Notes for Graduate Algebra

Ting Gong

Started Aug. 28, 2019, Last revision December 14, 2019

Contents

This is the lecture notes of Prof. Sam Evens in Graduate Algebra in Fall 2019

Chapter 1

Group Theory

1.1 Aug. 28, 2019

1.1.1 Groups

Definition 1.1.1. A *binary operation* on a set S is a map $m : S \times S \to S$. If $a, b \in S$, we write $m(a, b) = a \star b$ or ab or $a \cdot b$. $a \star b \in S$ by definition. We write $(S, \star)$ in place of (S, m).

Definition 1.1.2. A group $(G, \star)$ is a set G with the binary operation $\star$ such that

1. $\forall a, b, c \in G, (a \star b) \star c = a \star (b \star c)$
2. $\exists e \in G$ such that $a \star e = a = e \star a$
3. $\forall a \in G, \exists b \in G$ such that $a \star b = e = b \star a$

Example 1.1.3.

1. $(\mathbb{Z}, +)$, $\mathbb{Z} :=$ integers
2. F be a field, $(F, +) : (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$, etc.

Definition 1.1.4. A group G is abelian if $a \star b = b \star a$.

Notation: For $a_1, \ldots, a_n \in G$, set $a_1, \ldots, a_n = (a_1, \ldots, a_{n-1})a_n$. Associativity implies that the order of the parenthesis is irrelevant

If G is a group, $a \in G$, we write $b \in G$ so that $a \star b = e = b \star a$ as $b = a^{-1}$ in abstract group. In $(\mathbb{Z}, +), a^{-1} = a$.

Proposition 1.1.5 (Cancellation Laws)**.** *Let G be a group, $a, b, c \in G$, then*

(i) $ab = ac$ implies $b = c$

(ii) $ba = ca$ implies $b = c$

Proof. We multiply a^{-1} on the left for (i) and we multiply the same thing on the right for (ii). $\square$

Remark 1.1.6. (i) The identity e in a group G is unique. Indeed suppose $e' \in G$ consider $e = ee' = e'$.

(ii) For each $a \in G$, a^{-1} is unique. Consider cancellation laws.

(iii) $\forall a \in G$, $(a^{-1})^{-1} = a$. Consider multiplication by a^{-1} and use cancellation laws

Notation If G is a group, $a \in G$, for $n > 0$, $a^n = a \dots a$, where we have n factors. $a^0 = 1$. For $n < 0$, $a^{-n} = (a^n)^{-1}$. $a^{m+n} = a^m a^n$, $a^{mn} = (a^m)^n$

Definition 1.1.7. Let G be a group with operation $\star$, a subset H of G is called a *subgroup* if $(H, \star)$ is a group.

Lemma 1.1.8. *Let H be a subset of a group G, the following are equivalent*

(i) H is a subgroup

(ii) H is non-empty and $a, b \in H$ implies $ab^{-1} \in H$

(iii) $e \in H$, $a, b \in H$ implies $ab \in H$, $a \in H$ implies $a^{-1} \in H$

Proof. $(i) \Rightarrow (ii)$ $e \in H$, H is nonempty, then the rest follows.

$(ii) \Rightarrow (iii)$ Let $a \in H$, then $e = aa^{-1} \in H$. $e, a \in H$, then $ea^{-1} \in H$. $a, b \in H$, then $b^{-1} \in H$, then $a(b^{-1})^{-1} \in H$. Thus $ab \in H$

$(iii) \Rightarrow (i)$ If $a, b, c \in H$, then $a, b, c \in G$. So associativity follows. □

Remark 1.1.9. For $n \in \mathbb{Z}$, let $n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$, then $n\mathbb{Z}$ is a subgroup.

Proof. $n = n \times 1 \in n\mathbb{Z}$, so $n\mathbb{Z} \neq \emptyset$. If $a = nk, b = nl$, then $a - b = n(k - l) \in n\mathbb{Z}$. Then apply lemma. □

Proposition 1.1.10. *Let H be a subgroup of $\mathbb{Z}$. Then $H = n\mathbb{Z}$ for a unique $n \in \mathbb{Z}^+$.*

Proof. Assume well ordering principle: any subset S of $\mathbb{Z} \geq 0$ has a minimal element a so that $a \leq b$ for all $b \in S$

Assume division algorithm. If $a, b \in \mathbb{Z}$, $a > 0$, then $\exists q, r \in \mathbb{Z}$ so that $b = qa + r$ with $0 \leq r < a$.

Let H be a subgroup. If $H = \{0\}$, then $H = 0\mathbb{Z}$. Otherwise $\exists a \neq 0$, $a \in H$. Since $-a \in H$, $H \cap \mathbb{Z}^+ \neq \emptyset$. So $H \cap \mathbb{Z}^+ \neq \emptyset$ has a minimal element n. Then $n \in H$. so $n\mathbb{Z} \subset H$ since $nk = n + \dots + n \in H$.

We are going to show $H \subset n\mathbb{Z}$. For this, let $b \in H$. Then by division algorithm, $b = nq + r$ with $0 \leq r < n$. Then $r = b - qn \in H$ since $b, qn \in H, r > 0$ violates the assumption that n is minimal in $H \cap \mathbb{Z}^+ \neq \emptyset$. Therefore, $r = 0$. So $b - qn = 0, b = qn \in n\mathbb{Z}$. □

1.2 Aug. 30, 2019

1.2.1 More on $\mathbb{Z}$

Let $a, b \in \mathbb{Z}$, $a\mathbb{Z} + b\mathbb{Z} = \{ax + by | x, y \in \mathbb{Z}\}$. $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z} : a \in a\mathbb{Z} + b\mathbb{Z}$. If $u = xa + yb, v = x'a + y'b \in a\mathbb{Z} + b\mathbb{Z}$, $u - v = (x - x')a + (y - y')b \in a\mathbb{Z} + b\mathbb{Z}$. Hence $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ where $d = 0$ if $a = b = 0$, and d is minimal in $a\mathbb{Z} + b\mathbb{Z} \cap \mathbb{Z}^+$.

If a, b are not both 0. Write $d = (a, b)$ and call it the greatest common divisor (gcd) of a and b.

Notation: if $m, n \in \mathbb{Z}$, $m \neq 0$, write $m \mid n$ if $n = km, k \in \mathbb{Z}$. Notate: $m \mid n$ if and only if $n \in m\mathbb{Z}$.

Then $d \mid a$. Indeed, $a \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. $d \mid b$ similarly.

If $c \mid a$ and $c \mid b$, then $c \mid d$ so $d \geq c$. Indeed $c \mid a$ implies $ax \in c\mathbb{Z}$. $c \mid b$ implies $by \in c\mathbb{Z}$. Then $c\mathbb{Z}$ is a subgroup implies $ax + by \in c\mathbb{Z}$. Hence $d \in c\mathbb{Z}$ so $c \mid d$

Definition 1.2.1. If $a, b \in \mathbb{Z}$ and $(a, b) = 1$ we say a and b are *relatively prime.*

Note: $(a, b) = 1$ if and only if $\exists x, y \in \mathbb{Z}$ such that $xa + by = 1$

Proposition 1.2.2. *If $a, b, c \in \mathbb{Z}$ and $a \neq 0$, and $a \mid bc$, and $(a, b) = 1$ then $a \mid c$*

Proof. $(a, b) = 1$ implies $1 = ax + by$. Then $c = cax + cby$. To show $c \in a\mathbb{Z}$, $xac \in a\mathbb{Z}$ and $ybc \in a\mathbb{Z}$ since $a \mid bc$. Since $a\mathbb{Z}$ is a subgroup. $c = xac + ybc$, so $a \mid c$. □

Proposition 1.2.3. *Let a, b be not both 0, then $(a/(a, b), b/(a, b)) = 1$.*

Proof. Since $(a, b) = xa + by$. We divide (a, b), then we have $(a/(a, b), b/(a, b)) = 1$. Then by our note, we get what we desired. □

Proposition 1.2.4. *Let $[a, b]$ be the least common multiple of a, b, then $(a, b)[a, b] = ab$.*

1.2.2 Order of elements

Definition 1.2.5. Let G be a group and let $a \in G$, let $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$. Easy to check $\langle a \rangle$ is a subgroup. It is called the cyclic subgroup of G generated by a.

Definition 1.2.6. If H is a group, let $|H|$ be the *order* of H.

Definition 1.2.7. If $a^n \neq e$ for all $n > 0$, we say that the order $|a|$ of a is ∞. If $a^n = e$ for some $n > 0$, we say $|a| = d$, where d is minimal in $\mathbb{Z}^+$ so $a^d = e$.

Note: $\{n \in \mathbb{Z} | a^n = e\}$ is a subgroup of $\mathbb{Z}$. Indeed, $n = 0 \in K$, if $n, m \in K$, $a^n = e = a^m$, so $a^{n-m} = e$, so $n - m \in K$. Hence, K is a subgroup. Now we are going to show $|a| = |\langle a \rangle|$ where $|a| = \infty$ iff $|\langle a \rangle| = \infty$

Proof. Case 1: $|a| = \infty$. We claim that $a^n = a^m$ for $n, m \in \mathbb{Z}$ implies $n = m$. Indeed, let $a^n = a^m$, we can assume $n \geq m$. Then $a^{n-m} = e$, and $n - m \geq 0$. Since $|a| = \infty$ implying $n - m$ is not bigger than 0, $n - m = 0$, which means $n = m$. Hence all elements in $\{a^n | n \in \mathbb{Z}\}$ are distinct so $|\langle a \rangle| = \infty$

Case 2: let $|a| = d < \infty$. let $S = \{e, a \dots a^{n-1}\}$. Then $S = \langle a \rangle$. Indeed, if $a^n \in \langle a \rangle$, then $n = qd + r, 0 \leq r < d$ and $a^n = a^{qd+r} = (a^q)^d a^r = ea^r = a^r \in S$. $S \subset \langle a \rangle$ is clear, so $S = \langle a \rangle$. Let $a^i, a^j \in S$, with $j \geq i$. If $a^i = a^j$, then $a^{j-1} = e$. So $j - i = 0$. Since d is minimal among $n > 0$ with $a^n = e$, hence, S has d distinct elements. So $|S| = |\langle a \rangle| = d$, and $|a| = |\langle a \rangle|$. □

Definition 1.2.8. A group G is cyclic if $G = \langle a \rangle$ for some $a \in G$.

Example 1.2.9. $\mathbb{Z}$ is cyclic. Since $\mathbb{Z} = \langle 1 \rangle$

Note: if $|a| = d$, then $\{n \in \mathbb{Z} | a^n = d\}$ is a subgroup of $\mathbb{Z}$, and $\{n \in \mathbb{Z} | a^n = e\} = d\mathbb{Z}$.

