and contains all elements of the form $\mu(\alpha^2 - \beta^2)$.

We claim that $G = K$.

If $char(K) \neq 2$, then $\nu = (\frac{1}{2}(\nu + 1))^2 - (\frac{1}{2}(\nu - 1))^2$. Thus for given $\nu \in K$, $\nu\mu^{-1} = \xi^2 - \zeta^2$. It follows that $\nu \in G$.

If $char(K) = 2$, then $|K^*|$ is a cyclic group of odd order. Thus for $\nu \in K^*$, $\nu\mu^{-1} \in K^*$ and $\nu\mu^{-1} = \zeta^2$ for some ζ. Thus, $\nu = \mu\zeta^2 \in G$. □

Example 2.11.6.

On can even show that A_n is simple for $n \geq 5$. □

Example 2.11.7.

$|PSL(2,4)| = |PSL(2,5)| = 60$. And they are simple. So In fact, we have $PSL(2,4) \cong PSL(2,5) \cong A_5$.
$|PSL(2,7)| = 168$, so it can not be A_n.
$PSL(2,9) \cong A_6$. □

We finally give some more results concerning simple groups. However, we are not going to prove these.

Theorem 2.11.8 (Jordan-Dickson)**.** *If $m \geq 3$ and V is an m-dimensional vector space over a field K, then $PSL(V)$ is simple.*

Proposition 2.11.9. *$PSL(3,4)$ and A_8 are non-isomorphic simple groups of the same order.*

Nov. 3, 2006 (Fri.)

3. FIELD THEORY

3.1. **definitions and basic properties.** A field F is a set together two binary operation $+, *$ such that $(F,+)$ is an abelian group with identity 0, $(F^* := F - \{0\}, *)$ is an abelian group with identity 1, and satisfying $a*(b+c) = a*b + a*c$.

Let E, F be fields, a homomorphism of fields is nothing but a ring homomorphism $\varphi : E \to F$. Note that $\varphi(1_E) = 1_F$

Example 3.1.1.

Let p be a prime. Then $\mathbb{Z}_p$ is a field. Let F be a field of p elements, then clearly there is an isomorphism $F \cong \mathbb{Z}_p$ (by sending $1_{\mathbb{Z}_p}$ to 1_F). Thus we usually say *the* field of p-elements and denoted $\mathbb{F}_p$. □

Give a field F, let P be its minimal (non-zero) subfield. Then we have:

Proposition 3.1.2. *P is isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$.*

Proof. Consider the additive subgroup H generated by 1_F, then H is either $\mathbb{Z}$ or $\mathbb{Z}_p$. If it's $\mathbb{Z}_p$ then this is exactly P. And if $H = \mathbb{Z}$, then one can show that $P \cong \mathbb{Q}$. □

Definition 3.1.3. *The minimal subfield if called the* **prime field** *of F. If the prime field is $\mathbb{F}_p$, then we say that F has characteristic p, denoted $\operatorname{char}(F) = p$. Otherwise, we say that F has characteristic 0, denoted $\operatorname{char}(F) = 0$.*

The most important feature for field of characteristic p is that it has a non-trivial *Frobenius map* $\varphi : F \to F, \varphi(x) \mapsto x^p$. To verify that this is an homomorphism, we need to check that $\varphi(x) + \varphi(y) = \varphi(x+y)$. Note that $px = 0$ for all $x \in F$ and thus $nx = 0$ for all n divisible by p. It follows that $C^p_i x = 0$ for all $0 < i < p$ and all $x \in F$. Hence $(x+y)^p = x^p + y^p$.

In fact, the FRobenius map is always injective for if $x^p = y^p$, then $x^p - y^p = (x-y)^p = 0$. Thus $x - y = 0$.

Example 3.1.4.

We have the following important construction of fields. Let F be a field, $F[x]$ be the polynomial ring. Let $p(x) \in F[x]$ be an irreducible polynomial. We claim that $F[x]/(p(x))$ is a field.

Recall that there is a division algorithm on $F[x]$. That is, given $f(x), g(x) \neq 0 \in F[x]$, there exist $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ with either $r(x) = 0$ or $deg(r(x)) < deg(g(x))$. (This shows that $F[x]$ is an Euclidean domain (E.D.).)

With this properties, one can show that every ideal is of the form $(f(x))$, i.e. $F[x]$ is a principal ideal domain (PID). For a given ideal

$I \lhd F[x]$, this can be achieved by pick $f(x) \in I$ of minimal degree. For any $g(x) \in I$, performing the division algorithm, one sees that $r(x) = 0$ for otherwise one gets a polynomial of even smaller degree, which is absurd.

One method is to show that $(p(x))lhdF[x]$ is a maximal ideal. Suppose we have $(p(x)) < \mathfrak{m} \lneq F[x]$. Since $\mathfrak{m} = (f(x))$, it follows that $p(x) \in (f(x))$ and thus $p(x) = f(x)g(x)$. $p(x)$ is irreducible implies that $f(x) = cp(x)$ for some $c \in F$. Anyway, $(p(x)) = (f(x))$.

Or explicitly, a non-zero element in $F[x]/(p(x))$ is of the form $\overline{f(x)}$ for some $f(x) \in F[x]$ and $f(x) \notin (p(x))$. Thus $(f(x), p(x)) = 1$. By the division algorithm, there exists $s(x), t(x)$ such that $1 = s(x)f(x) + t(x)p(x)$. Hence $\overline{f(x)s(x)} = 1$.

If $n = deg(p(x))$, then the element in the field $F[x]/(p(x))$ can be written as $\{a_0 + a_1\bar{x} + ...a_{n-1}\bar{x}^{n-1}\}$. □

Before we move on, we need the following facts.

Proposition 3.1.5. *Let $f(x) \in F[x]$ be a polynomial of degree n, then there are at most n roots in F.*

Proof. a is said to be a root of $f(x)$ if $f(a) = 0$. Note that, by division algorithm, $f(x) = q(x)(x-a) + r(x)$ with $r(x) = 0$ or $deg(r(x)) = 0$. a is a root if and only if $r(x) = 0$ if and only if $(x-a)|f(x)$. Inductively and by the unique factorization of $F[x]$. One sees that there are at most n roots. □

Proposition 3.1.6. *Let $G < F^*$ be a finite group. Then G is cyclic.*

Proof. By Corollary 2.7.8, $G \cong \mathbb{Z}_{m_1} \oplus ... \oplus \mathbb{Z}_{m_d}$. Note that, on the right hand side, $m_d x = 0$ for all x. Thus $a^{m_d} = 1$ for all $a \in G$. (On G, we use multiplicative notations, while right hand side is additive). Thus every element in G is a root of $x^{m_d} - 1$. So we have

$$|G| = m_1...m_d \leq m_d.$$

This is possible only when $d = 1$. □

3.2. **field extensions.** Let K be a subfield of F, then we say that F is an extension over K and denote it by F/K. Recall that F can be viewed as a vector space over K. We say that the extension F/K is finite of infinite according the dimension of F as a vector space over K.

Let F/K be an extension, an element $u \in F$ is said to be *algebraic* over K if there is a non-zero polynomial $f(x) \in K[x]$ such that $f(u) = 0$. In other words, the ring homomorphism

$$\varphi : K[x] \to F,$$

$$f(x) \mapsto f(u)$$

has a non-zero kernel. Let I be the kernel. Since $K[x]$ is a PID, $I = (p(x))$ for some $p(x)$. Let $K[u]$ be the image of φ, then

$$K[x]/(p(x)) \cong K[u] \subset F.$$

It's easy that $(p(x))$ is a prime ideal, that is, $p(x)$ is irreducible. We may assume that $p(x)$ has leading coefficient 1. Such $p(x)$ is called the minimal polynomial of u over K.

We say that F/K is algebraic if every element of F is algebraic over K.

Let's recall some more properties. If F/K, then we denote $[F : K]$ to be the dimension $\dim_K F$.

Proposition 3.2.1. *If E/F and F/K, then $[E : F][F : K] = [E : K]$.*

Sketch of the proof. Let $\{u_i\}_{i\in I}$ be a basis of E/F and $\{v_j\}_{j\in J}$ be a basis of F/K. Then one can prove that $\{u_i v_j\}_{(i,j)\in I\times J}$ is a basis of E/K. Hence

$$[E : K] = |I \times J| = |I| \cdot |J| = [E : F] \cdot [F : K].$$

□

Proposition 3.2.2. *Suppose that we have a tower of fields $K \subset F \subset E$. Then E is finite over K if and only if E is finite over F and F is finite over K.*

Proof. Easy corollary of the previous proposition. □

Proposition 3.2.3. *If F/K is finite, then F/K is algebraic.*

Proof. suppose that $[F : K] = n$. For any $u \neq 0 \in F$, then $\{1, u, ..., u^n\}$ is linearly dependent over K. Thus there are $a_0, ..., a_n \in K$ non all zero such that $\sum_{i=0}^n a_i u^i = 0$. It follows that u satisfies the polynomial $f(x) = \sum_{i=0}^n a_i x^i \in K[x]$. □

Let F/K be an extension, and $u \in F$. We denote by $K(u)$ the smallest subfield of F containing K and u. It's easy to see that

$$K(u) = \{\frac{f(u)}{g(u)} | f(x), g(x) \in K[x], g(u) \neq 0\}.$$

Similarly, for $S \subset F$, we denote by $K(S)$ the smallest subfield containing both K and S. If $F = K(S)$ for a finite set S, then F is said to be *finitely generated* over K.

Proposition 3.2.4. *Let F/K be an extension. Then $u \in F$ is algebraic over K if and only if $K(u) = K[u]$. And in the algebraic case, $[K[u] : K] = deg(p(x))$, where $p(x)$ is the minimal polynomial.*

Sketch of the proof. If $u \in F$ is algebraic over K, let $p(x)$ be the minimal polynomial. One sees that $g(u) \neq 0$ if and only $(g(x), p(x)) = 1$. There are $s(x), t(x)$ such that

$$1 = s(x)g(x) + t(x)p(x),$$

hence $1 = s(u)g(u)$. One has $\frac{f(u)}{g(u)} = f(u)s(u)$ and hence $K(u) \subset K[u]$.

Conversely, $\frac{1}{u} \in K(u) = K[u]$. Thus $\frac{1}{u} = f(u)$ for some $f(x) \in K[x]$. One sees that u satisfies $xf(x) - 1$. □

Proposition 3.2.5. *F/K is finite if and only if F/K is finitely generated and algebraic.*

Sketch of the proof. If F/K is finite, let $\{u_1, ..., u_n\}$ be a basis of F/K, then $F = K(u_1, ..., u_n)$ hence is finitely generated.

Conversely, suppose that $F = K(u_1, ..., u_n)$ is algebraic over K. In particular, each u_i is algebraic over K. In particular, u_1 is algebraic over K, u_2 is algebraic over $K(u_1)$, and so on. Then one has that

$$[K(u_1, ..., u_n) : K] = [K(u_1, ..., u_n) : K(u_1, ..., u_{n-1})] \cdot [K(u_1, ..., u_{n-1}) : K]$$

is finite by induction. □

Proposition 3.2.6. *Suppose that we have a tower of fields $K \subset F \subset E$. Then E is algebraic over K if and only if E is algebraic over F and F is algebraic over K.*

Sketch of the proof. We will only prove that E is algebraic over F and F is algebraic over K implies that E is algebraic over K. The remaining statement are easy.

Pick any $u \in E$. Since u is algebraic over F, let $f(x) = \sum a_i x^i$ be the minimal polynomial of u over F.

We then consider the field $F' := K(a_0, ..., a_n)$. It's clear that u satisfies a polynomial $f(x) \in F'[x]$. It follows that $u \in F'(u)$ which is finite over K. Therefore, u is algebraic over K. □

Let L/K and M/K are extensions over K and both L, M are contained in a field F. We denote by LM the smallest subfield containing both L and M. LM is called the compositum of L and M.

A useful remark is that if $L = K(S)$ for some $S \subset L$, then $LM = M(S)$.

For a certain property of field extension, denoted $\mathcal{C}$, we are interested whether $\mathcal{C}$ is preserved after extension, lifting or compositum. More precisely, we would like to know a property $\mathcal{C}$ satisfying the following conditions:

(1) (extension) Both E/F and F/K are $\mathcal{C}$ if and only if E/K is $\mathcal{C}$.
(2) (lifting/ base change) If E/K is $\mathcal{C}$, then EF/F is $\mathcal{C}$.
(3) (compositum) If both $E/K, F/K$ are $\mathcal{C}$, then EF/K is $\mathcal{C}$.

Proposition 3.2.7. *The property of being finite or algebraic satisfying the above three.*

Sketch of the proof. It's easy to that being finite and finitely generated satisfies the above three statement. Hence so does being algebraic. □

Theorem 3.2.8. *Let F be an extension over K, and E the set of all elements in F which is algebraic over K. Then E is a field.*

Proof. If $u, v \in E$, we need to show that $u + v, uv \in E$. Note that $u + v, uv \in K(u, v)$ and $K(u, v)/K$ is finitely generated and algebraic, hence finite. It follows that both $u + v, uv$ are algebraic over K. □

Example 3.2.9.

Consider $\mathbb{C}/\mathbb{Q}$. A number $u \in \mathbb{C}$ which is algebraic over $\mathbb{Q}$ is called an algebraic number. The set of all algebraic numbers, denoted $\mathcal{A}$, is a field, algebraic but not finite over $\mathbb{Q}$.

Nov. 10, 2006 (Fri.)

3.3. **irreducibility.** One of the most important construction of field extension comes from the extension of the form $K[x]/(p(x))$ with $p(x)$ an irreducible polynomial. It is therefore natural to give some criterion for irreducibility of polynomials.

Theorem 3.3.1 (Gauss' Lemma)**.** *Let D be a UFD, and K be its field of quotients. Given a polynomial $f(x) \in D[x]$. Then $f(x)$ is irreducible in $D[x]$ if and only if $f(x)$ is irreducible in $K[x]$.*

Sketch. **1.** $f(x)$ is irreducible in $K[x]$ then $f(x)$ is irreducible in $D[x]$.
2. Given an irreducible $f(x) \in D[x]$. We may assume that $f(x)$ is primitive, that is, the g.c.d of coefficient is 1. If $f(x) = g(x)h(x) \in K[x]$, by clearing the denominators, we have $af(x) = (bg(x))(ch(x))$ with $a, b, c \in K$ and $af(x), bg(x), cf(x) \in D[x]$ being primitive.

The main ingredient is:
3. In $D[x]$, if $s[x], t[x]$ are primitive, then so is $s[x]t[x]$.

To see this, suppose that $d \neq 1$ is the g.c.d of coefficient of $s[x]t[x]$. Let p be a prime factor of d. We consider the ring homomorphism $- : D[x] \to D/(p)[x]$. Then

$$0 = \overline{s[x]t[x]} = (\overline{s[x]})(\overline{t[x]}) \neq 0.$$

4. It follows that $af(x) \in D[x]$ is also primitive. Write $a = \frac{q}{p}$ with $(p, q) = 1$. It follows that $p|(qa_0, ..., qa_n) = q$, where a_i are coefficients of $f(x)$. This is the required contradiction. □

The following observation is easy but useful:

Proposition 3.3.2. *Let $f(x) \in D[x]$ be a monic polynomial, $\mathfrak{p} \lhd d$ be a prime ideal. We consider $- : D[x] \to D/\mathfrak{p}[x]$. If $\overline{f(x)}$ is irreducible in $D/\mathfrak{p}[x]$, then $f(x)$ is irreducible in $D[x]$.*

Example 3.3.3.

Given $f(x) = x^2 + 517x + 65535 \in \mathbb{Z}[x]$, we may consider $- : \mathbb{Z}[x] \to \mathbb{Z}_2[x]$. Then $\overline{f(x)} = x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$, hence irreducible in $\mathbb{Z}[x]$. By Gauss' Lemma, it's also irreducible in $\mathbb{Q}[x]$. □

We also recall

Proposition 3.3.4 (Eisenstein's criterion)**.** *Let $f(x) = a_nx^n + ... + a_0 \in \mathbb{Z}[x]$. If there is a prime p such that $p \nmid a_n, p|a_{n-1}, ..., p|a_0$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible.*

Proof. If $f(x) = g(x)h(x)$, then we consider $- : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Thus

$$\overline{a_nx^n} = \overline{f(x)} = \overline{g(x)h(x)}.$$

It follows that both $\overline{g(x)}, \overline{h(x)}$ are of the form $\alpha x^m \in \mathbb{Z}_p[x]$ with $m \geq 1$. Therefore, we may write $g(x) = b_mx^m + ... + b_0$,$f(x) = c_kx^k + ... + c_0$ with $p|b_0, p|c_0$. Then $p^2|b_0c_0 = a_0$, a contradiction. □

3.4. **algebraic closed fields and algebraic closure.** In this section, we are going to prove the existence and uniqueness of algebraic closure. As a consequence, we are able to show the existence and uniqueness of splitting fields.

To motivate the study of algebraic closure, we start with examples:

Example 3.4.1.

Consider $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ and $\mathbb{Q}[\sqrt[3]{2}\omega]/\mathbb{Q}$. There is a isomorphism $\varphi : \mathbb{Q}[\sqrt[3]{2}] \to \mathbb{Q}[\sqrt[3]{2}\omega]$ with $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\omega$, and $\varphi(a) = a$ for $a \in \mathbb{Q}$.

This follows from the natural isomorphism $\mathbb{Q}[x]/(x^3 - 2) \to \mathbb{Q}[\sqrt[3]{2}]$ and $\mathbb{Q}[x]/(x^3 - 2) \to \mathbb{Q}[\sqrt[3]{2}\omega]$. □

In general, given a extension F/K, if $u, v \in F$ are two roots of an irreducible polynomial $p(x) \in K[x]$, then $K[u] \cong K[v]$. Therefore, starting with a field K and an irreducible polynomial $p(x) \in K[x]$. It's convenient that we have a field F containing all roots of $p(x)$ in advance. Or even more, we would like to have a field containing all roots of all polynomial in $K[x]$.

Proposition 3.4.2. *Let F be a field. The following are equivalent:*

(1) *Every polynomial of $F[x]$ of degree ≥ 1 has a root in F.*
(2) *Every polynomial of $F[x]$ of degree ≥ 1 has all the roots in F.*
(3) *Every irreducible polynomial in $F[x]$ has degree ≤ 1*
(4) *If E is an algebraic extension over F, then $E = F$.*
(5) *There is a subfield $K \subset F$ such that F is algebraic over K and every polynomial in $K[x]$ splits in $F[x]$.*

Definition 3.4.3. *A field F satisfying above conditions is said to be algebraically closed.*

Sketch. (1) $\Rightarrow$ (2) by induction on degree. And hence (1) $\Leftrightarrow$ (2) are equivalent. It's easy to see that (2) $\Leftrightarrow$ (3). We now look at (3) and (4). If E is an algebraic extension. Pick $u \in E$ algebraic over F with minimal polynomial $p(x)$. By (3), $p(x)$ has degree 1, hence $[E : F] = deg(p(x)) = 1$. In particular, $E = F$. Conversely, if there is an irreducible polynomial $p(x)$ of degree > 1, then $K[x]/(p(x))$ gives an algebraic extension of degree $deg(p(x))$. This leads to a contradiction, hence (4) implies (3).

Lastly, it's clear that (3) implies (5) by picking $K = F$. We now prove that (5) $\Rightarrow$ (4). Let E be an algebraic extension over F. For any $u \in E$, u is algebraic over K as well. Let $p_F(x), p_K(x)$ be the minimal polynomial of u over F, K respectively. By viewing $p_K(x)$ as a polynomial in F, then one has $p_F(x)|p_K(x) \in F[x]$. However, $p_K(x)$ splits in $F[x]$. It follows that $p_F(x)$ has degree 1. And hence $u \in F$. Thus $E = F$. □

We can also define the notion of algebraic closure.

Proposition 3.4.4. *Let F/K be an extension. The following are equivalent.*

(1) *F/K is algebraic, and F is algebraically closed.*
(2) *F/K is algebraic, and every polynomial in $K[x]$ splits in $F[x]$.*
(3) *F is a splitting field of all polynomials of K.*

Proof. The proof is an easy consequence of the Proposition 3.4.2, we leave it to the readers. □

Definition 3.4.5. *F is said to be an algebraical closure of K if F/K satisfies the above conditions.*

Theorem 3.4.6. *Algebraic closure exists.*

The following is due to M. Artin as it appeared in [Lang, Algebra].

Proof. Let K be a field.

Step 1. There is an extension E_1 over K such that every polynomial of degree ≥ 1 has a root in E_1.

To this end, let S be the set of all polynomials of degree ≥ 1. We consider $K[S]$ to be the polynomial ring with indeterminates x_f, for $f \in S$. Consider now an ideal $I =< f(x_f) >_{f\in S}$. We claim that $I \neq K[S]$, hence $I \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. The field $K[S]/\mathfrak{m}$ gives an extension E_1 over K. Now, for every $f(x) \in K[x]$, one sees that $f(\overline{x_f}) = \overline{f(x_f)} = 0 \in E$. Hence $f(x)$ has a root $\overline{x_f}$ in E_1.

It remains to show that $I \neq K[S]$. Suppose on the contrary that $I = K[S]$, in particular, $1 \in I$. We may write

$$1 = \sum_{i=1}^{r} g(X) f_i(x_{f_i}).$$

One can construct an algebraic extension F/K such that each f_i has a root u_i in F. Substitute x_{f_i} by u_i in F, one has

$$1 = \sum_{i=1}^{r} g(X) f_i(u_i) = 0 \in F,$$

which is the required contradiction.

Step 2. Inductively, one has $K = E_0 \subset E_1 \subset E_2 ....$ Let $E = \cup E_i$, then E is a field extension over K. And E is algebraically closed.

To see this, for any polynomial $f(x) = \sum a_i x^i \in E[x]$, $a_i \in E_{j_i}$ for some j_i. One can pick J maximal among j_i so that $a_i \in E_J$ for all i. Hence $f(x) \in E_J$. By construction, $f(x)$ has a root in E_{J+1}, and inductively, $f(x)$ has all its root in E_{J+d}, where $d = deg(f(x))$. Therefore, $f(x)$ has all its root in E.

Step 3. Let $E_a := \{u \in E | u \text{ is algebraic over } K\}$. Then E_a is an algebraic closure of K.

It's an easy exercise to check that E_a is a field extension over K. We leave it to the readers. It's also clear that E_a is algebraic over K. Hence, it suffices to check that E_a is algebraically closed.

To see this, one notices that every polynomial of $K[x]$ splits in E and it follows that every root of $K[x]$ is in E_a. Therefore, one has that every polynomial of $K[x]$ splits in E_a and we are done. □

Remark 3.4.7. *An algebraically closed field must be infinite.*
Suppose that F is algebraically closed and $F = \{a_1, .., a_n \neq 0\}$. We consider $f(x) := \prod(x - a_i) + a_n$. Then $f(x)$ has no root in F, a contradiction.

We next work on the uniqueness of algebraic closure. The main ingredient is the following extension theorem.

Theorem 3.4.8 (Extension theorem)**.** *Let $\sigma : K \to L$ be an embedding to an algebraically closed field L. Let E/K be an algebraic extension. Then one can extend the embedding σ to an embedding $\bar{\sigma} : E \to L$. That is, there is an embedding $\bar{\sigma} : E \to L$ such that $\bar{\sigma}|_K = \sigma$.*

We remark that L is not necessarily an algebraic closure of K. For example, L could be something like $\overline{K(x)}$, an algebraic closure of $K(x)$.

In order to prove the uniqueness, we need the following useful Lemma.

Lemma 3.4.9. *Let E/K be an algebraic extension and $\sigma : E \to E$ be an embedding such that $\sigma|_K = \mathbf{1}_K$. Then σ is an isomorphism.*

Proof. If E/K is finite, then injective implies isomorphic in the case of finite dimensional vector space.

In general, let's pick any $u \in E$. It suffices to show that u is in the image of σ. To see this, let $p(x)$ be the minimal polynomial of u over K and $u = u_1, u_2, ..., u_r$ be the roots of $p(x)$ in E. Let $E' := K(u_1, ..., u_r)$. It's clear that for each i, $\sigma(u_i) = u_j$ for some j. Hence $\sigma|_{E'}$ gives an homomorphism from E' to E'.

Now $\sigma|_{E'} : E' \to E'$ is an injective homomorphism of finite dimensional vector space E'/K. Therefore, $\sigma|_{E'}$ is an isomorphism. In particular, u is in the image of $\sigma|_{E'}$ and therefore in the image of σ. □

Sketch of the theorem. The staring point is an extension to a simple extension. More precisely, let $u \in E$ be algebraic over K with minimal polynomial $p(x)$. Then $p^\sigma(x)$ is an irreducible polynomial in $\sigma(K)[x]$. In L, Pick any root v of $p^\sigma(x)$ in $\sigma(K)[x]$. This is possible since L is algebraically closed. One claims that there is an isomorphism (hence an embedding to L)

$$\bar{\sigma} : K(u) \to \sigma(K)(v) \subset L$$

extending σ. We leave the detail to the readers.

In order to work on the general case, we apply Zorn's Lemma to the non-empty P.O. set of fields

$$S := \{(F, \tau) | K \subset F \subset E, \tau : F \to L, \tau|_K = \sigma\}.$$

The ordering is given naturally as: $(F_1, \tau_1) \leq (F_2, \tau_2)$ if $F_1 \subset F_2$ and $\tau_1 = \tau_2|_{F_1}$.

By Zorn's Lemma, there is a maximal element, say E_m. It's easy to see that $E_m = E$. Otherwise, pick any $u \in E$, which is algebraic over K and hence over E_m. There is an extension to $E_m(u)$ as we have seen in the first paragraph. This is a contradiction to the maximality of E_m. Hence $E_m = E$. □

Lemma 3.4.10. *Let E/K be an algebraic extension and $\sigma : E \to E$ be an embedding such that $\sigma|_K = \mathbf{1}_K$. Then σ is an isomorphism.*

Proof. If E/K is finite, then injective implies isomorphic in the case of finite dimensional vector space.

In general, let's pick any $u \in E$. It suffices to show that u is in the image of σ. To see this, let $p(x)$ be the minimal polynomial of u over K and $u = u_1, u_2, ..., u_r$ be the roots of $p(x)$ in E. Let $E' := K(u_1, ..., u_r)$. It's clear that for each i, $\sigma(u_i) = u_j$ for some j. Hence $\sigma|_{E'}$ gives an homomorphism from E' to E'.

Now $\sigma|_{E'} : E' \to E'$ is an injective homomorphism of finite dimensional vector space E'/K. Therefore, $\sigma|_{E'}$ is an isomorphism. In particular, u is in the image of $\sigma|_{E'}$ and therefore in the image of σ. □

Corollary 3.4.11. *Algebraic closure of a field is unique up to isomorphism.*

Proof. Suppose that E, F are algebraic closure of K. By the extension theorem, there are embedding $\sigma : E \to F$ and $\tau : F \to E$ such that $\sigma|_K = \tau|_K = \mathbf{1}_K$.

Hence one has an embedding $\sigma \circ \tau : F \to F$, which is an isomorphism by the Lemma. Similarly, $\tau \circ \sigma$ is an isomorphism. Hence E and F are isomorphic. □

Nov. 17, 2006

3.5. **splitting fields and normal extensions.** We have seen that given a field K, there is a unique (up to isomorphism) algebraic closure, denoted $\overline{K}$. Then it is convenient for our further study of roots of polynomial. Even though we do not know the roots explicitly, we know that there are *in* its algebraic closure. This make the discussion of root of polynomials more concrete.

Let K be a field and $f(x) \in K[x]$. Let $\{u_1, ..., u_r\}$ be the roots of $f(x)$ in its algebraic closure $\overline{K}$. Then the field $K(u_1, ..., u_r)$ is called the **splitting field of** $f(x)$ **over** K. The splitting field is the smallest field that containing all roots.

Given a set of polynomial $S \subset K[x]$, we can similarly define the splitting field of S to be the field generated by all roots of polynomials in S.

In this section, we are going to prove the existence and uniqueness of splitting fields. And we introduce the notion of normal extension.

Proposition 3.5.1. *Let K be a field. And S be a set of polynomial in $K[x]$. Then*

(1) *Any two splitting field are isomorphic.*
(2) *If F_1, F_2 are two splitting fields in a fixed algebraic closure $\overline{K}$, then $F_1 = F_2$.*

Proof. Let F_1 and F_2 be two splitting fields, one has an K-embedding $\sigma : K \to \overline{F_2} = \overline{K}$. This embedding can be extended to $\tilde{\sigma} : F_1 \to \overline{F_2}$ by the extension theorem. One can prove that image of $\tilde{\sigma}$ is in F_2. Hence one has an injective homomorphism $\tilde{\sigma} : F_1 \to F_2$. Similarly there is another one $\tilde{\tau} : F_2 \to F_1$. It's easy to show that these give the isomorphism. □

Proposition 3.5.2. *Let N be an algebraic extension over K contained in $\overline{K}$. Then the following are equivalent:*

(1) *Any K-embedding $\sigma : N \to \overline{K}$ induces an K-automorphism of N.*
(2) *N is a splitting field of some $S \subset K[x]$ over K.*
(3) *Every irreducible polynomial in $K[x]$ having a root in N splits in N.*

Proof. For (1) $\Rightarrow$ (2), (3), we prove that for every $u \in N$, with minimal polynomial $p(x)$, then $v \in N$ for every root of $p(x)$. To this end, start with an isomorphism $\sigma : K(u) \to K(v)$. By extension theorem, one can extend it to an embedding $N \to \overline{K(v)} = \overline{K}$. The embedding is an automorphism by (1). Thus, $v = \sigma(u) \in N$.

(3) $\Rightarrow$ (2) is trivial.

For (2) $\Rightarrow$ (1). Suppose that N is a splitting field of S over K. Let u be a root of $f(x) \in S$. Let $\sigma : N \to \overline{K}$ be any K-embedding. It's clear that $\sigma(u)$ is a root of $f(x)$, hence $\sigma(u) \in N$. Thus $\sigma(N) \subset N$. Since σ is injective and N/K is algebraic, σ is in fact an isomorphism. □

The property of being normal is not as well-behaved as begin algebraic or finite. For example, it's not preserve after "extension"

Example 3.5.3. *If F/E and E/K are normal, then F/K is not necessarily normal. For example, take $F = \mathbb{Q}(\sqrt[4]{2}), E = \mathbb{Q}(\sqrt{2}), K = \mathbb{Q}$. It's easy to see that a degree 2 extension is always normal, however, $\mathbb{Q}(\sqrt[4]{2})$ is not normal over $\mathbb{Q}$.*

Also let's consider $K \subset E \subset F$. Then F is normal over K implies that F is normal over E. But it doesn't imply that E is normal over K. For example, take $F = \mathbb{Q}(\sqrt[4]{2}, i), E = \mathbb{Q}(\sqrt[4]{2}), K = \mathbb{Q}$

Being normal is preserved by "lifting" and "compositum"

Proposition 3.5.4. *Let E, F be extensions over K and contained in a field L. If E/K is normal then EF/F is normal. Moreover, if both $E/K, F/K$ are normal, then EF/K is normal.*

Proof. In order to show that EF is normal over F, we look at F-embedding $\sigma : EF \to \overline{F}$. Since σ is identity on F, hence on K. By the extension theorem and the proof of the previous Proposition, one can show that $\sigma_{|E}$ is an automorphism. Hence $\sigma(E) = E$. It follows that

$$\sigma(EF) = \sigma(E)F = EF.$$

Thus EF is normal over F.

Suppose now that $E/K, F/K$ are normal. Let $\sigma : EF \to \overline{K}$ be a K-embedding. We have that $\sigma_{|E}, \sigma_{|F}$ are K-embeddings. One sees that $\sigma(E) = E$ and $\sigma(F) = F$ by the normal assumption. If follows that

$$\sigma(EF) = \sigma(E)\sigma(F) = EF.$$

□

3.6. **finite dimensional Galois extension.** In this section, we are going to prove the fundamental theorem for finite dimensional Galois extension.

Let F/K be an field extension, we define the Galois group of F over K, denoted $\mathrm{Gal}_{F/K}$ or $G_{F/K}$ or $\mathrm{Aut}_K(F)$, as

$$\mathrm{Gal}_{F/K} := \{\sigma | \sigma \in \mathrm{Aut}F, \sigma_{|K} = \mathbf{1}_K\}.$$

It's clear that for $\sigma \in \mathrm{Gal}_{F/K}$ and $u \in F$ algebraic over K with minimal polynomial $p(x)$, then $\sigma(u)$ satisfies the same minimal polynomial.

On the other hand, if F/K is normal, let u, v be two elements having the same minimal polynomial $p(x)$, then we claim that there is an $\sigma \in \mathrm{Gal}_{F/K}$ such that $\sigma(u) = v$. To see this, we fix an algebraic closure $\overline{K}$ containing F. There is an K-isomorphism $\sigma_0 : K(u) \to K(v)$ which extends to an embedding $\sigma : F \to \overline{K}$. Since F is normal over K, one has $\sigma(F) \subset F$. And hence $\sigma \in \mathrm{Aut}F$.

Example 3.6.1.

Consider the field $F := \mathbb{Q}(\sqrt[3]{2}, \omega)$ which is a splitting field of $x^3 - 2$ over $\mathbb{Q}$. Thus it's normal over $\mathbb{Q}$. One can check that the Galois group $\mathrm{Gal}_{F/\mathbb{Q}}$ is generated by σ, τ that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega, \sigma(\omega) = \omega$, and $\tau(\sqrt[3]{2}) = \sqrt[3]{2}, \tau(\omega) = \omega^2$. It's easy to check that $\mathrm{Gal}_{F/\mathbb{Q}} \cong S_3$. □

Example 3.6.2.

Consider the field $F := \mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. Then it's easy to check that $\mathrm{Gal}_{F/\mathbb{Q}} = \{\mathbf{1}_F\}$. □

There is a natural correspondence between subgroups of Galois groups and intermediate fields. To be precise, fix an extension F/K. Let $H < G := \mathrm{Gal}_{F/K}$ be a subgroup. One can define

$$H' := \{u \in F | \sigma(u) = u, \forall \sigma \in H\}.$$

It's clear that this is a field. On the other hand, given and intermediate field L such that $K \subset L \subset F$, then one can define

$$L' := \{\sigma \in \mathrm{Gal}_{F/K} | \sigma(u) = u, \forall u \in L\} = \{\sigma \in \mathrm{Gal}_{F/K} | \sigma_{|L} = \mathbf{1}_L\}.$$

It's easy to check the following properties:

Proposition 3.6.3. *Let F/K be an extension with Galois group G. Let L be an intermediate field, i.e. $K \subset L \subset F$, and $H < G$ is a subgroup.*

1. *$F' = \{\mathbf{1}_F\}$, $K' = G$, and $\{\mathbf{1}_F\}' = F$.*
2. *For any L, one has $L \subset L''$, $L' = L'''$.*
3. *For any H, one has $H < H''$, $H' = H'''$.*
4. *For any intermediate fields $L \subset M$, one has $M' < L'$.*
5. *For any subgroups $J < H$, one has $H' \subset J'$.*

Proof. Most of the proof follows directly from the definition. We only sketch the proof for $L' = L'''$.

By $L \subset L''$ and (4), one has

$$(L'')' < L'.$$

On the other hand, by (5), one has

$$L' < (L')''.$$

We are done. □

Proposition 3.6.4. *There is a one-to-one correspondence between*

$$\{L | K \subset L \subset F, L'' = L\} \leftrightarrow \{H | H < G, H'' = H\}.$$

Proof. The correspondence is given by $L \mapsto L'$ (or $H \mapsto H'$).