Proposition 1.2.10. *(adaptation of Ash) Let G be a group, $a \in G$, let $a \in G$ has order $d < \infty$. Let $k \in \mathbb{Z}$, then $|a^k| = d/(k, d)$.*

Proof. Certainly $(a^k)^{d/(k,d)} = a^{kd/(k,d)} = (a^d)^{k/(k,d)} = e$. Hence $|a^k| \leq d/(k, d)$. Show $(a^k)^m = e$ then $d/(k, d) \mid m$ so $|a^k| = d/(k, d)$ since $(k, d) \mid k$. Note $d/(k, d) \mid k/(k, d)$. From above we know that $(d/(k, d), k/(k, d)) = 1$ so we have what we desired. □

Proposition 1.2.11. *Let $G = \langle a \rangle$ be a finite cyclic group with n elements. Then $\forall k \mid n, \exists a!$ subgroup H_k of G such that $|H_k| = k$ and $|H_k| = \langle a^{n/k} \rangle$. Every subgroup of G is H_k for some k dividing n.*

Proof. Existence: $|a^{n/k}| = n/(n, k)$ by the last proposition, but $n/k \mid n$ so $n/(n, k) = n/k$. $|a^{n/k}| = k$. Let $H_k = \langle a^{n/k} \rangle$. Then $|H_k| = k$. Let $H \subset G$ be a subgroup, if $H = e$, then $H = \langle a^n \rangle = H_1$. If not, $\exists a^l \in H$ with $0 < l < n$. Choose $m > 0$ minimal so that $a^m \in H$. Then $\langle a^m \rangle$ in H. Show that $H = \langle a^m \rangle$. If $x \in H$, $x = a^l$. $l = qm + r$ with $0 \leq r < m$. Then $a^l = a^{qm+r} = a^{qm} a^r \leq 0$. $a^r = (a^{qm})^{-1} \in H$. By minimality of m, $r = 0$, so $H = \langle a^m \rangle$. Show $m \mid n$. Let $d = (m, n)$, $d = xm + yn$, $x, y \in \mathbb{Z}$. Then $a^d = a^{mx}$ since $a^n = e$. Hence $a^d \in H$ and $d \leq m$. By minimality of m, $m = d$. Therefore $m \mid n$. □

1.3 Sep. 2, 2019

1.3.1 Examples of groups

Definition 1.3.1. A field $(F, +, \cdot)$ is a set with 2 binary operations such that

1. $(F, +)$ is an abelian group
2. $(F', \cdot)$ is a abelian group
3. identity 0 of F is not identity 1 of F

4. $a(b+c) = ab + ac, \forall a, b, c \in F$

Definition 1.3.2. Let F be a field, and let $n > 0$, and let $u_n(F) = \{z \in F | z^n = 1\}$, where 1 is the identity of $(F', \cdot)$, then $u_n(F)$ is a subgroup of F'. $u_n(\mathbb{C}) = \{e^{2\pi ki/n} | k = 1, \ldots, n-1\}$ is defined as the nth roots of unity, where $e^{i\theta} = \cos\theta + i\sin\theta$. Then the roots of unity in $\mathbb{C}$ is a cyclic group of order n with generator $\zeta = e^{2\pi i/n}$

Definition 1.3.3. The *Orthogonal* group $O(n, F) = \{A \in M(n, F) | A \times A^T = I_n\}$

Notation: Frequently write AB in place of $A \times B$.

Example 1.3.4.
1. $(\mathbb{Z}_n, +)$, where $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ integers mod n. Will assume familarity, carefully later. $(\mathbb{Z}_n, +)$ is cyclic and 1 is the generator

2. Let F be a field $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$. Let $\cdot$ = multiplication on F. Let $F' = F - \{0\}$. Then $(F', \cdot)$ is a group by field axioms

3. Let F be a field, $n \in \mathbb{Z}^+$. $M(n, F)$ is the $n \times n$ matrices with entries in F. $M(n, F)$ is a group under matrix addition.

4. Let $A, B \in M(n, F)$, then $A \times B \in M(n, F)$. Set $GL(n, F) = \{A \in M(n, F) | A$ is invertible$\} = \{A \in M(n, F) | \det(A) \neq 0\}$. Therefore, $(GL(n, F), \times)$ is a group. Check: $A, B \in GL(n, F), A \times B \in GL(n, f)$ since $\det(AB) = \det(A)\det(B)$. If $n \geq 2$, then $GL(n, F)$ is nonabelian. If $|F| = q < \infty$, then $|GL(n, F)| = \prod_{i=0}^{n-1}(q^n - q^i)$. Idea: A is invertible if each column is linearly independent. So choosing a matrix in $GL(n, F)$ is same as choosing an n-tuple of linearly independent vectors. a_1 cannnot be chosen as 0, and a_2 is chosen not to be $F \cdot a_1$ and so on.

5. Let $A \in M(n, F)$. Let A^T =transpose of A. The orthogonal group is a group and is a subgroup of $GL(n, F)$.

1.4 Sep. 4, 2019

If $\det(A) = 1$, then A is a rotation, if $\det(A) = -1$, then A is a reflection. And $s_\alpha = R(\alpha)sR(-\alpha)$.

Definition 1.4.1. If $f : S \to T$ is a map of sets, then f is

(i) Injective: if $f(x_1) = f(x_2) \implies x_1 = x_2$ for $x_1, x_2 \in S$ (one to one)

(ii) Surjective: if $\forall y \in T, \exists x \in S$ such that $f(x) = y$ (Onto)

(iii) Bijective: if f is injective and surjective (one-to-one corespondence).

Lemma 1.4.2. *If $f : S \to T, g : T \to W$ be maps of sets. Define $g \circ f : S \to W$ by $(g \circ f)(x) = g(f(x))$*

1. *f, g injective implies $g \circ f$ injective*

2. f, g surjective implies $g \circ f$ surjective

3. f, g bijective implies $g \circ f$ bijective

4. If f is bijective then there exists $q : T \to S$ such that $f \circ q = q \circ f = x$, q is called the inverse of f.

Definition 1.4.3. $A(S) = \{f : S \to S | f \text{ is bijective}\}$.

Lemma 1.4.4. *$A(S)$ is a group with group operation composition.*

We continue the examples

Example 1.4.5. 6 The regular n-gon T_n is the n-gon with vertices (in polar coordinates $(1, 0), (1, 2\pi/n), \ldots (1, 2\pi(n-1)/n)$. Let the dihedral group $D_{2n} = \{A \in O(2)|$ a maps vertices of T_n to vertices of $T_n\}$. $D_{2n} = \{I, r, r^2, \ldots\} \cap \{s, sr, \ldots\}$. Therefore, the rotations and reflections. $D_{2n} = \{s, r | sr = r^{-1}s, r^n = e, s^2 = e\}$ is a subgroup of $O(2)$.

7 Symmetric Groups: Let S be a set possibly infinite. Let $S = \{1, \ldots, n\}$, $A(S) = S_n$ the symmetric group.

1.5 Sep. 6, 2019

Definition 1.5.1. If $\sigma \in S_n$, $supp(\sigma) = \{i | \sigma(i) \neq i\}$. A k-cycle is an element with $supp(\sigma) = \{i_1, \ldots, i_n\} \in \{1, \ldots, k\}$ such that $\sigma(i_i) = i_2, \ldots, \sigma(i_k) = \sigma(i_1)$. We write the above k-cycle as $(i_1\ i_2\ \ldots i_k)$. We call 2-cycles *transpositions*. A transposition τ is called *simple* if $\tau = (i\ i+1)$ for some $i \in \{1, \ldots, k\}$. If $\sigma, \tau \in S_n$ we say that they are disjoint if $supp(\sigma) \cap supp(\tau) = \emptyset$.

Results:

1. If $\sigma, \tau \in S_n$ are disjoint, then $\sigma\tau = \tau\sigma$.
2. If $\sigma \in S_n$, then σ can be written as a product of disjoint cycles. $\sigma = \sigma_1 \ldots \sigma_k$ where σ is a n-cycle. Further, the cycle decomposition it in a unique way up to reordering.
3. σ is a k-cycle, then $|\sigma| = k$ for this compute $\sigma^k = i$.
4. σ has cycles decomposition $\sigma = \sigma_1 \ldots \sigma_k$, where $l(\sigma) = n$, then $|\sigma| = lcm(n_1, \ldots, n_k)$.
5. if σ is a k-cycle, then $\sigma = (i_1\ i_2) \ldots (i_{k-1}\ i_k)$.
6. if $\sigma \in S_n$, σ is a product of transpositions by 2 and 5.
7. if $\sigma \in S_n$ and $\tau = (i_1 \ldots i_k)$ then $\sigma\tau\sigma^{-1} = (\sigma(i_1) \ldots \sigma(i_k))$
8. $|S_n| = n!$.

1.5.1 Cosets and Homomorphisms

Definition 1.5.2. Let G be a group with subgroup H. If $a \in G$, the *left coset* $aH = \{ax|x \in H\}$, the right coset $Ha = \{xa|x \in H\}$

Let $G/H = \{aH|a \in G\}$, $H\backslash G = \{Ha|a \in G\}$

Definition 1.5.3. For $a \in G$, wite $L_a : G \to G$ for the map $L_a(x) = ax$.

Lemma 1.5.4. *The map $L_a : H \to aH$ is bijective. In fact, $|H| = |aH|$.*

Proof. Let $y \in aH$, so $y = ax$. Then $y = L_a(x)$. So surjective. Injective: let $x_!, x_2 \in H$, $L_a(x_1) = l_a(x_2)$ implies $ax_1 = a_2$, so $x_1 = x_2$. $\square$

Lemma 1.5.5. *Let $a, b \in G$. Then either $aH = bH$ or $aH \cap bH = \emptyset$*

Proof. Suppose $aH \cap bH \neq \emptyset$. Let $y \in aH \cap bH$. Then $y = ax = bz, x, z \in H$. Therefore, $a = bzx^{-1}$, and $zx^{-1} \in H$, then $aH \subset bH$. Interchanging a and b, we get $bH \subset aH$. Therefore, $aH = bH$ $\square$

Notation: Let S be a set with subsets $\{T_i\}$. We say $S = \sqcup T_i$ if $S = \cap T_i$ and $T_i \cap T_j = \emptyset$. Then $|S| = \sum |T|$.

If G is a group with subgroup H and $\{aH|i \in I\}$ are the distinct left cosets, then $G = \sqcup a_i H$. Indeed, if $i \neq j$, $a_i H \neq a_j H$ by distinctness, so $a_i H \cap a_j H = \emptyset$. If $b \in G, b = be \in bH$, then $bH = aH$.

Theorem 1.5.6. *Let G be a group with subgroup $H_i, i \in I$, then $|G/H| = |G|/|H|$, in particular $|H| \mid |G|$.*

Proof. Let $a_1 H, \dots, a_k H$ be the distinct left cosets. By the remark, $G = a_1 \sqcup \dots \sqcup a_k$. Therefore, $|G| = \sum |a_i H| = k|H|$. $\square$

Corollary 1.5.7. *Let G be a finite group and let $a \in G$. Then $|a|/|G|$ and $a^{|G|} = e$.*

Proof. We checked that $|a| = |\langle a \rangle| \mid G$ by Lagrange Theorem. Thus $|G| = n|a|$ so $a^{|G|} = e^n = e$. $\square$

Definition 1.5.8. The index of a subgroup H of G is $|G/H|$. We say the index of H in G is $|G : H|$.

1.6 Sep. 9, 2019

let $n \in \mathbb{Z}^+$, for $a, b \in \mathbb{Z}$, $a \equiv b \mod n$ if $n/(a-b)$ is an equivalence notation, Let $\mathbb{Z}_n$ is an equivalence class $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, n \bar{-} 1\}$. We observe that $(\mathbb{Z}_n^\times, \cdot)$ is a group under multiplication.

Let $\phi(n) = |\mathbb{Z}_n^\times| < n$. If p is prime, $\mathbb{Z}_p^\times = \{\bar{0}, \bar{1}, \dots, p \bar{-} 1\}$. So $\phi(p) = p - 1$.