To show the injective, one sees that if $L_1' = L_2'$, then $L_1 = L_1'' = L_2'' = L_2$.

For any H with $H'' = H$, we take $L = H'$, then $H = L'$. It suffices to check that $L'' = L$. This follows from the fact that $H''' = H'$. □

In the proposition, one might expect that $G' = K$. However, this is not always the case (see e.g. Example 3.6.2). For extension with this property, we call it *Galois*. It turns out that this naive definition is a very delicate one which leads to some nice properties.

Definition 3.6.5. *An extension F/K is said to be Galois if* $(\mathrm{Gal}_{F/K})' = K$.

Example 3.6.6.

Keep the notation as in Example 3.6.1. One can check that $G' = \mathbb{Q}$, hence a Galois extension.

In fact the group G has the following subgroups: $\{\mathbf{1}\}, < \tau >, < \tau\sigma >, < \tau\sigma^2 >, < \sigma >, G$ of order $1, 2, 2, 2, 3, 6$ respectively. Their fixed fields are $\mathbb{Q}(\sqrt[3]{2}, \omega), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2), \mathbb{Q}(\omega), \mathbb{Q}$ respectively.

Conversely, for these intermediate subfields, their fixed groups are exactly those corresponding ones. □

In general, we have the following:

Theorem 3.6.7 (Fundamental theorem of finite dimensional Galois extension)**.** *Let F/K be a finite dimensional Galois extension with Galois group G, then*

(1) *There is an one-to-one correspondence between*

$$\{L | K \subset L \subset F\} \leftrightarrow \{H | H < G\}.$$

(2) *The corresponding degree are equal. That is, if $K \subset L \subset M \subset F$, then $[M : L] = [L' : M']$. And if $J < H < G$, then $[H : J] = [J' : H']$.*

(3) *An intermediate field E is Galois over K if and only if $E' \lhd G$. And in this case, $\mathrm{Gal}_{E/K} \cong G/E'$.*

Proof. **Step 1.** $[M : L] \geq [L' : M']$.
We prove the case that $M = L(u)$ for some $u \in M$ and by induction on $[M : L]$, we are done. Suppose now that $M = L(u)$ and let $p(x)$ be the minimal polynomial of u over L. Let S be the set of roots of $p(x)$ in F. Then one has a map

$$\Phi : L' \to S,$$

$$\sigma \mapsto \sigma(u).$$

One can check that Φ induces an injective map $L'/M' \to S$. Hence one has

$$[L' : M'] = |L'/M'| \leq |S| \leq deg(p(x)) = [M : L].$$

Step 2. $[H : J] \geq [J' : H']$.
Let $n = [H : J]$. Suppose on the contrary that there are $n+1$ elements $u_1, ..., u_{n+1} \in J'$ linearly independent over H'.

We consider the equation $\sum_{i=1}^{n+1} u_i x_i = 0$ in F Consider now a set of representative of H/J, denoted $\{e = \sigma_1, ..., \sigma_n\}$. By applying σ_i to the above equation. Then one has a system of linear equations in F.

$$(*) \begin{cases} \sigma_1(u_1)x_1 + \sigma_1(u_2)x_2 + ... + \sigma_1(u_{n+1})x_{n+1} = 0 \\ \sigma_2(u_1)x_1 + \sigma_2(u_2)x_2 + ... + \sigma_2(u_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(u_1)x_1 + \sigma_n(u_2)x_2 + ... + \sigma_n(u_{n+1})x_{n+1} = 0 \end{cases}$$

Pick a solution in F with smallest number of non-zero a_i's, may assume it's $(a_1, ..., a_s, 0..., 0)$ and $a_1 = 1$.

If there is an $\tau \in H$ such that $\tau(a_2) \neq a_2$, then by applying τ to the system $(*)$, one get the same system of equations with a solution $(\tau(a_1), \tau(a_2), ..., \tau(a_s), 0, ..., 0$. Hence

$$(a_1, ..., a_s, 0..., 0) - (\tau(a_1), \tau(a_2), ..., \tau(a_s), 0, ..., 0) = (0, a_2 - \tau(a_2), ..., 0)$$

is a non-zero solution of smaller length. This is the required contradiction.

To find τ. We look at $u_1 a_1 + ... + u_s a_s = 0$. Since $\{u_1, ..., u_s\}$ is independent over H', not all a_1 is in H'. We may assume that $a_2 \notin H'$. Hence there is a $\tau \in H$ such that $\tau(a_2) \neq a_2$. We are done.

Step 3. We show that every intermediate field L, $L'' = L$. And every subgroup $H < G$, $H'' = H$.

By Step 1, one has

$$[L'' : K] = [L'' : K''] \leq [K' : L'] \leq [L : K],$$

however, one has $L \subset L''$. Thus one has $L = L''$. Similarly, one can prove that $H'' = H$ by considering $[H'' : \{\mathbf{1}_F\}]$.

Step 4. $[M : L] = [L' : M']$ and $[H : J] = [J' : H']$.

This follows from $[M : L] = [M : K]/[L : K] = [K' : M']/[K' : L'] = [L' : M']$. And the other one is similar.

Step 5. F/K is normal and separable.

Given $u \in F$, with minimal polynomial $p(x)$ over K. As in the proof of Step 1. One has $[K(u)' : K'] \leq |S| \leq deg(p(x)) = [K(u) : K]$. By Step 4, they are equalities. In particular, every root of $p(x)$ is in F and there is no multiple roots. Thus F is normal and separable over K.

Step 6. If $N \lhd G$, then N' is stable. That is, for all $\sigma \in G$, $\sigma(N') \subset N'$ (indeed $= N'$).

Since $N \lhd G$, for all $\sigma \in G$ and for all $\tau \in N$, one has $\sigma^{-1}\tau\sigma \in N$. Thus, $\sigma^{-1}\tau\sigma(N') = N'$. It follows that $\tau\sigma(N') = \sigma(N')$, for all $\tau \in N$. Hence $\sigma(N')$ is fixed by all N and thus $\sigma(N') \subset N'$.

Step 7. If E is a stable intermediate subfield. Then the restriction map $\mathrm{Gal}_{F/K} \to \mathrm{Gal}_{E/K}$ is well-defined and surjective.

Since E is stable, then $\sigma_{|E} \in \mathrm{Gal}_{E/K}$ for any $\sigma \in \mathrm{Gal}_{F/K}$. Moreover, let $\tau \in \mathrm{Gal}_{E/K}$, by the extension theorem, there is an extension $\overline{\tau} : F \to \overline{K}$. Since F is normal over K, $\overline{\tau}$ is in fact an automorphism of F.

Step 8. If an intermediate field E is stable, then E/K is Galois.

To see this, it suffices to show that for any $u \in E-K$, there is an $\sigma \in \mathrm{Gal}_{E/K}$ such that $\sigma(u) \neq u$. Fix any $F \ni v \neq u$ with the same minimal polynomial as u. There is an K-isomorphism $\sigma_0 : K(u) \to K(v)$ such that $\sigma(u) = v$. σ can be extended to an embedding $\overline{\sigma} : F \to \overline{K}$, which gives an automorphism of F. The restriction $\sigma = \overline{\sigma}_{|E}$ gives an automorphism of E that $\sigma(u) \neq u$.

Step 9. If E/K is Galois, then E is stable.

One first notices that E/K is normal. For every $\sigma \in \mathrm{Gal}_{F/K}$, σ gives an embedding $\sigma_{|E} : E \to \overline{K}$. Since E/K is normal, $\sigma_{|E}$ is an automorphism of E. And hence E is stable under the Galois group $\mathrm{Gal}_{F/K}$ action.

Step 10. If E is stable, then E' is normal.

This can be checked directly. For all $\sigma \in G$ and $\tau \in E'$ and for all $u \in E$,

$$\sigma^{-1}\tau\sigma(u) = \sigma^{-1}\tau(\sigma(u)) = \sigma^{-1}\sigma(u) = u,$$

since $\sigma(u) \in E$. Therefore, $\sigma^{-1}\tau\sigma \in E'$. □

Dec. 1, 2006

Remark 3.6.8. *Some of the result we proved still true in a more general setting. We list some here:*

1. *If F/K is an extension, and an intermediate field E is stable, then $E' \lhd \mathrm{Gal}_{F/K}$.*
2. *Let F/K be an extension. If $N \lhd \mathrm{Gal}_{F/K}$, then H' is stable.*
3. *If F/K is Galois, and E is a stable intermediate field, then E is Galois over K. (finite-dimensional assumption is unnecessary here)*
4. *An intermediate field E is algebraic and Galois over K, then E is stable.*

We conclude this section with the following theorem concerning the relation between Galois extension, normal extension and splitting fields.

Definition 3.6.9. *An irreducible polynomial $f(x) \in K[x]$ is said to be* **separable** *if its roots are all distinct in $\overline{K}$.*

Let F be an extension over K and $u \in F$ is algebraic over K. Then u is separable over K if its minimal polynomial is separable.

An extesnion F over K is separable if every element of F is separable over K.

Theorem 3.6.10. *Let F/K be an extension, then the following are equivalent*

1. *F is algebraic and Galois over K.*
2. *F is separable over K and F is a splitting field over K of a set S of polynomials.*
3. *F is a splitting field of separable polynomials in $K[X]$.*
4. *F/K is normal and separable.*

Proof. Fix $u \in F$ with minimal polynomail $p(x)$ over K. Let $\{u = u_1, ..., u_r\}$ be distinct roots of $p(x)$ in F. For any σ, then σ permutes $\{u = u_1, ..., u_r\}$. Thus $f(x) := \prod_{i=1}^{r}(x - u_i)$ is invariant under σ. Hence $f(x) \in K[x]$. It follows that $f(x) = p(x)$. This proved that $(1) \Rightarrow (2), (3), (4)$.

One notices that $(2) \Leftrightarrow (4)$. Thus it remains to show that $(2) \Rightarrow (3)$, and $(3) \Rightarrow (1)$.

For $(2) \Rightarrow (3)$, let $f(x) \in S$ and let $g(x)$ be an monic irreducible component of $f(x)$. Since $f(x)$ splits in F, it's clear that $g(x)$ is an minimal polynomial of some element in F. Moreover, since F/K is separable, $g(x)$ is separable. One sees that F is in fact a splitting field of such $g(x)$'s.

For $(3) \Rightarrow (1)$, we first note that F/K is algebraic since F is a splitting field. We shall prove that $(4) \Rightarrow (1)$. The implication $(3) \rightarrow (4)$ follows from a general fact about separable extension that an algebraic extension F/K is separable if F is generated by separable elements.

To this end, pick any $u \in F - K$, with minimal polynomial $p(x)$ of degree ≥ 2 and separable. Hence there is a different root, say v, of $p(x)$ in F. It's natural to consider the K-isomorphism $\sigma : K(u) \to K(v)$. Which can be extended to $\bar{\sigma} : F \to \overline{K}$. Since F is normal, $\bar{\sigma}$ is an automorphism of F, hence in $\mathrm{Gal}_{F/K}$ sending u to $v \neq u$. So F/K is Galois.

□

3.7. **Galois group of a polynomial.** In this section, we are going to study Galois group of a polynomial. We will define this notion in general and study polynomial of degree 3,4 in more detail.

Definition 3.7.1. *Let $f \in K[x]$ be a polynomial with splitting field F. The Galois group of $f(x)$, denoted G_f is the Galois group of F/K.*

The Galois group of a polynomial have some basic properties.

Proposition 3.7.2. *Let $f(x)$ be a polynomial of degree n, then $G_f \hookrightarrow S_n$. Thus one can viewed G_f as a subgroup of S_n.*

If $f(x)$ is irreducible and separable, then G_f is transitive and $|G_f|$ is divided by n.

Sketch of the proof. Let $\{u_1, ..., u_r\}$ be roots of $f(x)$ in F. For $\sigma \in G_f$, $\sigma(u_i) = u_j$. Hence σ gives a permutation of r elements. It follows that G_f can be viewed as a subgroup of S_r hence S_n.

(r could possibly less than n because there might have multiple roots in general).

Now if $f(x)$ is separable. Then we have distinct roots $\{u_1, ..., u_n\}$ in F. For any u_i, we have $K[u_i] \cong K[x]/(f(x))$ since $f(x)$ is irreducible. If follows that there is a K-isomorphism $\sigma : K[u_i] \to K[x]/(f(x)) \to K[u_j]$ for all i, j. $sigma$ gives an K-embedding $K[u_i] \to \overline{K[u_j]} = \overline{K}$ and extended to a K-embedding $\bar{\sigma} : F \to \overline{K}$. Since F is normal, $\bar{\sigma}(F) = F$ (cf. Theorem ?). Thus $\bar{\sigma} \in G_f$ and $\bar{\sigma}(u_i) = \sigma(u_i) = u_j$. Therefore, G_f is transitive.

Moreover, since $K \subset K[u_i] \subset F$. So $|G_f| = [F : K] = [F : K[u_i]]n$ is divided by n. □

So now, we discuss irreducible separable polynomials of small degree. One might wondering how do we know a polynomial is separable or not. We have the following easy criteria:

Proposition 3.7.3. *Let $f(x) \in K[x]$ be an irreducible polynomial The following are equivalent:*
1. *$f(x)$ is separable.*
2. *$(f(x), f'(x)) = 1$ in $\overline{K}[x]$*
3. *$(f(x), f'(x)) = 1$ in $K[x]$*
4. *$f'(x) \neq 0$*

Recall that when $f(x) = \sum a_i x^i$, then $f'(x)$ is its formal differentiation which is $f'(x) := \sum i a_i x^{i-1}$.

Proof. If $f(x)$ is separable, then $f(x) = \prod_{i=1}^{n}(x - u_i)$ with distinct u_i in $\overline{K}[x]$. Thus $f'(x) = \sum \frac{\prod_{i=1}^{n}(x-u_i)}{x-u_i}$. If $(f(x), f'(x)) \neq 1$ in $\overline{K}[x]$, then $x - u_i | f'(x)$ for some i. However, $f'(u_i) = \prod_{j \neq i}(u_j - u_i) \neq 0$, a contradiction.

Conversely, if $f(x)$ is not separable, then $f(x) = \prod_{i=1}^{r}(x - u_i)^{a_i}$ with some $a_i \geq 2$. Let's say $a_1 \geq 2$. Then it's clear that $(x - u_1)$ is a factor of $f'(x)$ as well. Hence $(f(x), f'(x)) \neq 1$. This proved the equivalence of (1) and (2).

To see the equivalence of (2) and (3). Note that if $(f(x), f'(x)) = 1$ in $K[x]$, then $1 = f(x)s(x) + f'(x)t(x)$ for some $s(x), t(x) \in K[x]$. One can view this in $\overline{K}[x]$ and thus conclude that $(f(x), f'(x)) = 1$ in $\overline{K}[x]$. On the other hand, if $(f(x), f'(x)) = d(x) \neq 1$ in $K[x]$, then $d(x) = f(x)s(x) + f'(x)t(x)$ for some $s(x), t(x) \in K[x]$. One can view this in $\overline{K}[x]$ and thus conclude that $d(x)|(f(x), f'(x))$ in $\overline{K}[x]$. In particular, $(f(x), f'(x)) \neq 1$ in $\overline{K}[x]$

Now finally, since $f(x)$ is irreducible, $(f(x), f'(x))$ could only be 1 or $f(x)$. Since $f(x)|f'(x)$ if and only $f'(x) = 0$. Thus we are done. □

One notice that if char$K \neq 0$, then an irreducible polynomial is always separable. When char$K = p$, then an irreducible polynomial $f(x)$ is not separable if and only $f(x) = g(x^p)$ for some $g(x)$.

One can go a little bit further. If K is finite field with char$K = p$. Let $f(x) = \sum a_i x^i$ be an irreducible polynomial. $f'(x) = 0$ means that $p|i$ for all $a_i \neq 0$. Thus $f(x)$ can be rewrite as $\sum a_i x^{ip}$. Recall that each a_i can be written as b_i^p for some b_i because K is finite. Thus $f(x) = \sum b_i^p x^{ip} = (\sum b_i x^i)^p$. This contradicts to $f(x)$ being irreducible. To sum up, an irreducible polynomial over a finite field is always separable.

Let's now turn back to the discussion of Galois groups. If $f(x)$ is irreducible and separable of degree 2, then $G_f \cong S_2 \cong \mathbb{Z}_2$. If $f(x)$ is irreducible and separable of degree 3, then G_f is a subgroup of S_3 of order divided by 3. Thus G_f could be A_3 or S_3. The question now is how to distinguish these two cases.

Lemma 3.7.4. (char$K \neq 2$) *Let $f(x) \in K[x]$ be an irreducible and separable polynomial of degree 3 with splitting field F and roots u_1, u_2, u_3. Then $(G_f \cap A_3) = K[\Delta]$, where $\Delta := (u_1 - u_2)(u_1 - u_3)(u_2 - u_3)$*

Note that $f(x)$ is irreducible and separable, then F/K is Galois. And Δ^2 is invariant under G_f. Thus $D := \Delta^2 \in K$. We call D the discriminant of $f(x)$.

If $f(x)$ is written as $x^3 + bx^2 + cx + d$, then $s_1 := u_1 + u_2 + u_3 = -b$, $s_2 := u_1u_2 + u_1u_3 + u_2u_3 = c$, $s_3 := u_1u_2u_3 = -d$. We impose an ordering $u_1 > u_2 > u_3$. Then leading term of D is $u_1^4u_2^2$, which is the leading term of $s_1^2s_2^2$. Then we consider $D' := D - s_1^2s_2^2$ with lower leading term, which is $-4u_1^3u_2^3$. This leading term is the same as the leading term of $-4s_2^3$. So we consider $D^{(2)} := D' + 4s_2^3$. Inductively, one can write D in terms of s_1, s_2, s_3, hence in terms of b, c, d.

If $f(x)$ is normalized as $x^3 + px + q$, then $D = -4p^3 - 27q^2$.

Proof. $\sigma(\Delta) = \Delta$ if and only σ is an even permutation. So $\Delta \in (G_f \cap A_3)'$ clearly. Hence we have $K[\Delta] < (G_f \cap A_3)'$. Thus $K[\Delta]' > (G_f \cap A_3)$. If $\sigma \in K[\Delta]'$, then $\sigma(\Delta) = \Delta$, hence σ is even. Thus $K[\Delta]' < (G_f \cap A_3)$. So we have $K[\Delta]' = (G_f \cap A_3)$ and $K[\Delta] = (G_f \cap A_3)'$. □

We thus conclude that $G_f = A_3$ if and only if D_f is square in K. And $G_f = S_3$ if and only if D_f is not a square in K

Example 3.7.5.

Let $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$. It's irreducible.

Now we consider the case of degree 4 polynomial. One can also define Δ and discriminant D similarly. However, it turns out that this is not enough to classify all cases. The idea is to consider another normal subgroup $V_4 \lhd S_4$.

Let's first list at all possible subgroup in S_4. Since G_f is transitive with order divided by 4. We can have following

$\lvert G_f\rvert$	G_f	$G_f \cap V_4$	$\lvert G_f\rvert/\lvert G_f \cap V_4\rvert$
24	S_4	V_4	6
12	A_4	V_4	3
8	$\cong D_8$	V_4	2
4	$\cong \mathbb{Z}_4$	$\neq V_4$	2
4	V_4	V_4	1

Also we have the following

Lemma 3.7.6. *Let $f(x)$ be an irreducible separable polynomial of degree 4 with splitting field F and roots u_1, K, u_4. Let $\alpha = u_1u_2 + u_3u_4$ $\beta = u_1u_3 + u_2u_4$, $\gamma = u_1u_4 + u_2u_3$. Then $K[\alpha, \beta, \gamma] = (G_f \cap V_4)$.*

Let $g(x) = (x - \alpha)(x - \beta)(x - \gamma)$, then one can check that $\sigma(g(x) = g(x)$ for all $\sigma \in G_f$. Thus $g(x) \in K[x]$ for F/K is Galois. The cubic $g(x)$ is call the **resolvant cubic** of $f(x)$. If $f(x) = x^4 + bx^3 + cx^2 + dx + e$, then its resolvant cubic is $g(x) = x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2$ by computation on symmetric polynomials as we exhibited.

Proof. It clear that $K[\alpha, \beta, \gamma] < (G_f \cap V_4)'$. Hence we have $(G_f \cap V_4) < K[\alpha, \beta, \gamma]'$. Now if $\sigma \in K[\alpha, \beta, \gamma]'$ and $\sigma \ni V_4$. We claim that this would lead to a contradiction. And thus we are done.

The claim can be verified directly by exhausting all cases. For example, if $\sigma = (1, 3)$, then $\sigma(\alpha) = \alpha$ gives $u_3u_2 + u_1u_4 = u_1u_2 + u_3u_4$. Thus $(u_2 - u_4)(u_1 - u_3) = 0$ contradict to reparability of $f(x)$. The other cases can be computed similarly.

□

Let $m := |G_f|/|G_f \cap V_4| = [K[\alpha, \beta, \gamma] : K]$. By using this correspondence, one sees that:
1. $m = 1 \Leftrightarrow G_f = V_4 \Leftrightarrow g(x)$ splits into linear factors in $K[x]$.
2. $m = 3 \Leftrightarrow G_f = A_4 \Leftrightarrow g(x)$ is irreducible in $K[x]$ and D_g is a square in K.
3. $m = 6 \Leftrightarrow G_f = S_4 \Leftrightarrow g(x)$ is irreducible in $K[x]$ and D_g is not a square in K.

The only remaining unclear case is $m = 2$. This case corresponding to the case that $g(x)$ splits into a linear and a quadratic factors in $K[x]$. To see the Galois group, we claim that $G_f \cong D_8$ if and only if $f(x)$ is irreducible in $K[\alpha, \beta, \gamma][x]$.

First of all, if $f(x)$ is irreducible in $K[\alpha, \beta, \gamma][x]$, then

$$4 = [K[\alpha, \beta, \gamma][u_1] : K[\alpha, \beta, \gamma]] \leq [F : K[\alpha, \beta, \gamma]] = |G_f \cap V_4|.$$

So $G_f \cong D_8$.

On the other hand, F is the splitting field of $f(x)$ over $K[\alpha, \beta, \gamma]$ as well. Suppose that $f(x)$ is reducible. If $f(x)$ factors into a linear and a cubic factor in $K[\alpha, \beta, \gamma]$, then the Galois group of $f(x)$ over $K[\alpha, \beta, \gamma]$, which is $G_f \cap V_4$, can only $\cong A_3$ or S_3. This is a contradiction. Running over all cases, one sees that the only possible case is $f(x)$ factors into two linear and one quadratic factors. Thus $|G_f \cap V_4| = 2$ and hence $G_f \cong \mathbb{Z}_4$.

Dec. 8, 2006

3.8. **finite fields.** The Galois theory on finite fields is comparatively easy and basically governed by Frobenius map.

Recall that given a finite field F of q elements, it's prime field must be of the form $\mathbb{F}_p$ for some prime p. Let $n = [F : \mathbb{F}_p]$, then $|F| = p^n$.

Theorem 3.8.1. *F is a finite field with p^n elements if and only if F is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.*

Sketch. Recall that F^* is a multiplicative group of order $p^n - 1$. Hence it's easy to see that every element $u \in F$ satisfying $x^{p^n} - x$. Thus element of F are exactly roots of $x^{p^n} - x$, therefore, F is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

Conversely, if F is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Let $E \subset F$ be the subset of all roots of $x^{p^n} - x$. One can check that E is a subfield (containing $\mathbb{F}_p$ and all roots). By definition of splitting field, E is a splitting field, and $E = F$. So $|F| = |E| \leq p^n$. However, notice that $x^{p^n} - x$ is separable. So $|F| = p^n$. □

Proposition 3.8.2. *Let F be a finite field and F/K is an extension. Then F/K is Galois. The Galois group is cyclic, generated by Frobenius map.*

Proof. We shall prove the case that $K = \mathbb{F}_p$. For general K, $\mathbb{F}_p \subset K \subset F$. Since $F/\mathbb{F}_p$ is Galois, then F/K is also Galois with Galois group $K' < \mathrm{Gal}_{\mathbb{F}_p} F$ also a cyclic group.

Now we consider $F/\mathbb{F}_p$, and $|F| = p^n$. Since F is a splitting field of a separable polynomial $x^{p^n} - x$ over $\mathbb{F}_p$, F is Galois over $\mathbb{F}_p$.

The Galois group $\mathrm{Gal}_{\mathbb{F}_p} F$ has order $[F : \mathbb{F}_p] = n$. Consider the Frobenius map $\varphi : a \longrightarrow a^p$, which is clearly a $\mathbb{F}_p$-automorphism. So $\varphi \in \mathrm{Gal}_{\mathbb{F}_p} F$. Note that order of φ is n. So $\mathrm{Gal}_{\mathbb{F}_p} F$ can only be the cyclic group generated by φ. □

3.9. **cyclotomic extension.** We now start the study of cyclotomic extension.

Definition 3.9.1. *A cyclotomic extension of order n over K is a splitting field of $x^n - 1$.*

Remark 3.9.2. *If $char(K) = p$ and $n = p^r m$, then $x^n - 1 = (x^m - 1)^{p^r}$. Hence we may assume that either $char(K) = 0$ or $char(K) = p \nmid n$ in the study of cyclotomic extension.*

The main theorem is the following:

Theorem 3.9.3. *Keep the notation as above. Then we have*

1. *$F = K(\zeta)$, where ζ is a primitive n-th root of unity.*
2. *F/K is Galois whose Galois group $\mathrm{Gal}_{F/K}$ can be identified as a subgroup of $\mathbb{Z}_n^*$.*

(3) *If n is prime, then $\mathrm{Gal}_{F/K}$ is cyclic. More general, is $n = p^k$ with $p \neq 2$, then then $\mathrm{Gal}_{F/K}$ is cyclic.*

Proof. Let $S := \{u \in F | u^n = 1\}$. And let n' be the maximal order of elements in S. Clearly, $n' \leq n$ It's clear that S is an abelian multiplicative group. Therefore, it's easy to see that order of elements in S divides n'. It follows that $u^{n'} = 1$ for all $u \in S$. Hence $|S| \leq n'$.

Since we assume that $(n, \mathrm{char}(K)) = 1$, therefore $x^n - 1$ is separable. It follows that roots of $x^n - 1$ are all distinct, hence $|S| = n$. One sees that $n = n'$, therefore, there are elements of order n in S, denoted ζ. It follows that $F = K(S) = K(\zeta)$.

For any $\sigma \in \mathrm{Gal}_{F/K}$, $\sigma(\zeta) \in S$. Hence $\sigma(\zeta) = \zeta^i$ for some i. Therefore, we have a natural map $\phi : \mathrm{Gal}_{F/K} \to \mathbb{Z}_n$ by $\phi(\sigma) = i$ if $\sigma(\zeta) = \zeta^i$. Note that if ζ^i is not a primitive n-th root of unity, then $K(\zeta^i)$ is not the splitting field of $x^n - 1$, hence not equal to $K(\zeta)$, which is absurd. Thus sigma we conclude that ζ^i is a primitive n-th root of unity. It's easy to see that this is equivalent to $(i, n) = 1$. Thus $\phi : \mathrm{Gal}_{F/K} \to \mathbb{Z}_n^*$ is an injective group homomorphism.

Lastly, if $n = p^k$ with $p \neq 2$ or if $n = 2, 4$, then $\mathbb{Z}_n^*$ is cyclic. Hence every subgroup is cyclic. □

The structure of cyclotomic extension is thus determined by the primitive n-th root of unity. It's then natural to ask the degree of such extension and their minimal polynomials.

Definition 3.9.4. *If $\mathrm{char}K \nmid n$, then the n-th* **cyclotomic polynomial** *over K is defined as:*

$$g_n(x) := \prod_{\zeta_i\text{: prim. } n\text{-th root of } 1} (x - \zeta_i).$$

Proposition 3.9.5. *We have the following:*
1. $x^n - 1 = \prod_{d|n} g_d(x)$.
2. *$g_n(X) \in P[x]$, where P denoted the prime field. Moreover, if $\mathrm{char}K = 0$, we identify $P = \mathbb{Q}$, then $g_n(x) \in \mathbb{Z}[x]$.*
3. *$deg(g_n(x)) = \varphi(n)$, where φ denotes the Euler ϕ-function.*

Proof. (3) is clear from the definition.

For (1), we consider the following decomposition of sets

$$\{\zeta^i\}_{i=0,\dots,n-1} = \cup_{d|n} \{\zeta^i | o(\zeta^i) = d\}.$$

Note that $o(\zeta^i) = d$ implies that ζ^i is a primitive d-th root of unity. Thus we define $g_d'(x) := \prod_{o(\zeta^i)=d}(x - \zeta^i)$, and then $g_d'(x) | g_d(x)$. By the decomposition, we have

$$x^n - 1 = \prod_{i=0,\dots,n-1} (x - \zeta^i) = \prod_{d|n} g_d'(x).$$

Computing degrees, we have

$$n = \sum_{d|n} deg(g'_d(x)) \le \sum_{d|n} deg(g_d(x)) = \sum_{d|n} \varphi(d) = n.$$

Therefore, $g'_d(x) = g_d(x)$.

To see (2), we prove by induction on n. We assume that $g_d(x) \in P[x]$ for all $d < n$. We can write $x^n - 1 = g_n(x)f(x) \in F[x]$. In $P[x]$, we have $x^n - 1 = f(x)q(x) + r(x)$ by the division algorithm. We shall prove that $r(x) = 0$ and thus $g_n(x) = q(x) \in P[x]$ by the unique factorization of $F[x]$.

It suffices to show that $r(x) = 0$. To this end, note that $f(x)|x^n - 1$ in $F[x]$, and thus $f(x)|r(x)$ in $F[x]$. However, $deg(r(x)) < deg(f(x))$ unless $r(x) = 0$. This completes the proof of (2).

When $\mathrm{char}(K) = 0$, similar inductive argument plus Gauss Lemma will work. We leave it to the readers. □

Finally, if $K = \mathbb{Q}$ then the cyclotomic extension behave even nicer.

Proposition 3.9.6. *$F = \mathbb{Q}(\zeta)$ be the n-th cyclotomic extension over $\mathbb{Q}$. Then*
1. *$g_n(x)$ is irreducible.*
2. *$[F : bQ] = \varphi(n)$.*
3. *$\mathrm{Gal}_{\mathbb{Q}}F \cong \mathbb{Z}_n^*$.*

Example 3.9.7.

Consider the 3-rd cyclotomic extension over $\mathbb{F}_7$. Then $g_3(x) = \frac{x^3-1}{x-1} = (x-2)(x-4)$ is not irreducible. □

Proof. Asuuming (1), then $F = \mathbb{Q}[\zeta]$ is generated by ζ, where minimal polynomial of ζ over $\mathbb{Q}$ is $g_n(x)$. Thus $[\mathbb{Q}[\zeta] : \mathbb{Q}] = deg(g_n(x)) = \varphi(n)$. Morover, for every $i \in \mathbb{Z}_n^*$, the map $\zeta \mapsto \zeta^i$ produces an $\mathbb{Q}$-automorphism of F. Thus (3) follows.

It thus suffices to prove (1). Recall that $g_n(x) \in \mathbb{Z}[x]$. If $g_n(x) = f(x)h(x) \in \mathbb{Z}[x]$, where $f(x)$ is an irreducible polynomial with $f(\zeta) = 0$. We claim that ζ^p is also a root of $f(x)$ for all $(p, n) = 1$. Grant this claim, then by this process, we can conclude that ζ^i is a root of $f(x)$ for all $(i, n) = 1$. Therefore, $f(x) = g_n(x)$ is irreducible.

We now prove the claim. Suppose on the contrary that ζ^p is not a root of $f(x)$. Then it's a root of $h(x)$. We have $h(\zeta^p) = 0$. Hence ζ is a root of $h(x^p)$. Since $f(x)$ is irreducible, it's minimal polynomial of ζ over $\mathbb{Q}$. We have $f(x)|h(x^p)$. Thus we can write $h(x^p) = f(x)k(x)$ for some $k(x)$ in $\mathbb{Q}[x]$. By Gauss' Lemma, this equation holds in fact in $\mathbb{Z}[x]$. We now consider ring homomorphism $\bar{}:\mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Then

$$(\overline{h(x)})^p = \overline{h(x^p)} = \overline{f(x)k(x)}.$$

Thus $g.c.d(\overline{h(x)}, \overline{h(x)}) \neq 1$ in $\mathbb{Z}_p[x]$. It follows that

$$\overline{x^n - 1} = \overline{(\frac{x^n - 1}{g_n(x)})}\,\overline{f(x)h(x)}$$

has multiple roots. But $\overline{x^n - 1}' = n\bar{x}^{n-1} \neq 0$. So this is the required contradiction. □

Dec. 15, 2006

3.10. **solving cubic polynomials.** In this section, we are going to review classical result on solving polynomials by using non-classical language. I think this experience also serve a good start for Galois theory in general.

Definition 3.10.1. *A* **character** *from a group G to a field K is group homomorphism $\chi : G \to K^*$. The set of characters is denoted $Hom_{gp}(G, K^*)$.*

Let $Hom(G, K)$ be the set of functions from G to K. It's clear that $Hom(G, K)$ is a K-vector space.

Theorem 3.10.2 (E. Artin)**.** *$Hom_{gp}(G, K^*)$ is linearly independent in $Hom(G, K)$.*

Proof. Suppose on the contrary that $Hom_{gp}(G, K^*)$ is not linearly independent. Pick a linearly dependent subset $\{\chi_1, ..., \chi_n\}$ of minimal n. There are $a_i \in K$ such that $\sum a_i\chi_i = 0$, i.e.

$$\sum a_i\chi_i(g) = 0, \qquad (*)$$

for all $g \in G$. We can rewrite it as

$$\sum a_i\chi_i(gh) = 0, \qquad (**)$$

for all $g, h \in G$. Multiply $(*)$ by $\chi_1(h)$, we get

$$\sum a_i\chi_i(g)\chi_1(h) = 0. \qquad (***)$$

Compare $(*)$ with $(***)$, we get

$$\sum a_i(\chi_i(h) - \chi_1(h))\chi_i(g) = 0 \text{ for all } g \in G.$$

Thus $\sum_{i=2}^{n} a_i(\chi_i(h) - \chi_1(h))\chi_i = 0 \in Hom(G, K)$. It follows that the $n - 1$ elements $\{\chi_2, ..., \chi_n\}$ is linearly dependent, which is a contradiction to the minimality. □

Corollary 3.10.3. *Let F/K be an extension. The set of K-homomorphisms from F to $\overline{K}$ is linearly independent in the $\overline{K}$-vector space of linear maps from F to $\overline{K}$.*

Sketch. Take $G = F^*$. □

Let K be a field containing n-th root of unity ζ. Let F/K be a Galois extension with Galois group $\cong \mathbb{Z}_n$ generated by σ. We consider

$$\psi_\zeta := 1 + \zeta\sigma + \zeta^2\sigma^2 + ... + \zeta^{n-1}\sigma^{n-1} \in Hom(F, \overline{K}).$$

Any element of the form $\psi(x)$ is called a **Lagrange resolvent**.

By direct computation, we have the following properties.

Proposition 3.10.4. *Keep the notation as above, we have:*
1. $\sigma(\psi_\zeta(x)) = \zeta^{-1}\psi_\zeta(x)$.
2. $\psi_1(x) \in K$.
3. $(\psi_\zeta(x))^n \in K$.
4. $(\psi_\zeta(x))(\psi_{\zeta^{-1}}(x)) \in K$.
5. $\sum_{\zeta\in\mu_n} \zeta^{-r}\psi_\zeta(x) = n\sigma^r(x)$.