Corollary 1.6.1. *(Euler's Theorem) If $a \in \mathbb{Z}$ and $(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$. If p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \mod p$.*

Proof. Since $|\mathbb{Z}_n^\times| < n$, then $\mathbb{Z}_n^\times$ implies $\bar{a}^{\phi(n)} \equiv 1 \mod n$. Let $a \in \mathbb{Z}$, p is a prime, then $(a,p) \mid p$, so $(a,p) = 1$ or p. If $(a,p) = p$, then $p \mid a$. if $(a,p) = 1$, then $a^{p-1} \equiv 1 \mod p$. Hence $a^p \equiv a \mod p$. If $p \mid a$, then $a \equiv 0 \mod p$ so $a^p \equiv 0 \equiv a \mod p$. □

1.6.1 Cosetology

Proposition 1.6.2. *Let $H \subset G$ be a subgroup, let $a, b \in G$ then the following are equivalent:*

1. $aH = bH$
2. $b = ax, x \in H$
3. $a^{-1}b \in H$

Proof. $1 \Rightarrow 2$ since $b = be \in bH = aH$, so $b = ax, x \in H$

$2 \Rightarrow 1$ If $b = ax$, then $bH = axH \in aH$ since $x \in H$. so $xH = H$. $aH \cap bH \neq \emptyset$, so $bH = aH$. By Lemma 2 from last time

$2 \Rightarrow 3$ $b = ax, a^{-1}b = a^{-1}ax = x$, similarly for the other direction, □

Similarly for right cosets.

Notation: For $S \subset G$, a subset, and $a \in G$. Let $aS = \{ax | x \in S\}$, and $Sa = \{xa | x \in S\}$

Remark 1.6.3. If $a, b \in G$, S as above, then $a(bS) = (ab)S$, $(Sa)b = S(ab)$, $a(Sb) = (aS)b$

Definition 1.6.4. For G group, H subgroup of G, $[G : H] = |G/H|$ and is called the index of H in G. $[G : H] = \infty$ is allowed.

Proposition 1.6.5. *Let G be a group with subgroup H, K with $K \subset H$, then $[G : K] = [G : H][H : K]$.*

[This follows by Lagrange's Theorem $[G : H] = |G|/|H|$ if G is finite]

Proof. Let $\{a_iH | i \in I\}$ be the distinct left cosets of H in G, $\{b_jK | j \in J\}$ be the distinct left cosets of K in H. $S = \{a_i | i \in I\}$, $T = \{b_j | j \in J\}$. Then we define a map $\phi : S \times T \to G/K$ by $\phi(a_i, b_i) = a_ib_jK$. We claim that ϕ is bijective. Surjective: Let $xK \in G/K$, then $xH \in G/H$, so $xH = a_iH$ for some $i \in I$. By cosetology, $x = a_iy$ for some $y \in H$. Then $yK \in H/K$, then $yK = b_jK$ for some $j \in J$. Then $x = a_ib_jz$, where $y = b_jz, z \in K$. Therefore, $xK = a_ib_jK = \phi(a_i, b_j)$. ϕ is injective: let $\phi(a_i, b_j) = \phi(a_s, b_t), s \in I, t \in J$. Then $a_ib_jK = a_sb_tK$. Therefore, $a_ib_j = a_sb_tz$ for some $z \in K$. so $a_i = a_sb_tzb_j^{-1}$. Thus $a_iH = a_sH$ by cosetology. So $i = s$ by the choice of a_i being distincts of $\{a_iH\}$. Therefore, $a_ib_jK = a_ib_tK$, then $b_jK = b_tK$. Thus $j = t$. □

Definition 1.6.6. A subgroup N of a group G is *normal* if $aNa^{-1} \subset N$ $\forall a \in G$. $aNa^{-1} = \{ana^{-1} | x \in N\}$.

Remark 1.6.7. Let $N \subset G$ be a subgroup, then the following are equivalent

1. N is normal in G
2. $aNa^{-1} = N, \forall a \in G$
3. $aN = Na, \forall a \in G$.

Proof. $2 \Rightarrow 1$ is clear, $3 \Rightarrow 2$ is also clear. $1 \Rightarrow 2$ since $aNa^{-1} \subset N$, thus $aN \subset Na$, $\forall a \in G$. But $a^{-1} \in G$ and $a = (a^{-1})^{-1}$, so $a^{-1}Na \subset N, \forall a \in G$, $\implies aa^{-1}Na \subset aN, Na \subset aN$. □

Example 1.6.8. 1. G is Abelian, then $aH = Ha, \forall$ subgroups H of G, and $a \in G$, so H is normal.

2. $G = D_{2n}, N = \langle r \rangle$. if $g \in G$, and $x \in N$, since $gxg^{-1} \in N$ since $\det(gxg^{-1}) = \det(g)\det(x)\det(g^{-1}) = \det(x)$ since $x \in N$. Therefore, $gxg^{-1} \in N$, since N has determinant 1.

Remark 1.6.9. By problem set 2 number 12, a subgroup of index 2 is normal, so N is $Ex2$ is normal in D_{2n} automatically.

1.7 Sep. 11, 2019

If N is a normal subgroup, we can write G/N into a group. Let $aN, bN \in G/N$ be the left cosets. We'd like to define $aNbN = abN$. To do this, we must ensure abN depends only on aN and bN and not on a, b. Let $aN = a_1N$, $bN = b_1N$. Then $a_1 = ax, b = by, x, y \in N$. Then $a_1b_1N = axbyN$. But $xb \in Nb = bN$, so $xb = bx, x_1 \in N$, thus $a_1b_1N = abxyN = abN$, since $x, y \in N$. Thus is a well defined binary operation on G/N.

Proof that G/N is a group. Everything is ingerited from similar property on G. □

Usually, computing G/N is not transparent.

Example 1.7.1. $G = \mathbb{Z}, N = n\mathbb{Z}.(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is fairly transparent.

Notation: Usually we write $aNbN = aN \cdot bN$.

1.7.1 Group homomorphism

Definition 1.7.2. Let $\phi : G \to H$ be a map between two groups. ϕ is called a group *homomorphism* (hom) if $\phi(xy) = \phi(x)\phi(y)$, $\forall x, y \in G$.

Example 1.7.3. 1. G be a group N normal in G. Define $\pi : G \to G/N$ by $\pi(a) = aN$. π is a group homomorphism. Check $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$.

2. M is a subgroup of G. Define $j : M \to G$, by $j(a) = a$. Clear from defition that j is a group homomorphism.

3. Let $n \in \mathbb{Z}$, define $\phi : \mathbb{Z} \to \mathbb{Z}$ by $\phi(a) = na$. Then ϕ is a group homomorphism. Every group homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}$ is $\phi = \phi_n$ for some n.

4. Let f be a field, define $f : S_n \to GL(n, F)$ as follows, for $\sigma \in S_n$, let $f(\sigma)$ be matrix so that $f(\sigma)(e) = e_{\sigma(i)}$. This determines $f(\sigma)$ uniquely since $e_1, \ldots, e_n$ is a basis of F. This matrix are porentation matrices, exactly one entry of each columns is nonzero and that entry is 1. f is a group homomorphism.

5. $\det : GL(n, F) \to F^\times$, $A \mapsto \det(A)$. This is a group homomorphism since $\det(AB) = \det(A)\det(B), \forall A, B \in GL(n, F)$.

Remark 1.7.4. Let $\phi : G \to H$ be a group hom. Then $\phi(e_G) = e_H$, $\forall a \in G, \phi(a^{-1}) = \phi(a)^{-1}$.

Notation: Let $\phi : G \to H$ be a group. If $X \subset G$, let $\phi(X) = \{\phi(a) | a \in X\}$. If $Y \subset H$ let $\phi^{-1}(Y) = \{a \in G | \phi(a) \in Y\}$, there doesn't exists $\phi^{-1} : H \to G$. We say ϕ is a monomorphism is ϕ is injective. We say ϕ is a epimorphism is ϕ is surjective. We say ϕ is a isomorphism is ϕ is bijective.

Remark 1.7.5. If $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ are group hom's. Then $\psi \circ \phi : G_1 \to G_3$ is a group hom.

Example 1.7.6. Let $G_1 = S_n$, $G_2 = GL(n, F), G_3 = F^\times$. Define $sgn : S_n \to F^\times = \det \circ f$. So sgn is a group hormormophism by remark.

Proposition 1.7.7. *Let $\phi : G \to G_2$ be a group hom.*

Then (i) if $H \subset G_1$ is a subgroupm then phi(H) is a subgroup. If $N \subset G_1$ is a normal subgroup, and ϕ is surjective, then $\phi(N)$ is normal in G_2.

(ii) If $K \subset G_2$ is a subgroup, then $\phi^{-1}(K)$ is a subgroup of G_1, If $N \subset G_2$ is a normal subgroup, and ϕ is surjective, then $\phi^{-1}(N)$ is normal in G_1. (Don't need ϕ to be surjective)

1.8 Sep. 13, 2019

Proposition 1.8.1. *For a group M, $\{e_M\}$ and M are normal subgroups*

Let $\phi : G \to H$ be a group homomorphism

Definition 1.8.2. The image of $im(\phi) = \phi(G) = \{\phi(x) | x \in G\}$. This is a subgroup. The kernel $ker(\phi) = \phi^{-1}(\{e_H\}) = \{x \in G | \phi(x) = e_H\}$. $ker(\phi)$ is a normal subgroup.

Example 1.8.3.

1. Let $SL(n, F) = \{A \in GL(n, F) | \det(A) = 1\}$. $SL(n, F) = ker(\det), \det : GL(n, F) \to F^\times, A \to \det A$. $SL(n, F)$ is normal in $GL(n, F)$ and A_n is normal in S_n.

2. $\pi : \mathbb{Z} \to \mathbb{Z}_n, \pi(a) = a \mod \pi, \pi$ is a group homomorphism and $ker(\pi) = \{n \in \mathbb{Z} | a \equiv 0 \mod n\}$

Proposition 1.8.4. *Let $\phi : G \to H$ be a group homomorphism, then ϕ is injective iff $ker(\phi) = \{e_G\}$*

Proof. $\Rightarrow$ ϕ is injective then $\phi(e_G) = e_H$, then $e_G \in ker(\phi)$ If $x \in ker(\phi)$, $\phi(x) = e_H$, so $\phi(x) = \phi(e_G)$, then $x = e_G$

$\Leftarrow$ Let $x, y \in G$, if $\phi(x) = \phi(y)$, Then $\phi(xy^{-1}) = e_H$, so $xy^{-1} \in ker(\phi) = \{e_G\}$ $\square$

Let S be a set with equivalence relation $\sim$. This means for $a, b, c \in S$, $a \sim a, a \sim b \implies b \sim a, a \sim b, b \sim c \implies a \sim c$. For $a \in S$, let $[a] = \{b \in S | b \sim a\}$ =equivalence class of S. Let $S/\sim = \{[a] | a \in S\}$. If $[a_i]$ and $[a_i]$ are in $S/\sim$, then either $[a_i] \cap [a_j] = \emptyset$ or $[a_i] = [a_j]$. If $\{[a_i] | i \in I\}$ are distinct equivalence classes, then $S = \sqcup [a_i]$. Finally, define $\pi : S \to S/\sim$ by $\pi(a) = [a]$.

For S, T sets, let $Map(S, T) = \{\phi : S \to T | \phi$ is a map$\}$. If $f : R \to S$ is a map, we get $f^\times : Map(S, T) \to (R, T)$. $f^\times(\phi) = \phi \circ f : R \to T$. If $g : T \to U$ is a map, we get $g_\times Map(S, T) \to (S, U)$, $g_\times(\phi) = g \circ \phi$. Idea: $Map(S/\sim, T) = \{\phi \in Map(S, T) | \phi(a) = \phi(b)$ if $a \sim b\} = Map_\sim(S, T)$.

Lemma 1.8.5 (Meta-Lemma)**.** *$\pi^* : Map(S/\sim, T) \to Map(S, T)$ is bijective.*

$S/\sim$ is an example of a quotient. Quotient objects should always have the meta-lemma property.

1.8.1 Factor Theorem

Theorem 1.8.6. *Let G be a group with a normal subgroup N. For groups M, L, let $Hom(M, L) = \{\phi : M \to L | \phi$ is a group hom.$\}$. Let $\pi : G \to G/N$ be $\pi(a) = aN$. Let $Hom_N(G, H) = \{\phi \in Hom(G, H) | \phi(x) = e_H, \forall x \in N\}$. Then $\pi^* : Hom(G/N, H) \to Hom_N(G, H)$ is bijective*

Proof. If $\phi \in Hom(G/N, H), \pi^*\phi : G \to H$ is a group hom. Since $\pi^*(\phi) = \phi \circ \pi$ group hom. If $x \in N, \pi^*(\phi)(x) = e$. By meta lemma, π^* is bijective, π^* is injective if $\chi \in Hom(G, H)$, $\bar{\chi}$ from meta-lemma. Then $\bar{\chi}(aNbN) = \bar{\chi}(abN) = \chi(a)\chi(b) = \bar{\chi}(aN)\bar{\chi}(bN)$. $\square$

Theorem 1.8.7 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a surjective group homomorphism with $ker(\phi) = K$. Then the map $\bar{\phi} : G/K \to H$, $\bar{\phi}(aK) = \phi(a)$ is a group isomorphism. Hence $G/K \cong H$.*

Proof. We know $\bar{\phi}$ is a group homomorphism, $\bar{\phi}$ is surjective if $b \in H, b = \phi(a) = \bar{\phi}(aK)$. $\bar{\phi}$ is injective: let $aK \in \ker(\bar{\phi})$. Then $e_H = \bar{\phi}(aK) = \phi(a)$, so $a \in K$ and $aK = eK = e_{G/K}$. So injective. $\square$

Example 1.8.8. $\phi : \mathbb{R}^\times \to \mathbb{R}^\times$, $\phi(a) = a^2$, ϕ is a group homomorphism. $ker(a) = \{a | a^2 = 1\}$. $im(\phi) = \mathbb{R}_{>0}$. Can replace $\Phi : \mathbb{R}^\times \to \mathbb{R}_{>0}$. So $\mathbb{R}^\times/\{\pm 1\} \cong \mathbb{R}_{>0}$.

More generally, if $\phi : G \to H$ is a group homomorphism, and $K = \ker(\phi)$, then G/K is isomorphic to $im(\phi)$, in particular, $|im(\phi)| = |G|/|K|$, $|G|$ is finite.

1.9 Sep. 16, 2019

Example 1.9.1. 1. F a field, $\det : GL(n, F) \to F^{\times}$. Then $GL(n, F)/SL(n, F) \cong F^{\times}$.

2. Let $sgn : S_n \to \mathbb{R}^{\times}$. Then $S_n/A_n \cong \mathbb{Z}_2$

3. $G = \langle a \rangle$, if $|G| = \infty$, then $G \cong \mathbb{Z}$

4. $G = \langle a \rangle$, if $|G| = n < \infty$, then $G \cong \mathbb{Z}/n\mathbb{Z}$

Consequence: If p is prime, $|G| = p$, then $G \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. Let $a \in G - \{e\}$, then $\langle a \rangle$ is a subgroup of G, so $|\langle a \rangle| \mid p$. Since $|\langle a \rangle| \neq 1$, $|\langle a \rangle| = p$. Thus $G \cong \mathbb{Z}/p\mathbb{Z}$. □

Example 1.9.2. If $a \mid b$, then $a\mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/\frac{b}{a}\mathbb{Z}$.

Theorem 1.9.3 (Second Isomorphic Theorem)**.** *Setting: G is a group, H, N are subgroups of G, N is normal in G. Let $HN = \{xy | x \in H, y \in N\}$. Then $H/H \cap N \cong HN/N$.*

Lemma 1.9.4. *HN is a subgroup of G, N is normal in HN, $H \cap N$ is normal in H.*

Proof to the theorem: Need $\phi : H \to HN/N$, $\phi(x) = xN$. ϕ is a group homomorphism as $H \to G \to G/N$. $ker(\phi) = \{x \in H | xN = eN\} = \{x \in H | x \in N\} = H \cap N$. ϕ is surjective: let $aN \in HN/N$, so $a = xy, x \in H, y \in N$. Then $aN = xyN = xN$ since $y \in N$. Thus $aN = \phi(x)$. Thus $H/H \cap N \cong HN/N$ □

Let G be a group with normal subgroups H, N, and suppose $H \supset N$. Let $\pi : G \to G/N$ be $x \mapsto xN$. Then $\pi(H) = H/N$ is normal since π is surjective.

Theorem 1.9.5 (Third Isomorphism theorem)**.** *$(G/N)/(H/N) \cong G/H$.*

Proof. Consider $\pi_H : G \to G/H$. $\pi_H(a) = aH$, quotient group homomorphism. If $x \in N$, $\pi_H(x) = xH = eH$ since $x \in N \subset H$. Thus $\pi_H(N) = e$. So by first isomorphism theorem, we have $\bar{\pi_H}(aN) = aH$, a group homomorphism. π_H surjective implies $\bar{\pi}_H$ is surjective. $ker(\bar{\pi}_H) = \{aN | aH = eH\} = H/N$. Thus we have isomorphism theorem. □

1.10 Sep. 18, 2019

Theorem 1.10.1 (Correspondence Theorem)**.** *Let N be a normal subgroup of G. Then*

1. *Then $\phi : S_N(G) \to S(G/N)$ given by $\phi(H) = \pi(H)$ is bijective. Its inverse is $\psi : S(G/N) \to S_N(G)$ given by $\psi(\bar{H}) = \pi^{-1}(H)$.*

2. *ϕ and ψ preverse inclusions. If $H_1, H_2 \in S_N(G)$, then $H_1 \subset H_2$ iff $\phi(H_1) \subset \phi(H_2)$ and similarly for $\bar{H}_1, \bar{H}_2 \in S(G/H)$*

3. *If $H \in S_N(G)$, then H is normal in G iff $\pi(H)$ is normal in G/N.*

Proof. (i) Show $\psi_e(H) = H$, and $\psi\psi(\bar{H}) = \bar{H}$. Then ϕ is bijective and inverse of ψ.

Set theory: let $f : X \to Y$ be a map of sets. Let $Z \subset X$, $X \subset Y$. Then

1. $Z \subset f^{-1}f(Z)$ with equality if f is injective.
2. $ff^{-1}(V) \subset V$.

Since $\phi\psi(\bar{H}) = \pi\pi^{-1}(\bar{H}) = \bar{H}$. By (ii) above since π is surjective. $\psi\phi(H) = \pi^{-1}\pi(H)$ by (ii) above let $a \in \pi^{-1}\pi(H)$ so $\pi(a) = \pi(b)$ so $b \in H$. So $ab^{-1} \in ker(\pi) \subset N$. Therefore we have $\pi^{-1}\pi(H) = H$

(ii) $H_1 \subset H_2$, therefore $\pi(H_1) \subset \pi(H_2)$ is clear. Conversely, if $\pi(H_1) \subset \pi(H_2)$, then $\pi^{-1}\pi(H_1) \subset \pi^{-1}\pi(H_2)$. But in proof of (1), we showed $N \subset H_i$ implies $\pi^{-1}\pi(H_1) = H_1$. Thus $H_1 \subset H_2$

(iii) If $H \in S_N(G)$, is normal in G, then $\pi(H)$ is normal in G/N. If $\pi(H)$ is normal, $H = \pi^{-1}\pi(H)$ is normal. □

Remark 1.10.2. Subgroups of a finite cyclic group is cyclic. Alternative proof: Let $H = \langle a \rangle$ be cyclic of order n, then $\phi : \mathbb{Z} \to H$, $\phi(n) = a^n$ is a surjective group homomorphism with kernel $n\mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z} \cong H$, but all subgroups of $\mathbb{Z}$ are cyclic, so all subgroups of $\mathbb{Z}/n\mathbb{Z}$ are $\pi(k)$, k is cyclic so $\pi(k)$ is cyclic.

1.10.1 Products

Let $G_1, \ldots, G_n$ be groups, let $G = G_1 \times \ldots \times G_n = \{(g_1, \ldots, g_n) | g_i \in G_i\}$. Then G has a binary operation, $(g_1, \ldots, g_n)(x_1 \ldots, x_n) = (g_1x_1, \ldots, g_nx_n)$. $(G, \cdot)$ is a group.

Example 1.10.3. $G = (\mathbb{R}, +)$, then $G_1 \times \ldots \times G_n = (\mathbb{R}^n, +)$. Can take $G_i = \mathbb{Z}$. Then $G_1 \times \ldots \times G_n = \mathbb{Z}^n$.

More generally, if $\{G_i\}_{i\in I}$ is a family of groups, we can let $G = \prod_{i\in I} G_i\{(x_i)|x \in G\}$, then $(x_i) \cdot (y_i) = (x_iy_i)$. Then G is a group. $e = (e_i), (x_i)^{-1} = (x_i^{-1})$.

Let $G = \prod G_i$ has a group homomorphism $\phi : G \to G_j$ given by $\phi(x_i) = x_j$. Also we have a group homomorphism $i_j : G \to G$, such that $i_j(x_j) = (y_j)$ wjere $y_j = x_j$, or $y_j = e_{G_i}$. Thus we know $G_1, \ldots G_n$ are normal in G.

1.11 Sep. 20, 2019

Remark 1.11.1. Let G be a group, $x, y \in G$, we let $[x, y] = xyx^{-1}y^{-1}$ be the commutator of G, then $[x, y] = e$ iff $xy = yx$.