Now we can use this technique to solve cubic equations. Let $f(x) = x^3 + px + q \in K[x]$ be an irreducible polynomial with discriminant $D = -4p^3 - 27q^2 \in K$. We assume that K contains a primitive 3-root of unity ζ. We have extension $K \subset L := K[\sqrt{D}] \subset F := K[u_1, u_2, u_3]$. Note that F/L is Galois with Galois group $\cong \mathbb{Z}_3$.
Step 1. $\psi_\zeta \neq 0 \in Hom(F, \overline{K})$, in fact $\psi_\zeta(u_1) \neq 0$.

Step 2. $\psi_\zeta(u_1) \neq L$ and $(\psi_\zeta(u_1))^3 \in L$, thus $F = L[\psi_\zeta(u_1)]$.
And similarly, $\psi_{\zeta^2}(u_1) \in L, (\psi_{\zeta^2}(u_1))^3 \in L$. Moreover, $\psi_\zeta(u_1)\psi_{\zeta^2}(u_1) \in L$.
Step 3. Solve $\psi_\zeta(u_1)$,$\psi_{\zeta^2}(u_1)$.
Recall that

$$\Delta := (u_1-u_2)(u_2-u_3)(u_3-u_1) = u_1^2u_2+u_2^3u_3+u_3^2u_1-u_1u_2^2-u_2u_3^2-u_3u_1^2.$$

$$\psi_\zeta(u_1)^3 = u_1^3+u_2^3+u_3^3+3\zeta(u_1^2u_2+u_2^2u_3+u_3^2u_1)+\zeta^2(u_1u_2^2+u_2u_3^2+u_3u_1^2)+6u_1u_2u_3.$$

Let $v_1 = u_1^2u_2 + u_2^2u_3 + u_3^2u_1, v_2 = u_1u_2^2 + u_2u_3^2 + u_3u_1^2$, then

$$v_1 + v_2 = (u_1 + u_2 + u_3)(u_1u_2 + u_2u_3 + u_3u_1) - 3u_1u_2u_3 = 3q,$$

$$v_1 - v_2 = \Delta.$$

Thus $\psi_\zeta(u_1)^3$ can be expressed in terms of p, q, Δ.
Step 4. solve u_1, u_2, u_3 in terms of $\psi_\zeta(u_1)$,$\psi_{\zeta^2}(u_1)$.
By the property 5 above, we have

$$3u_1 = \psi_1(u_1) + \psi_\zeta(u_1) + \psi_{\zeta^2}(u_1),$$

$$3u_2 = 3\sigma(u_1) = \psi_1(u_1) + \zeta^{-1}\psi_\zeta(u_1) + \zeta^{-2}\psi_{\zeta^2}(u_1),$$

$$3u_3 = 3\sigma^2(u_1) = \psi_1(u_1) + \zeta^{-2}\psi_\zeta(u_1) + \zeta^{-1}\psi_{\zeta^2}(u_1).$$

And note that $\psi_1(u_1) = 0$. So one can solve cubic polynomial explicitly.

3.11. **cyclic extension.** The discussion in the previous section can be extended to a more general setting.

Definition 3.11.1. *We say that an extension is cyclic (resp. abelian) if it's algebraic Galois and* $\mathrm{Gal}_{F/K}$ *is cyclic (resp. abelian). An cyclic extension of order* n *is an cyclic extension whose Galois group is isomorphic to* $\mathbb{Z}_n$.

The following theorem characterize cyclic extension except some exceptional case.

Theorem 3.11.2. *Suppose that char$(K) = 0$ or char$(K) = p \nmid n$. Suppose furthermore that there is a primitive n-th root of unity in K, say ζ. Then F/K is a cyclic of order n if and only if $F = K(u)$ where u is a root of irreducible polynomial $x^n - a \in K[x]$.*

Before we get into the proof. Let's consider the "difference" between u and $\sigma(u)$ for $\sigma \in \mathrm{Gal}_{F/K}$. Let F/K be a finite Galois extension. Then in this circumstance, norm and trace (which we will define more generally later) are nothing but $N_{F/K}(u) := \prod_{\sigma \in \mathrm{Gal}_{F/K}} \sigma(u)$ and $T_{F/K} := \sum_{\sigma \in \mathrm{Gal}_{F/K}} \sigma(u)$. It's easy to see that $T(u - \sigma(u)) = 0$ and $N(u/\sigma(u)) = 1$. The follows lemma says that the converse is also true for cyclic extension, which will play the central role in the study of cyclic extension.

Lemma 3.11.3. *Let F/K be an cyclic extension with σ the generator of the Galois group.*

1. *If $T_{F/K}(u) = 0$, then there exists an $v \in F$ such that $u = v - \sigma(v)$.*
2. *(Hilbert's Theorem 90) If $N_{F/K}(u) = 1$, then there exists an $v \in F$ such that $u = v/\sigma(v)$.*

Proof of the Theorem 3.11.2. Let u be a root of $x^n - a$, then all the roots are $u\zeta^i$ for $i = 0, ..., n-1$. Since $\zeta \in K$. We can produce an element in Galois group by considering $\sigma_i : u \mapsto u\zeta^i$. Thus we have $\{\sigma_i\}_{i=0,\dots,n-1} \subset \mathrm{Gal}_K F$. It's clear that $\mathrm{Gal}_K F = \{\sigma_i\}_{i=0,\dots,n-1} =< \sigma_1 >$. Thus $F = K(u)$ is a cyclic extension over K.

Conversely, suppose that F/K is a cyclic extension of order n. Since there is a primitive n-th root $\zeta \in K$, one has $N(\zeta) = \zeta^n = 1$. By the Lemma, there exist an v such that $\zeta = v/\sigma(v)$. Let $u = v^{-1}$, then $\sigma(u) = \zeta u$. Hence $\sigma(u^n) = u^n \in K$. Therefore u satisfies $x^n - a \in K[x]$ for some $a \in K$.

Moreover, for $u\zeta^i$ and $u\zeta^j$, there is an automorphism sending $u\zeta^i$ to $u\zeta^j$. So they have the same minimal polynomial $p(x)$ dividing $x^n - a$. One the other hand, $p(x)$ has n distinct roots $u\zeta^i$ for $i = 0, ..., n-1$. It follows that $p(x) = x^n - a$ is irreducible. One has $[K(u) : K] = n$ and thus $F = K(u)$. □

Theorem 3.11.4. *Suppose that char$(K) = p \neq 0$. Then F/K is a cyclic extension of order n if and only if $F = K(u)$, where u is a root of an irreducible polynomial $x^p - x - a \in K[x]$.*

Proof. The proof is parallel to the previous one.

Let u be a root of $x^p - x - a$, then all the roots are $u + i$ for $i = 0, ..., p-1$. It's clear that $F = K(\zeta)$ is a cyclic extension over K with Galois group generated by σ such that $\sigma(u) = u + 1$.

Conversely, suppose that F/K is a cyclic extension of order n. One has $T(1) = p = 0$. By the Lemma, there exist an v such that $1 =$

$v - \sigma(v)$. Let $u = -v$, then $\sigma(u) = u + 1$. Hence $\sigma(u^p) = u^p + 1$ and $\sigma(u^p - u) = u^p - u$. Therefore u satisfies $x^p - x - a \in K[x]$ for some $a \in K$.

Moreover, for $u + i$ and $u + j$, there is an automorphism sending $u\zeta^i$ to $u\zeta^j$. So they have the same minimal polynomial $p(x)$ dividing $x^p - x - a$. One the other hand, $p(x)$ has p distinct roots $u + i$ for $i = 0, ..., p - 1$. It follows that $p(x) = x^p - x - a$ is irreducible. One has $[K(u) : K] = n$ and thus $F = K(u)$. □

It remains to define norm and trace, and prove the main lemma 3.11.3.

Definition 3.11.5. *Let $[F : K]$ be a finite separable extension. Let Σ be the set of K-embeddings of F into $\overline{K}$. For any $u \in F$, we define the norm, denoted*

$$N_{F/K}(u) := (\prod_{\sigma\in\Sigma} \sigma(u)).$$

Similarly, we define the trace as

$$T_{F/K}(u) := (\Sigma_{\sigma\in\Sigma}\sigma(u)).$$

Example 3.11.6. *If F/K is finite Galois extension, then the set of all K-embeddings of F is nothing but the Galois group of F (since F is normal). Therefore, $N_{F/K}(u) = \prod_{\sigma\in\mathrm{Gal}_{F/K}} \sigma(u)$ and $T_{F/K}(u) = \sum_{\sigma\in\mathrm{Gal}_{F/K}} \sigma(u)$*

Proof of Lemma 3.11.3. We only prove that $T(u) = 0$ implies $u = v - \sigma(v)$. The other implication is easy.

Step 1. Find an element $z \in F$ with $T(z) \neq 0$. This is an immediate consequence of independency of automorphism.

Step 2. We normalize it to get $w \in F$ with $T(w) = 1$. In fact, we take $w := \frac{z}{T(z)}$.

Step 3. Let

$$v = uw + (u + \sigma(u))\sigma(w) + ... + (u + \sigma(u) + ... + \sigma^{n-2}(u))\sigma^{n-2}(w).$$

Then by direct computation and $T(u) = \sum \sigma(u) = 0$, we are done.

For the norm, if $N(u) = 1$, then $u \neq 0$. Take

$$v = uy + u\sigma(u)\sigma(y) + ... + u\sigma(u)...\sigma^{n-1}(u)\sigma^{n-1}(y).$$

By independency of automorphism, there exist a y such that v is non-zero. One checks that $u^{-1}v = \sigma(v)$. We are done. □

3.12. **radical extension.**

Definition 3.12.1. *F/K is said to be an radical extension if $F = K(u_1, ..., u_n)$ such that for $1 \leq i \leq n$, $u_i^{n_i} \in K(u_1, ..., u_{n-1})$.*

For a polynomial $f(x) \in K[x]$. We say $f(x) = 0$ is solvable by radical if its splitting field E is contained in some radical extension.

Remark 3.12.2. *In the definition, it's not necessary that the splitting field itself is a radical extension over K.*

The main observation is the following:

Proposition 3.12.3. *Let F/K be a radical and Galois extension over K. Write $F = K(u_1, ..., u_n)$ such that for $1 \leq i \leq n$, $u_i^{n_i} \in K(u_1, ..., u_{n-1})$. Let $m = \prod n_i$ and assume that char$(K) \nmid m$. Suppose furthermore that K contains a primitive m-th root of unity. Then* $\mathrm{Gal}_{F/K}$ *is solvable.*

Proof. Let $K_i := K(u_1, ..., u_i)$. And let $G_i = K_i'$. One sees that K_1 is cyclic over K, hence Galois over K. Hence $G_1 \lhd G_0 = \mathrm{Gal}_{F/K}$. Consider next F/K_1 which is radical and Galois. Then K_2 is cyclic over K_1 and hence similarly, $G_2 \lhd G_1$. Therefore, we have a solvable series $\{e\} = G_n \lhd G_{n-1} \lhd ... \lhd G_0 = \mathrm{Gal}_{F/K}$ with G_{i-1}/G_i cyclic. We are done. □

One can actually generalize it to the following general setting:

Theorem 3.12.4. *Let F/K be a radical extension, and $K \subset E \subset F$. Then* $\mathrm{Gal}_{E/K}$ *is solvable. As a consequence, if $f(x) = 0$ is solvable by radical, then G_f is solvable.*

Proof. We first reduce to simpler situation.
Step 1. Let $G = \mathrm{Gal}_{E/K}$ and $K_0 = G'$. It's clear that F/K_0 is radical, and E/K_0 is Galois for $\mathrm{Gal}_{E/K_0} = G'' = G$ and $G''' = G'$. Thus F/K_0 is radical and E/K_0 is Galois with Galois group $\mathrm{Gal}_{E/K}$.

We thus replacing K by K_0 and assume that E/K is Galois.
Step 2. Reduce to the case that $E = F/K$ is Galois. To see this, let $\sigma : F \to \overline{K}$ be an K-embedding. One can show that $\sigma(F)$ is again a radical extension. One can also prove that if $F_1, F_2 \subset \overline{K}$ are radical extension over K, then F_1F_2 is a radical extension over K. Hence let N be the compositum of $\sigma(F)$ for all σ. It follows that N is radical over K. Moreover, N is normal over K.

Since E/K is Galois, in particular, E is normal over K and E is a stable intermediate subfield of N/K. Then one has a homomorphism $\mathrm{Gal}_{N/K} \to \mathrm{Gal}_{E/K}$. This is surjective because N is normal. Thus it suffices to prove that $\mathrm{Gal}_{N/K}$ is solvable.
Step 3. By the same trick an in Step 1. We may assume that N/K is Galois. Therefore, it suffices to show that if F/K is Galois and radical, then $\mathrm{Gal}_{F/K}$ is solvable.
Step 4. Since F/K is separable, we may assume that $(\mathrm{char}(K), n_i) = 1$. Let $m = \prod n_i$.

Let ζ be a primitive m-th root of unity. We claim that $F(\zeta)$ is Galois over K. Grant this for the time being, then $F(\zeta)$ is Galois over $K(\zeta)$ and $K(\zeta)' \lhd \mathrm{Gal}_{F(\zeta)/K}$. Moreover, $\mathrm{Gal}_{F(\zeta)/K}/K(\zeta)' \cong \mathrm{Gal}_{K(\zeta)/K}$. By Proposition 3.12.3, $K(\zeta)'$ is solvable. $K(\zeta)/K$ is cyclotomic, hence $\mathrm{Gal}_{K(\zeta)/K}$ is solvable. Thus, $\mathrm{Gal}_{F(\zeta)/K}$ is solvable.

Now F/K is Galois, $\mathrm{Gal}_{F/K} \cong \mathrm{Gal}_{F(\zeta)/K}/F'$ which is solvable.
Step 5. To prove the claim, suppose that F is a splitting field of separable polynomial $f_1, .., f_n \in K[x]$. Then $F(\zeta)$ is nothing but a splitting field of separable polynomials $f_1, ..., f_n, x^m - 1$. Thus we are done. □

Theorem 3.12.5. *Let E be a finite dimensional Galois extension over K with solvable Galois group. Assume that char$(K) \nmid [E : K]$, then there is a radical extension F/K containing E.*

Proof. We prover by induction on $[E : K]$. Let $n = [E : K]$ and assume the theorem is true for all Galois extension of degree $< n$.

Let ζ be a primitive n-th root of unity. Then $E(\zeta)/K(\zeta)$ is Galois. If $[E(\zeta) : K(\zeta)] < n$ then we are done by induction hypothesis and the fact that $K(\zeta)/K$ is radical.

By replacing E, K by $E(\zeta), K(\zeta)$ respectively, we my assume that K has m-th root of unity.

$\mathrm{Gal}_{E/K}$ is solvable, let H be a subgroup of index q, for some prime q. Then H'/K is a cyclic extension, hence a radical extension. By induction hypothesis, E/H' is radical. We are done. □

Corollary 3.12.6. *Let $f(x) \in K[x]$ be a polynomial of degree $n > 0$. Suppose that char$(K) \nmid n!$, then $f(x) = 0$ is solvable by radical if and only if G_f is solvable.*

Dec. 22, 2006

3.13. **separability and inseparability.** We first recall something about separable extension.

To start with, let $f(x)$ be an irreducible polynomial in $K[x]$ and $f'(x)$ be its derivative (formally). More precisely, if $f(x) = \sum_{i=0}^{n} a_i x^i$, then $f'(x) := \sum_{i=1}^{n} i a_i x^{i-1}$. One has the following equivalence:

(1) $f(x)$ is separable, i.e. no multiple roots in $\overline{K}$.
(2) $(f(x), f'(x)) = 1 \in \overline{K}[x]$.
(3) $(f(x), f'(x)) = 1 \in K[x]$.
(4) $f'(x) = 0$.

Therefore, the only possibility to have non-separable polynomial is $char(K) = p$ and $f(x) = g(x^p)$.

Given an element u algebraic over K, one can define the separable degree to be the number of distinct roots of minimal polynomial. This notion can be extended to a general setting:

Definition 3.13.1. *Let F/K be an extension. Fix an embedding $\sigma : K \to L = \overline{L}$. We define the separable degree of F/K, denoted $[F : K]_s$, to be the cardinality of*

$$S_\sigma := \{\tau : F \to L | \tau_{|K} = \sigma\}.$$

In particular, if $F = K(u)$ for some u with minimal polynomial $p(x)$, then $[F : K]_s$ is the number of distinct roots of $p(x)$ in $\overline{K}$.

One can check that $[F : K]_s$ is independent of σ and L. Hence the definition is well-defined. Moreover, if $F = K(u)$ for u algebraic over K, then $[F : K]_s = [K(u) : K]_s$ is the number of distinct roots of the minimal polynomial $p(x)$ of u. This can be seen by considering K-embedding $\tau : K(u) \to \overline{K}$, $\tau(u)$ must be a root of $p(x)$ and τ is determined by $\tau(u)$.

Proposition 3.13.2. *If $K \subset E \subset F$, then $[F : K]_s = [F : E]_s[E : K]_s$. Moreover, if F/K is finite, then $[F : K]_s \leq [F : K]$.*

Sketch. The first statement follows from the definition.

It's clear that $[K(u) : K]_s \leq [K(u) : K]$ by definition. Then by induction, we have $[F : K]_s \leq [F : K]$ if $[F : K]$ is finite. □

Then we have the following useful criterion:

Proposition 3.13.3. *If F/K is finite, then F/K is separable if and only if $[F : K]_s = [F : K]$.*

Sketch. Suppose that F/K is separable. Let L be the maximal intermediate subfield such that $[L : K]_s = [L : K]$. We claim that $L = F$. Suppose not, let $u \in F - L$. Since u is separable over K, it's separable over L. Thus $[L(u) : L]_s = [L(u) : L]$. So $[L(u) : K]_s = [L(u) : K]$ give the contradiction.