Remark 1.11.2. let G be a group with normal subgroups H, K with $H \cap K$, then if $x \in H, y \in K$, then $xy = yx$

Proof. Consider $[x, y] \in K$, and $[x, y] \in H$. Then $[x, y] \in H \cap K = e$. Thus $xy = yx$. □

Proposition 1.11.3. *let G be a group with normal subgroups H, K, with $H \cap K$. Define $m : H \times K \to G$ by $m(h,k) = hk$, with $h \in H$, $k \in K$. Then*

1. *m is an injective group homomorphism and $im(m) = HK$. So $H \times K \cong HK$*
2. *If $G = HK$, then m is an isomorphism*

Proof. 2 is clear from 1. Proof of 1. Let $x_1 = (h_1, k_1)$, $x_2 = (h_2, k_2) \in H \times K$. Then $m(x_1, x_2) = m(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = m(x_1)m(X_2)$. Thus m is a group homomorphism, and $ker(m) = \{(h,k)|hk = e\}$. If $hk = e$, then $h = k^{-1} = e$. Thus, $ker(m) = e$. Thus injective. Then $im(m) = HK$. □

Application: Let G be a group of order 4, then either $G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. let $a \in G$, then $a^4 = e$. Thus $|a| \mid 4$. And $a \neq e$. Thus $|a| = 2, 4$. If $|a| = 4$, then $|\langle a \rangle| = |G|$, so $\langle a \rangle = G$. So G is cyclic and $G \cong \mathbb{Z}_4$. Otherwise, $a^2 = e$. If so, let $c, b \in G - \{e\}$, then $|b| = |c| = 2$. Let $H = \langle b \rangle$, $K = \langle c \rangle$. Then H and K have index 2. So $H = \{e, b\}$, $K = \{e, c\}$. Then by proposition, we have $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Remark 1.11.4. Let G be a group, $g \in G$. Define $c_g : G \to G$ by $c_g(x) = gxg^{-1}$ conjugation by g. $c_gc_h = c_{gh}, c_e = id(G)$. So c_g is bijective. Finally $c_g : G \to G$ is a group homomorphism. Since $c_g(xy) = c_g(x)c_g(y)$. Hence, if $A(G) = c_g$, $A(g) \in Aut(G)$. Then $A : G \to Aut(G)$, $A(g) = c_g$ and A is a group homomorphism. $ker(A) = \{g \in G|c_g = id\} = \{g \in G|gxg^{-1} = x\}$. Thus $gx = xg$. We call this the center $Z(G) = \{g \in G|gx = xg, \forall x \in G\}$. Conclude that the center is the normal subgroup of G.

1.11.1 Group actions

Let G be a group, S be a set.

Definition 1.11.5. A G-action on X is a map $\alpha : G \times X \to X$, write as $\alpha(g,x) = g \cdot x$ such that

1. if $g_!, g_2 \in G, x \in X$, then $(g_1g_2)x = g_!(g_2x)$
2. $e \cdot x = x, \forall x \in X$.

Example 1.11.6.
1. If G is a group, $X = G$, then $\alpha(g,x) = gx$.
2. Let G be a group, $X = G$. Then $\alpha(g,x) = gxg^{-1}$.
3. $G = S_n, X = \{1, \ldots, n\}$. $\alpha(\sigma, i) = \sigma(i), i \in X$.
4. $G = GL(n,F)$, F field. $X = F^n$. Then $\alpha(g,r) = g(r)$.

Remark 1.11.7. A group action on a set X is the same as a group homomorphism $\phi : G \to A(X)$. Let $g \in G$, define $\phi(g) : X \to X$ by $\phi(g)(x) = gx$. $\phi(gh) = \phi(g)\phi(h), \forall g,h \in G$, then $\phi(g) \in A(x)$ because $\phi(g) \circ \phi(g^{-1}) = \phi(e)$. And thus we have a group homomorphism $\phi : G \to A(G)$. Converse is true as well.

1.12 Sep. 23, 2019

Theorem 1.12.1 (Cayley's Theorem)**.** *If G is a finite group, G is isomorphic to subgroup of S_n for some n*

Proof. use the left multiplication of G on itself, this gives $\phi : G \to A(G)$, $\phi(g) = lg$, $l_g(x) = gx$. Then $ker(\phi) = \{g \in G | gx = x\} = \{e\}$. Therefore, $G \cong im(\phi)$ a subgroup of $A(G)$. Since G is finite, $A(G) = S_n$. Thus, G is isomorphic to a subgroup of $S_{|G|}$. ☐

Example 1.12.2. Let $G = D_8$, G acts on vertices of a polygon T_4, so G can be regarded as a subgroup of S_4. So $D_8 \subset S_4$. But by Cayley's Theorem, $D_8 \subset S_8$

G can also acts on G using right multiplication, $(a, x) \to xa^{-1}$. This is also a group action. Every left action can be converted to a right action by taking the inverse.

Example 1.12.3. G acts on G by conjugation $(g, x) \to gxg^{-1}$.

Example 1.12.4. G a group, H its subgroup let $X = G/H = \{aH | a \in G\}$, where $(g, aH) \to gaH$. This is a group action.

Example 1.12.5. Suppose G is a group of order 36 with a subgroup H of order 9. We get $\phi : G \to A(G/H)$. But $|G/H| = |G|/|H| = 4$. Therefore, $|G| = 36, A(G/H) \cong S_4$, so $|A(G/H)| = 4! = 24$. Hence ϕ is not injective. But $ker(\phi) \subset H$, so $|ker(\phi)|/|H| = 9$. Thus $|ker(\phi)| = 3, 9$. Conclude that G has a proper normal subgroup of order 3 or 9

Definition 1.12.6. Let G act on X, let $x \in X$, (i) the *orbit* $G \cdot x$ is $G \cdot x = \{gx | g \in G\}$. The *stablizer* $G_x = \{g \in G | gx = x\}$, $G \cdot x$ is called $B(x)$ and G_x is called $G(x)$)

Remark 1.12.7. The stablizer is a subgroup of G. Indeed, $e \cdot x = x$ so $e \in G_x$, let $g, h \in G_x$. If $g \in G_x$, $g \cdot x = x$, then $g^{-1}gx = g^{-1}x$ so $g^{-1} \in G_x$.

Theorem 1.12.8. *let G act on a set X, and let $x \in X$. Then the map $\phi : G/G_x \to X$, $\phi(gG_x) = G \cdot x$ is a well-defined bijection.*

Proof. ϕ is well defined, ϕ depends only on gG_x, not on G. If $gG_x = hG_x$, then $h \in G_x$, $h = ga$, so $h \cdot x = (ga) \cdot x = g \cdot (a \cdot x)$. Then $\phi(hG_x) = \phi(gG_x), g, h \in G$. Then $g \cdot x = h \cdot x$. Thus $g^{-1}h \in G_x$. So $hG_x = gG_x$. Thus injective. Surjective is clear. ☐

We write the above as $G/G_x \cong G \cdot x$. Note: if G is finite, $|G|/|G_x| = |G \cdot x|$. Helps answer the questions: How can we descrive G/H? Answer: if we find G action on X and $x \in X$ with $G_x \cong H$, then G/H is bijective to $G \cdot x$.

Definition 1.12.9. G action on X is called *transitive*, if $\exists x \in X$ with $G \cdot x = X$, if so, $G \cdot x = X$, for all $x \in X$.

Example 1.12.10. S_n acts on $X = \{1, \ldots, n\}$ by $(\sigma, i) \to \sigma(i)$ with a subgroup. Let $x = n \in X$, $G \cdot x = S_n \cdot x = X$. Transitivity. Indeed, can take $\sigma = (i, n)$ so $\sigma(n) = i$. $G_n = \{\sigma \in S_n | \sigma(n) = n\} \cong S_{n-1}$, embedded in S_n as permutations fixing n. Conclude $S_n/S_{n-1} \cong \{1, \ldots, n\}$

Example 1.12.11. Let $G = D_{2n}$ acts on vertices $\{x_1, \dots, x_n\}$ at T_n by dihedral group action. Set $x_1 = (1, 0)$. $G_x = \{\sigma \in D_{2n} | \sigma(x_1) = x_1\} = \{e, s\}$. $G \cdot x_j = \{x_1, \dots, x_n\}$ via rotations, bijection to $D_{2n}/\{e, s\} \cong \{x_1, \dots, x_n\}$

Example 1.12.12. A matrix $A = (a_{ij})$ is upper triangular. Let $B(n, F)$ =upper triangular matrices. Instead, we'll find an action on $GL(n, F)$ on a set X such that $\exists x \in X$ with $GL(n, F)_x = B(n, F)$ so $B(n, F)$ is a subgroup of stablizers.

1.13 Sep. 25, 2019

Let $\{e_1, \dots e_n\}$ be the standard basis of F^n. Let V_i be generated by the basis. $V_i \in Gr(i, F^n)$. Note $V_1 \subset V_2 \subset \cdots \subset V_n = F^n$. If $G = GL(n, F)$, G acts on $Gr(1, F^n) \times Gr(2, F^n) \times \cdot \times Gr(n, F^n)$, by $(g, (U_1, \dots, U_n)) = (g(U_1), \dots, g(U_n))$. Can check this is a group action. We claim that $B(n, F) = G_x = \{g \in G | g \cdot x = x\}$. Hence $B(n, F)$ is a subgroup of G.

1.13.1 Sylow Theorems

Definition 1.13.1. Let G be a group of order $n = p^r m$ as above. We say a subgroup P of G is a p-Sylow subgroup if $|P| = p^r$

We are going to prove that if G is finite and p is prime, G has a p-Sylow subgroup.

Remark 1.13.2. If $F = \mathbb{Z}_p$, $N(n, F)$ is a p-Sylow subgroup of $GL(n, F)$. $|GL(n, F)| = \prod_{i=0}^{n-1}(p^n - p^i)$. Thus $|GL(n, F)| = p^{n(n-1)/2}m$ with $(p, m) = 1$, then $N(n, F)$ is a p-Sylow subgroup of $GL(n, F)$.

Definition 1.13.3. A group H is called a p-group of p prime, $|H| = p^k$ for some k.

Lemma 1.13.4. *let p be a prime, $n = p^r m$ with $(p, m) = 1$. Let $t = p^k$. Then $t = p^r$ iff $t \mid n$ and $(n/t, p) = 1$. Let $|G| = p^r m$ as above, let $H \subset G$ be a subgroup, which is a p-group, then H is a p-Sylow subgroup if $(|G|/|H|, p) = 1$*

Theorem 1.13.5.

1. *Every finite group G has a p-Sylow subgroup for each prime p*
2. *Let p be prime, let G be a finite group with a p-Sylow subgroup. Let H be a p-subgroup of G. Then H has a p-Sylow subgroup.*

The proof of this uses the injection of G/P.

1.14 Sep. 27, 2019

Remark 1.14.1. G be a group with subgroup S. G acts on $X = G/S$ by $g(xS) = gxS$. $G_{xS} = xSx^{-1}$: indeed, $g \in G_{xS}$ iff $gxS = xS$ iff $x^{-1}gxS = S$. Thus $x^{-1}gx \in S$. $g \in xSx^{-1}$. If $A \subset G$ is another subgroup, then A acts on $X = G/S$ by $g(xS) = gxS$ for $g \in A$. $A_{xS} = G_{xS} \cap A = A \cap xSx^{-1}$

Remark 1.14.2. Let G be a group, with subgroup H. Then $gHg^{-1} = c_g(H)$. $c_g(x) = gxg^{-1}$, since c_g is an automorphism of G, $gHg^{-1} = c_g(H)$ is a subgroup of G, and $|H| = |gHg^{-1}|$. For $k \in \mathbb{Z}_{>0}$, let $S_k = \{$ subgroups H by the above comments. It's easy to check this is a group action. The stabiliser G_H of a subgroup H is $G_H = \{g \in G | gHg^{-1}\}$. We call $G_H = N_G(H)$, normalizer of H in G. $N_G(H)$ is a subgroup of G since it is a stabilizer.

Proposition 1.14.3. *Let G be finite, with a p-Sylow subgroup P. Let $H \subset G$ be a subgroup. Then H has a p-Sylow subgroup Q*

Proof. If $g \in G$ and $P \subset G$ is a p-Sylow subgroup. $gPg^{-1} = c_g(P)$ is also a p-Sylow subgroup. By the orbit remark, $X = X_1 \sqcup \ldots \sqcup X_k$, where they are H-orbits of X. And $|X| = \sum |X_i|$. But $|X| = |G|/|P| = p^r m/p^r = m$. So $p \nmid |X|$. There exists j such that $p \neq |X_j|$. But if $X_j = H_j P$, $|X_j| = |H|/|H \cap gPg^{-1}|$ by stabilizer Remark. But $H \cap gPg^{-1}$ is a subgroup of gPg^{-1}, so $|H \cap gPg^{-1}| \mid |gPg^{-1}| = |P| = p^r$. So $H \cap gPg^{-1}$ is a p-subgroup of H. By Lemma, we have $H \cap gPg^{-1}$ is a p subgroup of G. $\square$

Theorem 1.14.4 (Sylow 1)**.** . *Let $|G| = p^r m$, $(p, m) = 1$. Then G has a p-Sylow subgroup*

Proof. We have a injection group homomorphism $G \to S_n$ with $n = |G|$. For $F = \mathbb{Z}_p$, we have a injection group homomorphism $p : S_n \to Gl(n, F)$. This is a injection homomorphism: $G \to GL(n, p)$. And this group has a p-Sylow subgroup. $\square$

Lemma 1.14.5. *Let H be a p-group, for p prime. Let H act on a finite set X. Let $X^H = \{x \in X | gx = x, \forall g \in H\}$, the fixed points of H. Then $|X| = |X^H| \mod p$.*

Proof. Observe that if $x \in X$, then $x \in X^H$ iff $Hx = \{x\}$ iff $|Hx| = 1$. Indeed, $x \in X^H$ then $gx = x, \forall g \in H$,so $Hx = \{x\}$ is similar $Hx = \{x\}$ iff $|Hx| = 1$ because $x \in Hx$. By the orbit remark, $|X| = \sum |Hx_i|$ where $Hx_1, \ldots, Hx_l$ are distinct orbits number so $|Hx_1| = 1$. And $|Hx_i| < 1$ for $i > q$. Then $|X| = \sum 1 + |Hx_i|$. but $|Hx_i| = |H|/|H_{x_i}|$. H is a p-group, so $|H| = p^a$, since $|Hx_i| = p^a$ some $a_i \leq a$. For $i = q+1, \ldots, k$, $|Hx_i| > 1$. So $|X| = |X^H| + \sum p^{a_i}$ so $|X| = |X^H| \mod p$. Since $p^a = 0 \mod p$ for $a_i > 0$. $\square$

Theorem 1.14.6. *Let $|G| = p^r m$ with $(p, m) = 1$. (i) Let P, Q are Sylow p subgroups,then $P = xQx^{-1}$*

Proof. H act on $X = G/P$ by $a_i(xP) = axP, a \in A, x \in G$. Then $|X| = |G|/|P| = m$. So $p \nmid |X|$, but $|X| = |X^H| \mod p$. $|X^H| \neq 0 \mod p$. So $|X^H| \neq 0$, $X^H \neq \emptyset$. Let $gP \in X^H$. Then $agP = gP, \forall a \in H$ so $H \subset G_P$. But $G_{gP} = gPg^{-1}$ by stabilizer remark. So $H \subset gPg^{-1}$. Similarly one can prove the other side. $\square$

1.15 Sep. 30, 2019

Lemma 1.15.1. *Let $P, Q \in Syl_p$, If $P \subset N_G(Q)$, then $P = Q$.*

We consider the Q action on Syl_p, by $(g, Q) \to gQg^{-1}$. $Syl^Q = \{Q_1 \in Syl_p | gQ_1 = Q_1\}$. By the lemma, $Syl^Q = Q$.

Theorem 1.15.2. *Let $|G| = p^r m$ with p a prime, $(p, m) = 1$ as above. Let $n_p = |Syl_p|$, the number of Sylow subgroups of G. Then $n_p \mid m$, $n_p \equiv 1 \mod p$.*

Proof. We know G acts transitively on Syl_p, and $|Syl_p| = n_p$. Therefore, $\exists$ a bijection by orbit-stablizer theorem, $G/N_G(P) \cong Syl_p$. Therefore, $n_p = |Syl_p| = |G|/|N_G(P)| = |G|/|N_G(P)| \cdot |N_G(P)||P|$. Thus $n_p \mid m$. Then by the lemma from last time, for action of p-group A on a finite set X, $|X| \equiv |X^A| \mod p$. Apply to P action on Syl_p. P is a p-Sylow subgroup. Conclude that $n_p \equiv 1 \mod p$. □

Remark 1.15.3. Often the third Sylow theorem is sufficient to compute n_p to show $n_p = 1$.

Example 1.15.4. If $|G| = 63 = 3^2 7$, then $n_7 = 1$ since $n_7 \equiv 1 \mod 7, n_7 \mid 9$, so $n_7 = 1$

Remark 1.15.5. Let G be a finite group, $p \mid |G|$. Then $n_p = 1$ iff any p-Sylow subgroup of G is normal.

Proof. If $n_p = 1$, then $g \in G$, gQg^{-1} is a p Sylow subgroup. Thus $Q = gQg^{-1}$. Let Q, P be p-Sylow subgroups with Q normal. Then by the second Sylow theorem, $\exists g \in G$ such that $Q = gPg^{-1}$, but $Q = gQg^{-1}$. Thus $Q = P$. □

Conclude: A group of order 63 has a normal 7-Sylow subgroup.

Definition 1.15.6. A group G is *simple* if it has no proper normal subgroups, i.e., no normal subgroups besides the trivial subgroup and the group itself.

Hence a group of order 63 is not simple.

Example 1.15.7. $\mathbb{Z}_p$ is simple for p-prime. A_n is simple for $n \geq 5$.

Example 1.15.8. Let G be a group of order 6. Then either $G \cong S_3$ or $G \cong \mathbb{Z}_6$.

Proof. Let A be a 2-Sylow subgroup, B a 3-Sylow subgroup. $|A| = 2$, $A = \langle 2 \rangle$, $|a| = 2$. $B = \langle b \rangle$, $|b| = 3$. Then G acts on $G/A = \Psi$. Then $|\Psi| = 3$, we get a homomorphism $\Phi : G \to A(\Psi)$. So $\Phi(g) = g \times A$. Then $A(\Psi) \cong S_3$. If $ker(\Phi) = 1$. Then $\Phi : G \to Im(\Phi)$. Thus $Im(\Phi) = A(\Psi)$. Thus we get $G \cong A(\Psi) \cong S_3$. If $ker(\Phi) = A$, then $ab\Psi = b\Psi$. So we know that the order is 2. Thus A is normalized by B. Therefore, $\{e, a, b, b^2\} \subset N_G(A)$. so $|N_G(A)| \geq 4$. So $|N_G(A)| = 6$. Also, B is normal since the index is 2. Thus $|A \times B| = G$. Thus $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong G \cong \mathbb{Z}_6$. □

Corollary 1.15.9 (Cauchy's Theorem)**.** *Let G be finite, p be prime. Then $p \mid |G|$ iff $\exists a \in G$ such that $|a| = p$.*

Proof. One way is clear since $|\langle a \rangle| \mid |G|$. The other way gives, if $Q \subset G$ be a p-Sylow subgroup. So $|Q| = p^r$, $r > 0$ since $p \mid |G|$. Let $x \in Q$. Then $|X| \mid |Q|$, so $|x| = p^k$. Thus, $|x^{p^k - 1}| = p$. □

1.16 Oct. 2, 2019

Corollary 1.16.1. *If G is a finite, then G is a p-group if and only if $\forall a \in G$, $|a| = p^{k_a}$*

Proof. If $|G| = p^n$, If $a \in G$, $|a| \mid |G| = p^n$, thus $|a| = p^{k_a}$ for some k_a.

By contradiction, if $|G| = p^n$, $\exists$ a prime $q \neq p$ so $q \mid |G|$. $\exists a \in G$ such that $|a| = q$, contradicting right handside. $\square$

Definition 1.16.2. A group G is called a p-group of $\forall a \in G$, $\exists k_a$ such that $|a| = p^{k_a}$

Example 1.16.3. $G = \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p = \mathbb{Z}_p^\infty$. If $a \in G$, $a^f = e$, so G is a p-group.

1.16.1 The class equation

Let a group A act on a finite set X. $X^A = \{x \in X | g \cdot x = x, \forall g \in A\}$. Then $|X| = |X^A| + \sum_{i=1}^r |X_i|$, where $X_1, \ldots, X_r$ are the distinct A-orbits such that $|X_i| > 1$. Indeed, we saw $|X| = \sum |X_j|$ as X_j ranges over distinct A-orbits. $|X_j| = 1$ if and only if $X_j = \{x_j\}, x_j \in X$.

Apply G-action on $X = G$ by $(g, x) \to gxg^{-1}$, $g \in G, x \in X$. If $x \in X$, the G-orbit $G \cdot x = \{gxg^{-1} | g \in G\} = C(x)$, the conjugacy class of x. By orbit stablizer theorem, $G/G_x \cong G \cdot x$. $G_x = \{g \in G | gxg^{-1} = x\} = C_G(x)$ the *centralizer* of x in G. Conclude, $\exists$ a bijection $G/C_G(x) \cong C_x$, $gC_G(x) \to gxg^{-1}$

And $X^G = \{x \in X | g \cdot x = x\} = \{x \in G | gxg^{-1} = x\} = Z(G)$ center of G normal subgroup. Distinct G-orbits a X are distinct conjugacy classes. By generality with $G = A, X = X$, conclude $|X| = |Z(G)| + \sum |C(x)|$, where the sum is over distinct conjugacy classes. This is called the *class equation*.

Proposition 1.16.4. *Let G be a finite p-group. Then $Z(G) \neq \{e\}$. In fact, $p \mid |Z(G)|$*

Proof. Let $|G| = p^n$. Write down the class equation $p^n = |Z(G)| + \sum |C_{x_i}|$. But $|C_{x_i}| = (|G|/|C_G(x_i)|) \mid G = p^n$, thus $|C_{x_i}| = p^a$. Thus $p^n \equiv |Z(G)| + \sum p^a \mod p$, then $|Z(G)| \equiv 0 \mod p$, so $p \mid |Z(G)|$. $\square$

Proposition 1.16.5. *Let G be a group of order pq with p, q primes, and $p < q$. Then G has a normal p-Sylow subgroup, and $q \not\equiv 1 \mod p$, then G is cyclic.*

Proof. Let n_q be the number of q-Sylow subgroups $|G| = qm$, where $m = p$. $n_q \equiv 1 \mod p, n_q \mid m = p$, thus $n_q = 1$. Thus there is a normal q-Sylow subgroup. Suppose $q \not\equiv 1 \mod p$, $|G| = pm$, with $m = q$. By Sylow theorem, $n_p = 1$. Since the intersection is trivial, $G = C_q \times C_p$ $\square$

Corollary 1.16.6. *If $|G| = pq$, then G is not simple.*

Proposition 1.16.7. *Let p, q be distinct primes and let $|G| = p^2q$, then G has a normal p-Sylow subgroup or a normal q-Sylow subgroup.*

1.17 Oct. 4, 2019

Proposition 1.17.1. *The alternating group A_5 is a simple group, i.e, it has no proper normal subgroups.*