Conversely, for any $u \in F$, one sees that

$$[F:K]_s = [F:K(u)]_s[K(u):K]_s \leq [F:K(u)][K(u):K] \leq [F:K].$$

Since $[F:K]_s = [F:K]$, we have $[K(u):K]_s = [K(u):K]$. Thus u is separable over K. □

we can then prove the following:

Theorem 3.13.4. *Suppose that $F = K(S)$ such that each elements of S is separable over K, then F/K is separable.*

Sketch. By the previous Proposition, one can see that if u_1, u_2 are separable over K, then $K(u_1, u_2)$ is separable over K.

In general, if $u \in K(S)$, then $u \in K(u_1, ..., u_n)$ for some $u_1, ..., u_n \in S$, hence separable over K. Then so is u. □

In particular, let

$$S := \{u \in F | u \text{ is separable over } K\}.$$

Then S is an intermediate subfield over K. The reason can be seen as following: $u, v \in S$, $u + v, uv \in K(u, v)$. Since u, v are separable over K. Then $K(u, v)$ is an separable extension. Thus elements in $K(u, v)$ are separable over K.

Exercise 3.13.5.

Separable extension has the following properties:
1. Let $K \subset E \subset F$. Then F/K is separable if and only if F/E and E/K are separable.
2 If E/K is separable then FE/F is separable for an extension F/K.
3 If $E, F \subset L$ are separable extension over K. Then EF is separable over K. □

Exercise 3.13.6.

Let F/K be a finite extension, then $[F:K]_s = [S:K]$. □
Before we move onto the study of inseparability, we would like to prove the famous theorem of primitive element.

Theorem 3.13.7. *If F/K is separable and finite, then $F = K(\alpha)$ for some $\alpha \in F$.*

In order to prove the theorem we need to study simple extensions. When the base field is finite, then things are easy.

Proposition 3.13.8. *If K is a finite field and F/K is an algebraic field extension. The following are equivalent:*

(1) *F/K is finite.*
(2) *$F = K(\alpha)$ for some $\alpha \in f$. That is, F/K is a simple extension.*
(3) *There is only finitely many intermediate fields.*

Proof. For (1) $\Rightarrow$ (2), if F/K is finite, then F is finite. F^* is a cyclic multiplicative group, say $F^* =< \alpha >$. Then it's clear that $F = K(\alpha)$.

(2) $\Rightarrow$ (1) is trivial.

(1) $\Rightarrow$ (3). Suppose that $|K| = q, |F| = q^n$. Let E be an intermediate field, then it's clear that $|E| = q^d$ for some $d|n$. One can prove that for any $d|n$, there is exactly one intermediate field with q^d elements. Hence there are only finitely many intermediate fields.

(3) $\Rightarrow$ (1). Suppose on the other hand that F/K is not finite. First consider the case that F/K is not algebraic, i.e. there is $u \in F$ not algebraic over K. Then we have infinitele many intermediate subfields $K(u) \supset K(u^2) \subset K(u^4)$.... Which is a contradiction.

Secondly, if F/K is algebraic. Then it is not finitely generated, otherwise it's finite. We can easily get (by axiom of choice) a infinite sequence of intermediate fields

$$K \subset K(a_1) \subset K(a_1, a_2)...$$

by adding generators. □

Proposition 3.13.9. *Let F/K be a finite extension, then $F = K(\alpha)$ if and only if there is only finitely many intermediate fields.*

Proof. If K is finite, then we are done by the previous Proposition. We assume that K is infinite.

Suppose that there is only finitely many intermediate fields. For any $\alpha, \beta \in F$, we can consider intermediate fields $K(\alpha + c\beta)$ as c ranging in K. Since K is infinite. There must exists $c_1, c_2 \in K$ such that $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. It's easy to check that

$$K(\alpha, \beta) = K(\alpha + c\beta).$$

By induction on number of generators of F/K, we proved that F/K is a simple extension.

Suppose now that $F = K(\alpha)$. We would like to prove the finiteness by using the following map:

$$\phi : \{E|K \subset E \subset F\} \to \Sigma := \{p_E(x)\},$$

where $p_E(x)$ denotes the minimal polynomial of α over E. Since every $p_E(x)$ is a divisor of $p_K(x)$ in the algebraic closure (or in the splitting field), it's clear that Σ is finite.

It's enough to prove that ϕ is injective. To this end, let E_0 be the extension over K generated by coefficient of $p_E(x)$. One sees that $p_E(x) \in E_0[x]$ is irreducible and hence a minimal polynomial of α over E_0. Hence we have

$$[K(\alpha) : E] = deg(p_E(x)) = [K(\alpha) : E_0].$$

It follows that $E = E_0$. Thus, if $\phi(E) = \phi(E')$, then $E = E_0 = E'$. This proved the injectivity. □

Proof of Theorem 3.13.7. We may assume that K is infinite. By induction on generators of F/K, we may assume that $F = K(\alpha, \beta)$. Let $n := [F : K]_s$, and $\sigma_1, ..., \sigma_n$ be the distinct embedding of F in $\overline{K}$. Let

$$P(x) := \prod_{i \neq j} (\sigma_i(\alpha + \beta x) - \sigma_j(\alpha - \beta x).$$

Since $deg(P(x)) = n(n-1)$ and there are infinitely many elements in K, there must be an $c \in K$ such that $P(c) \neq 0$. Thus all $\sigma_i(\alpha + c\beta)$ are all distinct. This gives n distinct embedding of $K(\alpha + c\beta)$. One has

$$[F : K]_s = n \leq [K(\alpha + c\beta) : K]_s \leq [K(\alpha + c\beta) : K] \leq [F : K].$$

Since F/K is separable, so is $[F : K]_s = [F : K]$. Thus $[K(\alpha + c\beta) : K] \leq [F : K]$, and therefore, $K(\alpha, \beta) = F = K(\alpha + c\beta)$. □

We now turn our interest to non-separable extension. Instead of non-separable extension in general, we first study the special case the all roots of minimal polynomial are the same.

Definition 3.13.10. *Let F/K be an extension. An element $u \in F$ is purely inseparable over K if its minimal polynomial $p(x) \in K[x]$ factors in $F[x]$ as $(x-u)^m$. An extension F/K is purely inseparable over K if every element of F is purely inseparable over K.*

It's easy to see that an element $u \in F$ which is both separable and purely inseparable over K if and only if $u \in K$.

Another useful observation is:

Lemma 3.13.11. *Let F/K be an extension with $char(K) = 0 \neq 0$. If $u \in F$ is algebraic over K, then u^{p^n} is separable over K for some $n \geq 0$.*

Proof. The point is that if u is not separable, then its minimal polynomial $p(x)$ is of the form $f(x^p)$. Then $f(x)$ is the minimal polynomial of u^p. By induction on degree of u, we are done. □

Being purely inseparable has the following equivalent formulation:

Theorem 3.13.12. *Let F/K be an algebraic extension with* $\mathrm{char}(K) = p \neq 0$. *The following are equivalent:*

1. *F/K is purely inseparable, i.e. every element $u \in F$ has minimal polynomial of the form $(x-u)^m$.*
2. *for all $u \in F$, the minimal polynomial is of the form $x^{p^n} - a \in K[x]$.*
3. *for all $u \in F$, $u^{p^n} \in K$ for some $n \geq 0$.*
4. *$S = K$, that is, the only element of F which is separable over K are the elements in K.*
5. *F/K is generated by purely inseparable elements.*

Proof. Let $m = p^n r$.

$(x-u)^m = (x-u)^{p^n r} = (x^{p^n} - u^{p^n})^r = x^m - ru^{p^n}x^{p^n(r-1)} + ... \in K[x]$.

Therefore, $u^{p^n} \in K$, this proved (1) $\Rightarrow$ (3).

Moreover, $p'(x) := x^{p^n} - u^{p^n}) \in K[x]$ and $p'(x)^r$ is the minimal polynomial of u (hence irreducible). Therefore, $r = 1$. This proved (1) $\Rightarrow$ (2).

(2) $\Rightarrow$ (3) is trivial.

For (3) $\Rightarrow$ (1), let $a = u^{p^n} \in K$, then $f(x) := x^{p^n} - a \in K[x]$ and factors in $F[x]$ as $(x-u)^{p^n}$. Hence the minimal polynomial of u over K is a factor of $f(x)$ and factors into $(x-u)^m$ in $F[x]$.

We have seen (1) $\Rightarrow$ (4) and (5), (4) $\Rightarrow$ (3) follows from the above Lemma 3.13.11.

It remains to show that (5) $\Rightarrow$ (3). To see this, first note that $F = K(\Sigma)$ where Σ consists of elements u_i such that $u_i^{p^n} \in K$ for some n (By the proof of (1) $\Rightarrow$ (3)). For any $u \in F$, say $u = \frac{f(u_1,...,u_r)}{g(u_1,...,u_r)}$. Pick N such that $u_i^{p^N} \in K, \forall i = 1,...,r$. Then $u^{p^N} \in K$. □

As a corollary, one can show that

$$P := \{u \in F | u \text{ is purely inseparable over } K\}$$

is an intermediate subfield.

Theorem 3.13.13. *Let F/K be an algebraic extension. Keep the notation as above for S, P.*

(1) *S/K is separable.*
(2) *P/K is purely inseparable.*
(3) *F/S is purely inseparable.*
(4) *F/P is separable if and only $F = PS$.*
(5) *$P \cap S = K$.*
(6) *if F/K is normal, then S/K and F/P are Galois. And $\mathrm{Gal}_{F/K} = \mathrm{Gal}_{F/P} \cong \mathrm{Gal}_{S/K}$.*

Proof. We have seen (1), (2), (5). (3) follows from Lemm 3.13.11. For (4), look at $P \subset SP \subset F$. If F/P is separable, then F/SP is separable. Look at $S \subset SP \subset F$ now. We have F/K is purely inseparable, thus so is F/SP. Thus $F = SP$.

On the other hand, if $F = SP = P(S)$, then clearly $F = P(S)$ is separable over P.

Lastly, we look at $G := \mathrm{Gal}_{F/K}$. We claim that $G' = P$, hence F/P is Galois with Galois group $\mathrm{Gal}_{F/P} = \mathrm{Gal}_{F/K}$.

To see the claim, if $u \in P$, then it's clear that $\sigma(u) = u$ for all $\sigma \in G$. Therefore, $P \subset G'$. On the other hand, if $u \in G'$ and v is another root of $p(x)$, the minimal polynomial of u. There is an σ such that $\sigma(u) = v$. Since F/K is normal, this σ can be extended to G. But $u \in G'$, thus $v = u$, in other words, $p(x) = (x-u)^m$.

F is Galois over P because $P = G'$. Hence F/P is separable. By (5), $F = PS$.

Lastly, we consider $\mathrm{Gal}_{F/P} = \mathrm{Gal}_{F/K} \to \mathrm{Gal}_{S/K}$ by restriction. This is well-defined since S is stable. More precisely, for $u \in S$, $\sigma(u) \in S$ for all $\sigma \in G$ because $\sigma(u)$ has the same minimal polynomial as u does. This is surjective by extension theorem. It remains to show the injectivity. If $\sigma|_S = \tau|_S$, then for all $u \in F$ we have $u^{p^n} \in S$. Thus,

$$\sigma(u)^{p^n} = \sigma(u^{p^n}) = \tau(u^{p^n}) = \tau(u)^{p^n}.$$

It follows that $\sigma(u) = \tau(u)$.

It remains to show that S/K is Galois. To see this, suppose $u \in S$ is fixed by all $\sigma \in G$, then $u \in G' = P$. Hence $u \in K$. We are done. □

Definition 3.13.14. *Let F/K be a finite extension. We define the inseparable degree of F/K, denoted $[F:K]_i$, to be $[F:K]/[F:K]_s$.*

Note that $[F:K]_i = [F:S] = p^n$ for some n.

If $\mathrm{char}(K) = p \neq 0$, we write $K^p = \{u^p | u \in K\}$.

Definition 3.13.15. *K is said to be perfect if $K^p = K$*

Example 3.13.16. *Finite fields are perfect. $\mathbb{F}_p(x)$ is not perfect.*

Corollary 3.13.17. *Let F/K be an algebraic extension with* $\mathrm{char}(K) = p \neq 0$. *We have*

(1) *If F/K is separable, then $F = KF^{p^n}$ for each $n \geq 1$.*
(2) *If F/K is finite and $F = KF^p$, then F/K is separable.*
(3) *In particular, $u \in F$ is separable over K if and only if $K(u^p) = K(u)$.*

Note that F^p is not necessarily an extension over K. So is F^{p^n}. But we can take KF^{p^n}, which is an extension over K.

Proof. We first suppose that F/K is finite, hence finitely generated. Write $F = K(u_1, ..., u_r)$. It's clear that there is $N \geq 1$ such that $u^{p^N} \in S$. Hence $F^{p^N} \subset S$, therefore, $KF^{p^N} \subset S$.

We claim that $S = KF^{p^N}$. To see this, one notices that F is purely inseparable over KF^{p^N}, so is S purely inseparable over KF^{p^N}. And on the other hand, S is separable over K, so is over KF^{p^N}. Hence $S = KF^{p^N}$.

For (1), if F/K is separable and finite, then we have $F = KF^{p^N}$. However, in the proof, one can choose N to be arbitrary large. More precisely, one has $F = KF^{p^N}$ for all $N \geq N_0$. By looking at the inclusion

$$F = KF^{p^N} \subset KF^{p^{N-1}} \subset ... \subset KF^p \subset F.$$

One has $F = KF^{p^n}$ for all $n \geq 1$.

Suppose now that F/K is separable but not necessarily finite. For any $u \in F$, we consider $F_0 := K(u)$ which is separable and finite over K. Thus $u \in F_0 = KF_0^{p^n} \subset KF^{p^n}$ for all $n \geq 1$. This proves (1).

We now prove (2). If $F = KF^p$, then $F = K(KF^p)^p = KF^{p^2}$. Inductively, one has $F = KF^{p^n}$ for all $n \geq 1$. Since we have show that $S = KF^{p^N}$, it follows that $F = S$.

Apply the statement to a single element. We consider $F = K(u)$. $F^p \subset K^p(u^p) \subset K(u^p)$. Indeed, $KF^p = K(u^p)$. By (2), if $K(u) = K(u^p)$, then u is separable. By (1), if u is separable, then $K(u) = K(u^p)$. □

3.14. **transcendental extension.** We now start our discussion on transcendental extension. The main purpose is to show that the concept of *transcendental degree*, which is the cardinality of transcendental basis, can be well-defined. Moreover, transcendental degree is a good candidate for defining dimension.

Definition 3.14.1. *Let F/K be an extension. $S \subset F$ is said to be algebraically dependent (over K) if there is an $n \geq 1$ and an $f \neq 0 \in K[x_1, ..., x_n]$ such that $f(s_1, ..., s_n) = 0$ for some $s_1, ..., s_n \in S$. Roughly speaking, some element of S satisfy a non-zero algebraic relation f over K.*

S is said to be algebraically independent over K if it's not algebraically dependent over K.

Example 3.14.2. *For any $u \in F$, $\{u\}$ is algebraically dependent over K if and only if u is algebraic over K.*

Example 3.14.3. *In the extension $K(x_1, ..., x_n)/K$, $S = \{x_1, ..., x_n\}$ is algebraically independent over K.*

Dec. 29, 2006

The following theorem says that finitely generated purely transcendental extension are just rational function fields.

Theorem 3.14.4. *If $\{s_1, ..., s_n\} \subset F$ is algebraically independent over K. Then $K(s_1, ..., s_n) \cong K(x_1, ..., x_n)$.*

Proof. We consider the homomorphism $\theta : K[x_1, ..., x_n] \to K[s_1, ..., s_n]$. θ is surjective by definition. It's injective because $\{s_1, ..., s_n\} \subset F$ is algebraically independent. Then θ induces an isomorphism on quotient fields. □

One notices that the notion of being algebraic independent is an analogue of being linearly independent. Therefore, one can try to define the notion of "basis" and "dimension" in a similar way.

Definition 3.14.5. *$S \subset F$ is said to be a transcendental basis of F/K if S is a maximal algebraically independent set. In other words, for all $u \in F - S$, $S \cup \{u\}$ is algebraically dependent.*

We will then define the *transcendental degree* to be the cardinality of a transcendental basis (in a analogue of dimension). In order to show that this is well-defined. We need to work harder.

Proposition 3.14.6. *Let $S \subset F$ be an algebraically independent set over K and $u \in F - K(S)$. Then $S \cup \{u\}$ is algebraically independent if and only if u is transcendental over $K(S)$.*

Proof. The proof is straightforward. □

Corollary 3.14.7. *S is a transcendental basis of F/K if and only if $F/K(S)$ is algebraic.*

Proof. Suppose that S is a transcendental basis of F/K. If $u \in F - K(S)$, then $S \cup \{u\}$ is not algebraically independent. Thus, u is algebraic over $K(S)$ by the Proposition.

On the other hand, suppose that $F/K(S)$ is algebraic. Then for all $u \in F - S$, u is algebraic over $K(S)$. By the Proposition, $S \cup \{u\}$ is algebraically dependent if $u \in F - K(S)$. In fact, it's easy to see directly that $S \cup \{u\}$ is algebraically dependent if $u \in K(S)$. Thus S is a maximal algebraically independent set. □

Corollary 3.14.8. *Let $S \subset F$ be an subset over such that $F/K(S)$ is algebraic. Then S contains a transcendental basis.*

Proof. By Zorn's Lemma, there exists a maximal algebraically independent subset $S' \subset S$. Then $K(S)$ is algebraic over $K(S')$ and hence F is algebraic over $K(S')$. □

Theorem 3.14.9. *Let S, T be transcendental bases of F/K. If S is finite, then $|T| = |S|$.*

Proof. Let $S = \{s_1, ..., s_n\}$ and $S' := \{s_2, ..., s_n\}$. We first claim that there is an element $t \in T$, say $t = t_1$ such that $\{t_1, s_2, ..., s_n\}$ is a transcendental basis.

to see this, if every element of T is algebraic over $K(S')$, then F is algebraic over $K(T)$ hence over $K(S')$ which is a contradiction. Thus, there is an element $t \in T$, say $t = t_1$ such that t_1 is transcendental over $K(S')$. And hence $T' := \{t_1, s_2, ..., s_n\}$ is algebraically independent.

By the maximality of S, one sees that s_1 is algebraic over $K(T')$. It follows that F is algebraic over $K(t_1, s_1, ..., s_n)$ and hence algebraic over $K(T')$. Therefore, T' is a transcendental basis.

By induction, one sees that there is a transcendental basis $\{t_1, ..., t_n\} \subset T$. Thus $T = \{t_1, ..., t_n\}$. □

Theorem 3.14.10. *Let S,T be transcendental bases of F/K. If S is infinite, then $|T| = |S|$.*

Proof. By the previous theorem, we may assume that T is infinite as well.

For $s \in S$, we have $s \in F$ hence algebraic over $K(T)$. Let $T_s \subset T$ be the subset of T of elements that appearing in the minimal polynomial of s. It's clear that $T_s \neq \emptyset$ otherwise, s is algebraic K which is not the case. Also note that T_s is finite.

Let $T' := \cup_{s\in S} T_s$. We claim that $T' = T$. To this end, one sees that for $u \in F$, u is algebraic over $K(S)$ and hence algebraic over $K(T')$. Thus $F/K(T')$ is algebraic. T is a transcendental basis, hence $T = T'$.

Lastly, one sees that

$$|T| = |T'| = | \cup_{s\in S} T_s| \leq |S| \cdot \aleph_0 = |S|.$$

Replace S by T, one has $|S| \leq |T|$. We are done. □

With these two theorem, we can define the transcendental degree of an extension. And the definition is independent of choices of basis.

Definition 3.14.11. *Let F/K be an extension and S be a transcendental basis. We define the transcendental degree of F/K, denoted* tr.d.F/K*, to be $|S|$.*

Theorem 3.14.12. *Let F/E and E/K be extensions. Then*

$$\text{tr.d.}F/K = \text{tr.d.}F/E + \text{tr.d.}E/K.$$

Proof. Let T be a transcendental basis of F/E and S be a transcendental basis of E/K. We would like to show that $S \cup T$ is a transcendental basis of F/K. Note that $T \cap E = \emptyset$, hence $S \cap T = \emptyset$. Thus $|S \cup T| = |S| + |T|$, and we are done.

To see the claim, it's easy to check that $E(T) = EK(S \cup T)$. Hence $E(T)/K(S \cup T)$ is algebraic if $E/K(S)$ is algebraic. Also, $F/E(T)$ is algebraic, therefore, $F/K(S \cup T)$ is algebraic.

It suffices to show that $S \cup T$ is algebraically independent. Suppose that there is $f(x_1, ..., x_n, y_1, ..., y_m)$ such that $f(s_1, ..., s_n, t_1, ..., t_m) = 0$. We can write

$$f(x_1, ..., x_n, y_1, ..., y_m) = \sum_I h_I(x_1, ..., x_n)y^I,$$

and we have $\sum_I h_I(s_1, ..., s_n)t^I$. Since T is algebraically independent over $E \ni h_I(s_1, ..., s_n)$. It follows that $h_I(s_1, ..., s_n) = 0$ for all I. Since S is algebraically independent over K, if follows that $h_I(x_1, ..., x_n) = 0 \in K[x_1, ..., x_n]$ for all I. Therefore $f(x_1, ..., x_n, y_1, ..., y_m) = 0$. Hence $S \cup T$ is algebraically independent. □

Example 3.14.13.

Let $V := \{(a, b)|a^3 = b^2, a, b \in K\}$. Then "polynomial function on V can be described as $R := K[x, y]/(y^2 - x^3)$. And rational functions on V is nothing but the field of quotient of R, denoted F. Then $\text{tr.d.}_K F = 1$, which is the same as the "dimension of V". □

Some related problems:

1. Lüroth's theorem and rationality problem.
The Lüroth's theorem states that a non-trivial subfield of $k(x)$ is of the form $k(t)$, where $t \in K(x)$. More generally, one can ask a subfield $E \subset K(x, y)$ of $\mathrm{tr.d_K} = 2$ is purely transcendental or not. One can prove that this is true when $K = \mathbb{C}$ by geometric method. However, this is not true in general when transcendental degree is higher.

Nevertheless, suppose that there is a finite group G acts on $k(x_1, ..., x_n)$. One can ask whether the subfield of invariant purely transcendental or not. Or under what condition, the field of invariant is purely transcendental. A variety (as V above) is called **rational** if its rational function field is purely transcendental. So this is called **rationality problem**.

2. Automorphism of function fields.
Consider $F = K(x)$. It's well-known that $\mathrm{Aut}_K(F) = PGL(2, K)$. How about K-automorphism $F = K(x_1, ..., x_n)$?

3. Characterize birational invariants.
Varieties as said to be birational if their function fields are isomorphic. Therefore, those birational invariant, which reflect the birational geometry of varieties, are invariant of fields. Can you read it from the fields?

4. Homological Algebra

Some useful references:
Serge Lang,*Algebra*, GTM 211, Springer
S. Gelfand, Y. Manin, *Methods of homological algebra*, Springer
David Eisenbud, *Commutative algebra*, GTM 150, Springer

4.1. **categories and functors.**

In this section, we are going to define some basic notions.

Definition 4.1.1. *A* **category** *is a class* $\mathcal{C}$ *of objects, denoted* $A, B, C, ...,$ *etc., together with*

(1) *a class of disjoint set, denoted* $\mathrm{Hom}_{\mathcal{C}}(A, B)$*, called* **morphism** *and*
(2) *for each triple* (A, B, C) *of objects a function* $Hom(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C)$*, called the* **composition** *subjects to*
  (a) $h \circ (g \circ f) = (h \circ g) \circ f$*.*
  (b) *for each object* $A \in \mathcal{C}$*, there exists* $\mathbf{1}_A \in \mathrm{Hom}(A, A)$ *such that* $\mathbf{1}_A \circ f = f, f \circ \mathbf{1}_A = f$*.*

Example 4.1.2.

(1) The category of Sets, denoted *Set*.
(2) The category of groups, denoted *Gp*, is a subcategory of *Set*.
(3) The category of abelian groups, denoted *Ab*, is a subcategory of *Gp*.

Definition 4.1.3. *Let* $\mathcal{C}, \mathcal{D}$ *be categories. A covariant functor (resp. contravariant functor)* F *of* $\mathcal{C}$ *to* $\mathcal{D}$ *is a rule which to each object* $A \in \mathcal{C}$ *associate an object* $F(A) \in \mathcal{D}$*, and to each morphism* $f : A \to B$ *associate a morphism* $F(f) : F(A) \to F(B)$ *(resp.* $F(f) : F(B) \to F(A)$*) such that:*

(1) $F(\mathbf{1}_A) = \mathbf{1}_{F(A)}$*.*
(2) $F(g \circ f) = F(g) \circ F(f)$ *(resp.* $F(g \circ f) = F(f) \circ F(g)$*).*

There are many cases we met the *universal property*. This can be seen via the universal object in a suitable category.

Definition 4.1.4. *In a category* $\mathcal{C}$*, an object* P *is said to be universally attracting (resp. repelling) if* $\mathrm{Hom}(A, P)$ *(resp.* $\mathrm{Hom}(P, A)$*) has only one element for all* $A \in \mathcal{C}$*.*

Example 4.1.5.

The group of one element is the universally repelling and attracting object in *Gp*.

Example 4.1.6.

Fixed a set S. Let $\mathcal{C}$ be the category of maps form S to abelian groups. The free abelian group is the universally repelling object.

Similarly, if we consider the category of maps from S to groups. Then we get free group by considering the universal repelling object. □

Example 4.1.7.

In a category $\mathcal{C}$, the product of A, B can be defined as (P, f, g) consisting of an object P and $f : P \to A$, $g : P \to B$ such that for any (C, s, t), there exist a unique $h : C \to P$, which makes the diagram commute.

In other words, let $\mathcal{D}$ be the category of the triple (C, s, t), then P is nothing but the universal attracting object. □

We now formulate the axioms of **additive category** and **abelian category**.

A1. $\mathrm{Hom}(A, B)$ is an abelian group. And composition is bilinear.

A2. There exist a zero object 0, i.e. such that $\mathrm{Hom}(0, A), \mathrm{Hom}(A, 0)$ has precisely one element.

A3. Finite direct sum and finite direct product exist. In other words, for $A_1, A_2 \in \mathcal{C}$, there exist an object $C \in \mathcal{C}$ and $p_i : C \to A_i$, $\imath_i : A_i \to C$ such that $p_i\imath_i = \mathbf{1}_{A_i}$, $p_i\imath_j = 0$ if $i \neq j$, $\imath_1 p_1 + \imath_2 p_2 = \mathbf{1}_C$.

A4. For any morphism $f : A \to B$, there exist a sequence, called a *canonical decomposition*

$$K \xrightarrow{k} A \xrightarrow{\imath} I \xrightarrow{\jmath} B \xrightarrow{c} K'$$

such that

(1) $\jmath \circ \imath = f$
(2) K is the kernel of f and K' is the cokernel of f.
(3) I is cokernel of k and kernel of c.

In the above canonical decomposition, K can be viewed as kernel, I as the image and K' as the cokernel.

Definition 4.1.8. *A category satisfying $A1, A2, A3$ is called an additive category. An additive category satisfying $A4$ is called an abelian category.*

Remark 4.1.9. *The kernel and cokernel should be defined abstractly. For example, given $A \in \mathcal{C}$, one can define a functor $h_A : \mathcal{C}^\circ \to Set$ such that $h_A(C) = \mathrm{Hom}(C, A)$. A functor F is* **representable** *by B is $F \cong h_B$.*

In an additive categoty $\mathcal{C}$, for a morphism $f : A \to B$, one can define a kernel functor $Ker(f) : \mathcal{C}^\circ \to Ab$ such that $Ker(f)(C) = Ker(h_A(C) \to h_B(C))$.

We say that kernel of f exists if the functor $Ker(f)$ is representable.

Cokernel can be defined similarly but a little bit subtle. It's $ker(f^\circ)^\circ$.

Example 4.1.10.

The followings are abelian categories:

(1) *Ab*.
(2) category of R-modules, where R is a ring.
(3) category of finite dimensional vector space over k.
(4) category of sheaves of abelian groups over a topological space.

□

4.2. **complexes, examples of homology and cohomology groups.** There are various situation where we need to consider a sequence of abelian group. This is basically why homological algebra arise.

Definition 4.2.1. *Let $\mathcal{A}$ be an abelian category. A comlpex $K^\bullet = (K^i, d_i)_{i\in\mathbb{Z}}$ consists of $K^i \in \mathcal{A}$, $d^i : K^i \to K^{i+1}$ such that $d^{i+1}d^i = 0$ for all i.*

A complex is said to be exact if $\ker(d^{i+1}) = \mathrm{im}(d^i)$.

Example 4.2.2 (Homology of simplicial complex)**.**

Given a simplicial complex X, we can view it as $\cup X_n$, where X_n denotes the n-skeleton. To each n, we attach a free abelian C_n on n-simlpex. Note that there is a natural *boundary map* ∂_n from a n-complex to $(n-1)-$ complex. Note that one need to handle signs by considering the orientation. It follows that $\partial \circ \partial = 0$. Hence we have a complex of free abelian groups (C_n, ∂).

The homology can be considered as the obstruction of this complex being exactness. That is, $H_i(X, \mathbb{Z}) := \ker(\partial_n)/\mathrm{im}(\partial_{n-1})$.

For example, the homology of S^2 can be realized by

$$0 \to \mathbb{Z}[f] \to \mathbb{Z}[e_1] \oplus \mathbb{Z}[e_2] \to \mathbb{Z}[x_1] \oplus \mathbb{Z}[x_2] \oplus \mathbb{Z}[x_3] \to 0.$$

And $\partial[f] = [e_1] + [e_2] - [e_2] - [e_1], \partial[e_1] = [x_2] - [x_1], \partial[e_2] = [x_3] - [x_2], \partial[x_i] = 0$. Therefore, $H_2(S^2) \cong \mathbb{Z}$, $H_1 \cong 0$, $H_0 \cong \mathbb{Z}$. □

Exercise 4.2.3. *compute the homology of $S^n, \mathbb{RP}^2, T^2$ and Klein bottle.*

Example 4.2.4.

[differential forms, De Rham complex and cohomology] Let X be a differentiable manifold, e.g $\mathbb{R}^n$. Let C^i be the vector space of $\mathcal{C}^\infty$ i-forms on X. There is the natural differential $d : C^i \to C^{i+1}$. Then we have a complex (C^i, d), called the de Rham complex. Similarly, we have de Rham cohomology $H^i := \ker(d^i)/\mathrm{im}(d^{i-1})$. □

Example 4.2.5 (Koszul complex, free resolution)**.**

Given a ring $R = k[x, y, z, w]/(xz - y^2, xw - yz, yw - z^2)$. How can we realize it via describing generators and relations?

Let $S = k[x, y, x]$, then there is an exact sequence

$$0 \to \oplus S^2 \to \oplus^3 S \overset{(xz-y^2, xw-yz, yw-z^2)}{\longrightarrow} S \to R \to 0.$$

So the ring R can be realized as the complex of free modules. This is an example of so-called *free-resolution*. □

What we would like to do is more or less the algebraic structure needed for this kind of situation.

Jan. 5, 2007

4.3. **complexes, exact sequences.** .

Definition 4.3.1. *By a short exact sequence, we mean an exact sequence* $0 \to A \to B \to C \to 0$.

Example 4.3.2.

1. Let A, B be abelian groups, then we have exact sequence:

$$0 \to A \overset{\imath_A}{\to} A \oplus B \overset{p_B}{\to} B \to 0.$$

2. Let $A \lhd B$ be abelain groups, then we have exact sequence:

$$0 \to A \to B \to B/A \to 0.$$

3. Let $\varphi : B \to C$ be a surjective homomorphism, then we have exact sequence:

$$0 \to \ker(\varphi) \to B \to C \to 0.$$

□

Given a long exact sequence $K^\bullet = (K^i, d_i)$, it can be decomposed into short exact sequences

$$0 \to \ker(d^i) = \mathrm{im}(d^{i-1}) \to K^i \to \mathrm{im}(d^i) = \ker(d^{i+1}) \to 0.$$

Therefore, short exact sequences play the most important role in our studies.

Given a morphism $\phi \in \mathrm{Hom}(K^\bullet, L^\bullet)$ of complexes, one can define its kernel, image, cokernel, in a natural way. Thus we can formulate a new category $Kom(\mathcal{A})$, whose objects are complexes over $\mathcal{A}$ and morphisms are morphism of complexes.

Exercise 4.3.3. *$Kom(\mathcal{A})$ is an abelian category in which $\mathcal{A}$ is a subcategory.*

Let $K^\bullet$ be a complex. We let $Z^i := \ker(d^i)$, called the **i-th cocycle** and $B^i := \mathrm{im}(d^{i-1})$, called the **$i$-th coboundary**. Then $H^i(K^\bullet) := Z^i/B^i$ is called the **i-th cohomology** of $K^\bullet$. Cohomology can be viewed as a tool detecting the non-exactness of complexes.

Given two complexes $K^\bullet, L^\bullet$, a morphism of complexes $\phi \in Hom_{\mathcal{A}}(K^\bullet, L^\bullet)$ consists of morphisms $\phi^i : K^i \to L^i$ such that $\phi^{i+1} \circ d^i_K = d^i_L \circ \phi^i$ for all i. Another way to put it is the following diagram commute:

$$\begin{tikzcd}
{} \arrow[r] & K^i \arrow[r, "d^i_K"] \arrow[d, "\phi^i"'] & K^{i+1} \arrow[r] \arrow[d, "\phi^{i+1}"'] & {} \\
{} \arrow[r] & L^i \arrow[r, "d^i_L"] & L^{i+1} \arrow[r] & {}
\end{tikzcd}$$

One can easily checked that there is an induced map $H^i(\phi) : H^i(K^\bullet) \to H^i(L^\bullet)$ for all i. Moreover, if ϕ, ψ are morphism of complexes, then $H^i(\psi) \circ H^i(\phi) = H^i(\psi \circ \phi)$ for all i whenever it make sense.

Before we move on, we discuss the following useful lemmas:

Lemma 4.3.4 (Snake Lemma). *Given a diagram*

$$\begin{tikzcd}
 & A' \arrow[r, "f"] \arrow[d, "d'"'] & A \arrow[r] \arrow[d, "d"'] & A'' \arrow[r] \arrow[d, "d''"'] & 0 \\
0 \arrow[r] & B' \arrow[r] & B \arrow[r, "g"] & B'' &
\end{tikzcd}$$

with each rows are exact. Then there is a well-defined map $\delta : \ker(d'') \to \operatorname{coker}(d')$ *such that we have an exact sequence*

$$\ker(d') \xrightarrow{f} \ker(d) \to \ker(d'') \xrightarrow{\delta} \operatorname{coker}(d') \to \operatorname{coker}(d) \xrightarrow{\bar{g}} \operatorname{coker}(d'').$$

If moreover that $f : A' \to A$ *is injective, then* $f : \ker(d') \to \ker(d)$ *is injective. And if* $g : B \to B''$ *is surjective, then* $\bar{g} : \operatorname{coker}(d) \to \operatorname{coker}(d'')$ *is surjective.*

Proof. The proof consists of various diagram chasing. We leave it to the reader. □

Corollary 4.3.5. *Keep the notation as above. If both* d', d'' *are injective (resp. surjective) then so is* d.