Proof. $60 = 5 \cdot 12$, then $n_5 \mid 12$, $n_5 \equiv 1 \mod 5$, so $n_5 = 1, 6$. In fact, $n_5 = 6$. Let $\sigma = (1\ 2\ 3\ 4\ 5)$, then $\langle \sigma \rangle$ has order of 5. If $\tau = (1\ 3\ 2\ 4\ 5) \notin \langle \sigma \rangle$. Thus $\langle \tau \rangle$ is distinct from that of σ. So $n_5 = 6$. Now assume $G = A_5$ is not simple, then find a contradiction. Show $\exists$ a proper normal subgroup H of G such that $5 \mid |H|$. By assumption, $\exists$ a proper normal subgroup N of G. Since $|N| \mid |G| = 60$, $|N| = 2, 3, 4, 5, 6, 10, 12, 15, 20, 30$. If $|N| = 5, 10, 15, 20, 30$, we take $H = N$. If not $|N| = 2, 3, 4, 6, 12$, if $|N| = 6$, then N has a normal 3-Sylow subgroup H_1. And if $|N| = 12$, then N has a normal 3 or 4 Sylow subgroup H_1. The subgroup H_1 of G of N is normal in G. Hence if $5 \nmid |N|$, then G has a normal subgroup of order $2, 3, 4$. If $|N| = 6, 12$, take $N_1 = H_1$, if $|N| = 2, 3, 4$, then take $N_1 = N$. Let $\bar{G} = G/N_1$, and $\pi : G \to \bar{G}$. Then $|\bar{G}| = 20, 30, 15$. If $|\bar{G}| = 30$, then $\bar{G}$ has normal 5-Sylow subgroup by remark 1. If $\bar{G} = 20$, then $\bar{G}$ has normal 5-Sylow subgroup. Hence $\bar{G}$ has a normal 5-Sylow subgroup. $\bar{Q}$, $|\bar{Q}| = 5$. Then take $H = \pi^{-1}(\bar{Q})$. Then $H/N \cong \bar{Q}$, H is normal in G by the correspondence theorem. then $|H| = |N||\bar{Q}| = 5|N|$, so $5 \mid |H|$ and H is proper since $|N_1| = 2, 3, 4$. Hence $\exists$ a proper normal subgroup H of G such that $5 \mid |H|$. Thsu $|H| = 5, 10, 15, 20, 30$. By problem set 8(i), every 5-Sylow subgroup of H is contained in G. Therefore H has 6 distinguished 5-Sylow subgroups, so by argument H has 24 element of order 5. thus $|H| = 30$. However, a group of order 30 has a unique 5-Sylow subgroup Q. Since H is normal in G, by problem set 6: 8(ii), G has a unique 5-Sylow subgroup. But $n_5 = 1$, thus $n_5 = 6$. Thus a contradiction. Thus A_5 is simple. $\square$

Theorem 1.17.2. *A_n is simple if $n \geq 5$.*

The proof is inductive.

1.18 Oct. 7, 2019

1.18.1 Composition Series

Definition 1.18.1. Let G be a group a composition series for G is a sequence of subgroup $e \subset G_0 \subset \ldots \subset G_r = G$ such that $G_{i-1} \trianglelefteq G_i$ and G_i/G_{i-1} is simple.

Notation: Given a composition series $G_0 = e \subset G_1 \subset \ldots \subset G_r = G$, we say that the length of the composition series is r and the composition factors are G_i/G_{i-1}

Theorem 1.18.2 (Jordan Holder Theorem)**.** *Let G be a group with composition series $e = G_0 \subset G_1 \subset \ldots \subset G_g = G$ and $e = H_0 \subset H_1 \subset \ldots \subset H_r = H$. and $G = H$. Then $r = g$. Further more is $\bar{G}_i = G_i/G_{i-1}$, and $\bar{H}_i = H_i/H_{i-1}$, then $\exists \sigma(i)$ such that $\bar{G}_{\sigma(i)} = \bar{H}_i$. In other words, the composition factors are are the same up to permutation.*

Example 1.18.3. Let $n \in \mathbb{Z}_{>0}$, $n = p_1^{e_1} \dots p_n^{e_n}$ be the prime factorization. Then $\exists$ a composition series of G of length $e_1 \dots e_k$ with the composition factors of $\mathbb{Z}_{p_1} \dots \mathbb{Z}_{p_n}$. By Jordan Holder theorem, we see that the prime factorization is unique.

Proposition 1.18.4. *Let G be a non-trivial finite group, then G has a composition series.*

Proof. We use induction on $|G|$. If $|G|$ is 2, then $G \cong \mathbb{Z}_2$ which is simple. Thus $G_0 = e$, $G_1 = \mathbb{Z}_2$. Thus G is a composition series. Let $|G| = n$, and assume $|H| < n$, then H has a composition series. Case 1: if G is simple, $G_0 = e, G_1 = G$. So we have a composition series. Case 2: if G is not simple, then G has a proper normal subgroup, say N. By induction hypothesis, N has a composition series. And $\bar{G} = G/N$, then $\bar{G}$ has a composition series. Thus G has a composition series. $\square$

1.19 Oct. 9, 2019

1.19.1 Solvable groups

Let G be a group, let $X \subset G$ be a subset. $\langle X \rangle$ = smallest subgroup of G containing X. We call $\langle X \rangle$ the subgroup of G generated by X.

Remark 1.19.1. $\langle X \rangle = \{x_1^{n_1} \dots x_k^{n_k} | k \geq 0, x_1, \dots, x_k \in X$ not necessarily distinct$\}$. Let this be H_x, it is easy to see that H_x is a subgroup, and $X \subset H_x$, so $\langle x \rangle \subset H_x$. Conversely, $X \subset H$ and H a group, $H_x \subset H$, so $H_x \in \langle X \rangle$. Thus $H_x = \langle X \rangle$.

Definition 1.19.2. If $H, K \subset G$ are subgroups, $[H, K]$ is the subgroup of G generated by all $[a, b]$, $a \in H, b \in K$. Especially if $H = G, K = G$, then $[G, G] = \langle [a, b] | a, b \in G \rangle$. $[G, G]$ is called the *commutator subgroup* of G.

Remark 1.19.3. let $X \subset G$ be a subset, and let $g \in G$. Then $\langle gXg^{-1} \rangle = g\langle X \rangle g^{-1}$ by remark. Hence, if $gXg^{-1} \subset X, \forall g \in G$, then $g\langle X \rangle g^{-1} = \langle gXg^{-1} \rangle \subset \langle X \rangle$. Thus $\langle X \rangle$ is normal.

Lemma 1.19.4. *1. If H, K are normal subgroups of G, then $[H, K]$ is normal.*

2. *$[G, G]$ is a normal subgroup of G.*

3. *G is abelian iff $[G, G] = \{e\}$*

4. *$G^{(1)} = [G, G]$, then $G/G^{(1)}$ is abelian.*

5. *If $N \subset G$ is normal, G/N is abelian, iff $G^{(1)} \subset N$.*

Proof. 1. Let $a \in H, b \in K$, $a[a, b]g^{-1} = g(aba^{-1}b^{-1})g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1})g^{-1} = [gag^{-1}, gbg^{-1}]$. Hence, it is in $[H, K]$ since H, K are normal.

4. Let $aG^{(1)}, bG^{(1)} \in G/G^{(1)}$. Then $aG^{(1)}bG^{(1)} = abG^{(1)} = ab[b^{-1}, a^{-1}]G^{(1)} = baG^{(1)}$.

5. Suppose $G^{(1)}$ is not in N, $\exists a, b \in G$ such that $[a, b] \notin N$. So $[a, b]N \neq N$. But $[a, b]N = aba^{-1}b^{-1}N = [aN, bN]$. So $[aN, bN] \neq N$. So G/N is not abelian. $\square$

Remark 1.19.5. Let $\phi : G \to H$ be a group homomorphism. $\phi([G,G]) = [\phi(G), \phi(G)]$.

Remark 1.19.6. Let $G_0 = G$, $G^{(1)} = [G,G]$, and we continue inductively. By lemma 1, $G^{(1)}$ is normal in G, $G^{(2)}$ is similarly normal in $G^{(1)}$. And $G^{(i)}$ is normal in G. We have a sequence of normal subgroup $G = G^0 \supset G^{(1)} \ldots$.

Definition 1.19.7. A group G is solvable if $\exists r > 0$ such that $G^{(r)} = 1$.

Example 1.19.8. If G is abelian, then $G^{(1)} = e$. Thus G is solvable. If G is non-abelian and simple, then G is not solvable. Indeed $G^{(1)}$ is a normal subgroup of G, and G is not abelian, then $G^{(1)} \neq e$. G simple implies $G = G^{(1)} = \ldots$. Hence $A_n, n \geq 5$ is not solvable.

Theorem 1.19.9. *If G is a finite group, G is solvable, then it has a composition series with abelian composition factors.*

1.20 Oct. 11, 2019

Proposition 1.20.1. *Let G be a group, the the following are equivalent*

1. *G is solvable*
2. *$\exists$ a sequence $G = G_0 \supset G_1 \supset G_2 \ldots \supset G_r = \{e\}$ of normal subgroups of G such that for G_i/G_{i+1} is abelian*
3. *Same as 2 except we only assume G_{i+1} is normal in G.*

Proof. $1 \Rightarrow 2$ Since $G^{(i)}$ is normal in G, we set the sequence to be $G^{(i)}$. $2 \Rightarrow 3$ is trivial. $3 \Rightarrow 1$. Given $G_{i+1} \supset G^{(i)}$ since G_i/G_{i+1} is abelian. Then by induction, we have a sequence of $G^{(i)}$. □

Proposition 1.20.2. *Let G be a group: (i) if G is solvable, and $A \subset G$ is a subgroup, then A is solvable. (ii) Let $N \subset G$ be normal, then G is solvable iff N and G/N are solvable.*

Proof. $A \subset G$, then $A^{(i)} \subset G^{(i)}$. Therefore if $G^{(r)}$ is trivial then $A^{(r)}$ is trivial.

Consider the quotient homomorphism. Then $\pi(G^{(i)}) = \pi(G)^{(i)}$. So if $G^{(r)}$ is trivial then $G/N^{(r)}$ is trivial.

Since G/N is solvable, then if $G/N^{(r)}$ is trivial, $\pi^{-1}(G/N^{(r)}) \subset N$. But N is solvable. So G is solvable. □

Definition 1.20.3. A group G is nilpotent if $\exists r > 0$ such that $G_{(r)} = [G, G_{i-1}] = e$

Theorem 1.20.4. *If $G/Z(G)$ is nilpotent, then G is nilpotent*

Proof. Let π be the quotient group homomorphism. $\forall \phi : G \to H$ group homomorphism, $\phi(G_i) = \phi(G)_i$. Then $G/Z(G)$ is nilpotent then $\pi(G)$ is nilpotent, so there is an r such that $G_r \subset Z(G)$, but $[G, Z(G)] = 1$. So G is nilpotent. □

Corollary 1.20.5. *A finite p-group G is nilpotent, and hence solvable.*

Proof. let $|G| = p^r$, use induction on r. If $r = 0$, then G is nilpotent. Assume for a nilpotent group A if $|A| = p^k$, $k < r$. G has nontrivial $Z(G)$, so $|Z(G)| = p^t, t > 0$. Thus $|G/Z(G)| = p^{r-t} < p^r$. Thus $G/Z(G)$ is nilpotent. thus G is nilpotent. Hence G is solvable. □

1.20.1 Free Groups

Definition 1.20.6. Let S be a set, a *free group* G on S is a group G with a map $g : S \to G$ such that if $\phi : S \to H$ is a map to a group H, $\exists$ a unique group homomorphism $\tilde{\phi} : G \to H$ such that $\phi = \tilde{\phi} \circ j$.