Assume that f *is injective and* g *is surjective. If any two of* d', d, d'' *are isomorphism. So is the third one.*

Lemma 4.3.6 (Five Lemma). *Given a diagram*

$$\begin{tikzcd}
A_1 \arrow[r] \arrow[d, "d_1"'] & A_2 \arrow[r] \arrow[d, "d_2"'] & A_3 \arrow[r] \arrow[d, "d_3"'] & A_4 \arrow[r] \arrow[d, "d_4"'] & A_5 \arrow[d, "d_5"'] \\
B_1 \arrow[r] & B_2 \arrow[r] & B_3 \arrow[r] & B_4 \arrow[r] & b_5
\end{tikzcd}$$

with each rows are exact.

If d_1 *is surjective (resp. injective) and* d_2, d_4 *are injective (resp. surjective), then* d_3 *is injective (resp. surjective).*

In particular, if d_1, d_2, d_4, d_5 *are isomorphic, then so is* d_3.

Proof. Decompose the sequence into short exact sequences. □

An immediate application is the following:

Proposition 4.3.7. *Given an exact sequence* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$, *the following are equivalent:*

(1) *there is* $h : C \to B$ *such that* $gh = \mathbf{1}_C$.
(2) *there is* $l : B \to A$ *such that* $lf = \mathbf{1}_A$.
(3) *the sequence is isomorphic to* $0 \to A \xrightarrow{\imath_A} A \oplus C \xrightarrow{p_C} C \to 0$.

Such sequence is called **split**.

If the sequence split, then in particular, $B \cong A \oplus C$.

Proof. Given $h : C \to B$, we can construct the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & A \arrow[r, "\imath_A"] \arrow[d, "\mathbf{1}_A"'] & A \oplus C \arrow[r, "p_C"] \arrow[d, "fp_A + hp_C"'] & C \arrow[r] \arrow[d, "\mathbf{1}_C"'] & 0 \arrow[d] \\
0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0
\end{tikzcd}$$

By Five Lemma, $fp_A + hp_C$ is an isomorphism. Hence those two sequences are isomorphic.

On the other hand, if the two sequence are isomorphic. That is we have the following commutative diagram, which is invertible:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\imath_A"] \arrow[d, "\mathbf{1}_A"'] & A \oplus C \arrow[r, "p_C"] \arrow[d, "\phi"'] & C \arrow[r] \arrow[d, "\mathbf{1}_C"'] & 0 \\
0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0
\end{tikzcd}$$

Let $h = \phi \circ \imath_C : C \to B$, then $gh = g\phi\imath_C = \mathbf{1}_C p_C \imath_C = \mathbf{1}_C$.

The proof for other equivalence is similar. □

Theorem 4.3.8. *Given a short exact of complexes, then it induces a long exact sequences of cohomology.*

Proof. This can be proved directly, or by Snake Lemma.

We briefly sketch the proof by using Snake Lemma here.

First look at the diagram

$$\begin{tikzcd}
0 \arrow[r] & A^{i-1} \arrow[r] \arrow[d] & B^{i-1} \arrow[r] \arrow[d] & C^{i-1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A^i \arrow[r] & B^i \arrow[r] & C^i \arrow[r] & 0
\end{tikzcd}$$

Then we have exact sequence $A^i/B^i(A^\bullet) \to B^i/B^i(B^\bullet) \to C^i/B^i(C^\bullet) \to$ 0 by looking at cokernel of the maps.

Next we look at the diagram

$$\begin{tikzcd}
0 \arrow[r] & A^{i+1} \arrow[r] \arrow[d] & B^{i+1} \arrow[r] \arrow[d] & C^{i+1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A^{i+2} \arrow[r] & B^{i+2} \arrow[r] & C^{i+2} \arrow[r] & 0
\end{tikzcd}$$

Then we have exact sequence $0 \to Z^{i+1}(A^\bullet) \to Z^{i+1}(B^\bullet) \to Z^{i+1}(C^\bullet)$ by looking at kernels.

These two exact sequences fit into a commutative diagram

$$\begin{tikzcd}
& A^i/B^i(A^\bullet) \arrow[r] \arrow[d, "\bar{d}^i_A"'] & B^i/B^i(B^\bullet) \arrow[r] \arrow[d] & C^i/B^i(C^\bullet) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Z^{i+1}(A^\bullet) \arrow[r] & Z^{i+1}(B^\bullet) \arrow[r] & Z^{i+1}(C^\bullet) &
\end{tikzcd}$$

One can check that $\ker(\bar{d}^i_A) = H^i(A^\bullet)$ and $\operatorname{coker}(\bar{d}^i_A) = H^{i+1}(A^\bullet)$. And similarly for $B^\bullet$ and $C^\bullet$. Hence by Snake Lemma, we are done. □

Definition 4.3.9. *Let $F : \mathcal{A} \to \mathcal{B}$ be a functor between two abelian categories. We say that F is* **exact** *if for an exact sequence $K^\bullet$ over over $\mathcal{A}$, $F(K^\bullet)$ is exact over $\mathcal{B}$.*

Exercise 4.3.10. *Show that F is exact if and only if for any short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{A}$, the induced sequence $0 \to F(A) \to F(B) \to F(C) \to 0$ is exact in $\mathcal{B}$.*

Definition 4.3.11. *Keep the notation as above. We say that F is left-exact (resp. right-exact) if for any short exact sequence $0 \to A \to B \to C \to 0$ in $\mathcal{A}$, the induced sequence $0 \to F(A) \to F(B) \to F(C)$ (resp. $F(A) \to F(B) \to F(C) \to 0$) is exact in $\mathcal{B}$.*

Unfortunately, most natural functors are left-exact (or right-exact) but not exact. We list some of them:

Example 4.3.12.

Let X be a topological space. Let Sh_X be the category of sheaves on X, which is an abelian category. The global section functor $\Gamma(X, \cdot) : Sh_X \to Ab$ is left exact but not exact. □

Example 4.3.13.

Let Ab be the category of abelian groups. Fixed $M \in Ab$, we consider $\mathrm{Hom}(M.\cdot) : Ab \to Ab$ by $A \mapsto \mathrm{Hom}(M, A)$. This is left-exact but not right exact. □

It is natural to ask what the defect of these functors. Which will be realized in the next section

Jan. 12, 2007

4.4. **injective.** In this section, we are going to define injective objects. Then one has injective resolution if the category has enough injectives. Moreover, we will see that injective resolution are convenient for handling left exact but not exact functors.

Definition 4.4.1. *Let $\mathcal{A}$ be an abelian category. An object $I \in \mathcal{A}$ is injective if for all $0 \to A \to B$ and $A \to I$, there exists $B \to I$ makes the diagram commute.*

Proposition 4.4.2. *I is injective if and only if the functor $M \mapsto Hom_{\mathcal{A}}(M, I)$ is exact.*

Proof. For every exact sequence $0 \to A \to B \to C \to 0$, we have exact sequence

$$\mathrm{Hom}(A, I) \leftarrow \mathrm{Hom}(B, I) \leftarrow \mathrm{Hom}(C, I) \leftarrow 0.$$

The definition of injective says nothing more than that $\mathrm{Hom}(B, I) \to \mathrm{Hom}(A, I)$ is surjective. □

Exercise 4.4.3. *If I is injective, then every sequence $0 \to I \to B \to C \to 0$ splits.*

An abelian category $\mathcal{A}$ is said to have **enough injectives** if for every $A \in \mathcal{A}$, there exist an injective object $I \in \mathcal{A}$ and an injection $0 \to A \to I$.

Suppose now that $\mathcal{A}$ has enough injectives. Then for every $A \in A$, one has $0 \to A \xrightarrow{\imath} I^0$ for some injective I^0. Next look at $\mathrm{coker}(\imath)$, one has $0 \to \mathrm{coker}(\imath) \to I^1$ for some injective I^1 and let $d^0 : I^0 \to I^1$ be the composition map. Inductively, we obtained a sequence

$$0 \to A \to I^0 \to I^1 ...$$

It's easy to see that it's an exact sequence because it patches short exact sequences $0 \to \mathrm{coker}(\imath_{j-1}) \xrightarrow{\imath_j} I^j \to \mathrm{coker}(\imath_j) \to 0$.

Before we move on, it worthwhile to think what indeed injective object is and why we expect an abelian category has enough injectives.

Let *Ab* be the abelian category of abelian groups. A group G is said to be **divisible** if $m : G \to G$ by $m : x \mapsto mx$ is surjective for all $m \neq 0 \in \mathbb{Z}$. In other words, for $x \in G$, and for all $m \neq 0 \in \mathbb{Z}$, there is $y \in G$ such that $ny = x$. We will show that in *Ab*:

Lemma 4.4.4. *G is divisible, then G is injective.*

Lemma 4.4.5. *Every abelian group can be embedded into a divisible group.*

Thus the abelian category *Ab* has enough injective. It also follows that those natural abelian categories, such as category of R-modules, category of sheaves of abelian groups, has enough injective.

In order to prove the Lemmata, we observe that:

(1) if G is divisible, so if G/N for any normal subgroup N.
(2) if G_i are divisible for all i, then $\sum_{i\in I} G_i$ is divisible.

proof of 4.4.4. Suppose that G is divisible and $0 \to A' \to A$ is exact with a map $f' : A' \to G$. We need to show that there is $f : A \to G$ extending f'.

We shall use Zorn's Lemma. Let $\Sigma = \{(B, g) | A' < B < A, g : B \to G, g|_{A'} = f'\}$. There exists a maximal element (M, h) in Σ. One verifies that $M = A$. □

proof of 4.4.5. $G \cong F/K$, $F \cong \sum_{x\in I} \mathbb{Z}x$. $F \overset{f}{\hookrightarrow} \sum_{x\in I} \mathbb{Q}x$. $G \cong F/K \cong f(F)/f(K) < \sum_{x\in I} \mathbb{Q}x/f(K)$ is divisible. □

Lemma 4.4.6. *Let $I^\bullet$ be an injective resolution of A and $J^\bullet$ an injective resolution of B. If there is $\varphi : A \to B$, then there exists $f : I^\bullet \to J^\bullet$ compatible with φ.*

Moreover any two such $f, g : I^\bullet \to J^\bullet$ are homotopic.

Definition 4.4.7. *$f, g \in \operatorname{Hom}(K^\bullet, L^\bullet)$ are homotopic if there are $h^i : K^i \to L^{i-1}$ such that $d_L h + h d_K = f - g$.*

Injective resolution is very useful in the study of left exact functors which is not exact. More, precise the following Lemma show that injective rsln splits

Lemma 4.4.8. *Given $0 \to A \to B \to C \to 0$, there is an exact sequence of complexes $0 \to I^\bullet \to J^\bullet \to K^\bullet \to 0$ such that $I^\bullet$ (resp, $J^\bullet, K^\bullet$) is an injective resolution of A (resp. B, C). Moreover, $J^i = I^i \oplus K^i$.*

Proof. We define I^0, K^0 first. Then there is a natural map $B \to J^0 := I^0 \oplus K^0$. This map is injective.

Then inductively, we get the resolutions. □

Warning: J is not $I \oplus K$ as complex. For example, the map $I^0 \oplus K^0 \to I^1 \oplus K^1$ is of the form $(d_I(i^0) + *, d_K(k^0))$ where $*$ is not necessarily zero.

We are now ready to study the left-exact functors. Apply F to

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & I^\bullet \arrow[r] & J^\bullet \arrow[r] & K^\bullet \arrow[r] & 0
\end{tikzcd}$$

We get

$$\begin{tikzcd}
0 \arrow[r] & F(A) \arrow[r] \arrow[d] & F(B) \arrow[r] \arrow[d] & F(C) \arrow[d] & \\
0 \arrow[r] & F(I^\bullet) \arrow[r] & F(J^\bullet) \arrow[r] & F(K^\bullet) \arrow[r] & 0
\end{tikzcd}$$

Notice that the bottom row is exact because $J^i = I^i \oplus K^i$ by our construction, hence $F(J^i) = F(I^i) \oplus F(K^i)$ for all i.

Proposition 4.4.9. *Let $R^iF(A) := H^i(F(I^\bullet))$. Then we have:*

(1) $R^0F(A) = A$.
(2) *there is a long exact sequence*

$$0 \to F(A) \to F(B) \to F(C) \to R^1F(A) \to R^1F(B) \to ...$$

Proof. It's easy to see that $\ker(F(I^0) \to F(I^1)) \cong F(A)$ by the left exactness. And the second statement follows from the long exact sequence of cohomology of short exact sequence of complexes. □

Exercise 4.4.10. *Show that $R^iF(A)$ is well-defined. That is, independent of choice of injective resolution.*

4.5. **derived category.** In this section, we are going to describe derived category briefly. It's a category over which cohomology theory can be defined and convenient to operate.

Exercise 4.5.1. *If h is homotopic to 0, denoted $h \sim 0$, then $fh \sim 0$, $hg \sim 0$ for all f, g whenever it makes sense.*

So we can think of the class of homotopic equivalence as an ideal.

Let $\mathcal{K}(\mathcal{A})$ be the category whose objects are complex in $\mathcal{A}$ and morphisms are morphism in $\mathcal{A}$ quotient homotopic equivalence. More precisely, $\mathrm{Hom}_{\mathcal{K}(\mathcal{A})}(K^\bullet, L^\bullet)$ consists of homotopic equivalent class of $\mathrm{Hom}_{Kom(\mathcal{A})}(K^\bullet, L^\bullet)$.

Then in $\mathcal{K}(\mathcal{A})$, injective resolution is unique (up to isomorphism).

Definition 4.5.2. *Given a complex $K^\bullet = (K^i, d^i_K)$, we define $K[n]^\bullet$ such that $K[n]^i = K^{n+1}, d^i_{K[n]} = (-1)^n d^{n+i}_K$.*

And given a morphism $f : K^\bullet \to L^\bullet$, we define a complex $C(f)^\bullet$, called the **mapping cone of** *f, by $C(f)^i = K^{i+1} \oplus L^i$ and $d^i_C(k^{i+1}, l^i) = (-d^{i+1}_K(k^{i+1}), f(k^{i+1}) + d^i_L(l^i))$.*

Example 4.5.3.

If $K^\bullet = K, L^\bullet = L$, then $C(f) = 0 \to K \to L \to 0$. □

Example 4.5.4.

If $f = 0$, then $C(f) = K^\bullet \oplus L^\bullet$.

Definition 4.5.5. *Given a morphsim $f : K^\bullet \to L^\bullet$, we define a complex $Cyl(f)^\bullet$ such that $Cyl(f)^i = K^i \oplus K^{i+1} \oplus L^i$. And $d^i_{Cyl}(k^i, k^{i+1}, l^i) = (d_K k^i - k^{i+1}, -d_K k^{i+1}, f(k^{i+1}) + d_L l^i)$.*

Theorem 4.5.6. *We have the following diagram*

$$\begin{tikzcd}
 & 0 \arrow[r] & L^\bullet \arrow[r] \arrow[d, "\alpha"'] & C(f)^\bullet \arrow[r, "\delta"] \arrow[d] & K[1]^\bullet \arrow[r] & 0 \\
0 \arrow[r] & K^\bullet \arrow[r, "\bar{f}"] \arrow[d, "="'] & Cyl(f)^\bullet \arrow[r, "\pi"] \arrow[d, "\beta"'] & C(f)^\bullet \arrow[r] & 0 & \\
 & K^\bullet \arrow[r, "f"] & L^\bullet & & &
\end{tikzcd}$$

Such that each row is exact. α, β *are quasi-isomorphisms. Moreover,* $\beta\alpha = \mathbf{1}_L$ *and* $\alpha\beta \sim \mathbf{1}_{Cyl(f)}$.

Proof. All the above maps are the natural ones. One has to check that all the maps indeed gives morphism of complexes and the diagram commutes. We leave the detail to the readers.

The homotopy is defined by $h^i(k^i, k^{i+1}, l^i) = (0, k^i, 0)$. □

Theorem 4.5.7. *Given an exact sequence* $0 \to K^\bullet \to L^\bullet \to M^\bullet \to 0$*, we have the following commutative diagram with each vertical map being quasi-isomorphic.*

$$\begin{tikzcd}
0 \arrow[r] & K^\bullet \arrow[r, "f"] & L^\bullet \arrow[r, "g"] & M^\bullet \arrow[r] & 0 \\
0 \arrow[r] & K^\bullet \arrow[r, "\bar{f}"] \arrow[u] & Cyl(f)^\bullet \arrow[r, "\pi"] \arrow[u, "\beta"] & C(f)^\bullet \arrow[r] \arrow[u, "\gamma"] & 0
\end{tikzcd},$$

where $\gamma(k^{i+1}, l^i) = g(l^i)$.

The second row is called **distinguished triangle**.

Derived category $D(\mathcal{A})$ is the category localizing $\mathcal{K}(\mathcal{A})$ with respect to quasi-isomorphisms. That is, a morphism $\mathrm{Hom}_{D(\mathcal{A})}(X, Y)$ in $D(\mathcal{A})$ is a roof (t, f) where $t : Z^\bullet \to X^\bullet$ is a quasi-isomorphism and $f : Z^\bullet \to Y^\bullet$ is a morphism in $\mathcal{K}(\mathcal{A})$. Then in this setting, a quasi-isomorphism $s : X^\bullet \to Y^\bullet$ has inverse $(s, \mathbf{1}_X) \in \mathrm{Hom}_{D(\mathcal{A})}(Y^\bullet, X^\bullet)$.

Derived category has the universal property that any functor $F : Kom(\mathcal{A}) \to \mathcal{D}$ sending quasi-isomorphism into isomorphism can be uniquely factored through $D(\mathcal{A})$.

Note that a cohomology (homology) theory on $\mathcal{A}$ is nothing but a functor $F : Kom(\mathcal{A}) \to Kom(Ab)$ and thus factors through derived category.