Example 1.20.7. $S = \{x\}$, $|S| = 1$. We take $G = \mathbb{Z}$, $j : S \to \mathbb{Z}$ is $j(x) = 1$. $(\mathbb{Z}, j)$ is a free group on S.

1.21 Oct. 14, 2019

Definition 1.21.1. Let $k \geq 0$, a word of length k on S is a formal expression $x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}$ with $x_i \in S$, $\varepsilon = \pm 1$. And if $x_j = x_{j+1}$, then $\varepsilon_j = \varepsilon_{j+1}$. A word of length 0 is the empty set.

Definition 1.21.2. $F(S)$ is the collection of all words in S of length $x \geq 0$. If a is a word of length k and b is a word of length l, we define ab by appending b to the end of a and cancelling all expressions $x_i^{-1}x_i$ or $x_i x_i^{-1}$ that result.

Define $c : S \to F(S)$ by $c(x) = x^c$ for $x \in S$

Proposition 1.21.3. *(i) $F(S)$ is a group. (ii) $(F(S), c)$ is a free group on S.*

Free groups exist; formally, they are objects in group theory, but they are best studied using topology or logic

Corollary 1.21.4. *Let H be a group, then $\exists$ a free group $(F(S), c)$ and a surjective group homomorphism $\psi : F(S) \to H$. Hence, $H \cong F(S)/ker(\psi)$*

Suppose $H \cong F(S)/ker(\psi)$, $R \subset ker(\psi)$ is a subset so that $ker(\psi)$ is the smallest normal subgroup of $F(S)$ containing R. Then we call R the relations of $F(S)$.

1.22 Oct. 18, 2019

1.22.1 Category

Definition 1.22.1. A category C consists a collection of objects $Ob(C)$, and $\forall x, y \in Ob(C)$, a collection of morphisms $Hom_C(x, y)$ such that if $x, y, z \in Ob(C)$, there is a map

$Hom_C(y,z) \times Hom_C(x,y) \to Hom_C(x,z)$ written $(g,f) \to g \circ f$ called composition, satisfying axioms (i) $\forall x \in C, \exists Hom_C(X,X)$ such that if $f \in Hom_C(x,y)$, $g \in Hom_C(z,x)$, then $f \circ id_x = f$ and $id_x \circ g = g$. (ii)$\forall x,y,z,w \in Ob(C)$ and $f \in Hom_C(x,y)$, $g \in Hom_C(y,z)$, $h \in Hom_C(z,w)$ then $(h \circ g) \circ f = h \circ (g \circ f)$

Note: $x \in Ob(C)$ need not be a set, say $id_x : x \to x$ is the identity map of x. Often we write $x \in C$ in place of $x \in Ob(C)$ and $Hom(x,y)$ for $Hom_C(x,y)$ when C is understand.

Example 1.22.2. C = Sets. $Ob(C)$ = Sets. If $x,y \in$Sets, then $Hom_{Sets}(x,y) = \{f : x \to y | f \text{ is a map}\}$

Example 1.22.3. C = Groups, then $Ob(C)$ =Groups. If G,H are groups, $Hom_{Groups}(G,H) = \{f \text{ is a group homomorphism}\}$. If G,H are groups, they are also sets, but $Hom_{Groups} \neq Hom_{Sets}(G,H)$ execept when $H = 1$.

There will be category of rings, a category of R-modules for R a ring.

Definition 1.22.4. A category C is called small if $\forall x,y \in C, Hom_C(x,y)$ is a set.

Definition 1.22.5. Let C be a category, $x,y \in C$, and $f : x \to y$ in $Hom_C(x,y)$, then f is an isomorphism if $\exists g \in Hom_C(y,x)$ such that $g \circ f = id_X$ and $f \circ g = id_Y$. If so, we write $x \cong y$.

A small category with 1 object for which every morphism is an isomorphism is the same as a group.

Definition 1.22.6. Let C be a category, and object $X_0 \in C$ is called an initial object if $\forall x \in Ob(C)$, $\exists$ a unique element $f_x \in Hom_C(x_0,x)$. An object X_1 is called final if $\forall x \in Ob(C)$, $\exists!$ element $g_x \in Hom_C(x,x_1)$

Lemma 1.22.7. *Let C be a category, if x_0, y_0 are initial objects, there is an $\cong$ $f_0 : x_0 \to x_0$. If $x,y \in C_0$ are final objects, there is an $\cong$ $f_{x_1} : x_1 \to y_1$.*

Chapter 2

Ring Theory

2.1 Oct. 28, 2019

Definition 2.1.1. A *ring* $(R, +, \cdot)$ is a set R with 2 binary operations, written as $(a, b) \to a + b$ and $(a, b) \to ab$ such that

1. $(R, +)$ is an abelian group
2. $\forall a, b, c \in R$, $(ab)c = a(bc)$
3. $\forall a, b, c \in R$, $(a + b)c = ac + bc$ and $c(a + b) = ca + cb$
4. $\exists 1_R \in R$, $1_R \neq 0_R$ where 0_R is identity of $(R, +)$ such that $1_R a = a 1_R = a$.

Remark 2.1.2. One can check that $\forall a, b, c \in R$

1. $a0_R = 0_R a = 0_R$,
2. $(-a)b = a(-b) = -ab$
3. $1_R 1_R = 1_R$
4. $(-a)(-b) = ab$
5. $b - c = b + (-c)$
6. $(a - b)c = ac - bc$
7. $c(a - b) = ca - cb$
8. 1_R is the unique element with the identity property.

Therefore, usual rules of arithmetic apply in a ring, except those that use $ab = ba$ or existence of multiplicative inverses. If we allowed $1_R = 0_R$, then $R = \{0_R\}$ since $a1 = a = a0 = 0$.

Proposition 2.1.3. *Let $(R, +, \cdot)$ be a ring. Let $R^\times = \{a \in R | \exists b \in R$ with $ab = 1 = ba\}$. Then $R^\times$ is a group with identity 1_R*

Definition 2.1.4. If $a, b \in R - \{0\}$ but $ab = 0$, then we call a, b zero divisors. We call the elements of $R^\times$ the units of R. R is called commutative if $ab = ba \forall a, b \in R$. If $R^\times = R - \{0\}$, we call R a division ring. We call commutative division ring a field. This agrees with our earlier definition of a field.

Definition 2.1.5. Let R be a ring with operations $+$ and $\cdot$. If $S \subset R$ is a subset, we say S is a subring if $(S, +, \cdot)$ is a ring and $1_R \in S$

Remark 2.1.6. A subset S is a subring iff (1) $(S, +)$ is a subgroup, (2) $a, b \in S, ab \in S$ (3) $1_R \in S$.

Example 2.1.7. Let $R = \mathbb{C}$, complex numbers, then $\mathbb{Z}$ is a subring of $\mathbb{C}$.

Let $d \in \mathbb{Z} - \{0, 1\}$, we say d is square free if $n^2 \mid d$, then $n = \pm 1$ for $n \in \mathbb{Z}$. Let $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}, \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$. These are both subrings of $\mathbb{C}$. And $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$. $\mathbb{Z}[\sqrt{-5}]$

Definition 2.1.8. A commutative ring R is an integral domain if it has no zero divisors. A field F is an integral domain. Let $a, b \in F$, $ab = 0$, and $a \neq 0$ then $\exists 1/a \in F$. And $1/a(ab) = 1b = b$, so $b = 0$. Thus $ab = 0$ in $R \subset F$, then $ab = 0$ implies a or b is 0.

Remark 2.1.9. A subring of an integral domain is an integral domain. Hence $\mathbb{Z}[\sqrt{d}]$ and $\mathbb{Q}[\sqrt{d}]$ are integral domains. Moreover, $\mathbb{Q}[\sqrt{d}]$ is a field.

Example 2.1.10. Let $n \in \mathbb{Z}_{>1}$, $\mathbb{Z}_n = \{0, \ldots, n-1\}$. Then $\mathbb{Z}_n$ is a ring. In particular, $\mathbb{Z}_p^\times$ is a field iff p is a prime.

Remark 2.1.11. Let R be a finite integral domain. Then R is a field.

Proof. Assume $|R| < \infty$ for $a \in R$, define $L_a : R \to R$ by $L_a(x) = ax$. Then $L_a : (R, +) \to (R, +)$ is a group homomorphism. Indeed if $x, y \in R$, $L_a(x + y) = a(x + y) = ax + ay = L_a(x) + L_a(y)$. But $\ker(L_a) = \{x \in R | ax = 0\} = \{0\}$. Since R is an integral domain. Hence, L_a is injective, so $|im(L)| = |R|$, so since $im(L_a) \subset R$, and $|R| < \infty$, $im(L_a) = R$. But $1 \in R$, so $1 \in im(L_a)$, so $\exists x \in R$ s.t. $ax = 1$. Hence $R^\times = R - \{0\}$, so R is an integral domain. □

We apply this to $\mathbb{Z}_n$, so for p a prime, $\mathbb{Z}_p$ is a field, otherwise $\mathbb{Z}_n$ is not a integral domain.

2.2 Oct. 30, 2019

Let R be a ring, $M(n, R) = \{A = (a_{ij} | a_{ij} \in R\}$. $M(n, R)$ is a ring using usual addition and multiplication of matrices.

Remark 2.2.1. If $R = F$ is a field, then $M(n, F)^\times = GL(n, F)$

Definition 2.2.2. let $R = M(2, \mathbb{C})$, let $S = \{\begin{bmatrix} u & v \\ -\bar{v} & \bar{u} \end{bmatrix} | u, v \in \mathbb{C}\} \subset M(2, \mathbb{C})$ is a subring. We write $\mathbb{H} = S$, and call $\mathbb{H}$ the quarternions. And the quarternions is a noncommutative division ring.

2.2.1 Polynomial rings

Let R be a ring, define $R[x] = \{p = \sum_{i=0} a_i x^i | \exists d(p) \geq 0 \text{ such that } a = 0, \forall i > d(p)\}$. When we write p, we typically omit terms of form $0x^i$. We claim that $(R[x], +, \cdot)$ is a ring.

Definition 2.2.3. Let $p = \sum_{i=0}^{\infty} a_i x^i \in R[x]$, $p \neq 0$. Then $p = a_0 + a_1 x + \ldots + a_d x^d$ with $a_d \neq 0$. We set $deg(p) = d$ and $l(p) = a_d$ (leading coefficients). We set $deg(0) = -\infty$.

We claim that if R is an integral domain, and $q, p \in R[x] - \{0\}$, then $deg(pq) = deg(p) + deg(q)$ and $l(pq) = l(p)l(q)$

Example 2.2.4. Let R be a ring, $R[[x]] = \{\sum_{i=0}^{\infty} a_i x^i | a_i \in \mathbb{R}\}$. Then $R[[x]]$ is a ring using the same formulas for $+$ and $\cdot$ as for $R[x]$.

Proposition 2.2.5. *Let R be a ring. Let $a, b \in R$. Assume $ab = ba$, then $(a + b)^n = \sum \binom{n}{k} a^k b^{n-k}$.*

Proof. Use induction and binomial coefficient identity. □

Definition 2.2.6. Let R, S be rings. A map $f : R \to S$ is called a ring homomorphism if $f(a + b) = f(a) + f(b), f(ab) = f(a)f(b)$, $f(1_R) = 1_S$

Example 2.2.7. Let $R = \mathbb{C}$, then $\tau : R \to R$, and $\tau(x) = \bar{x}$. τ is a ring homomorphism

2.3 Nov. 1, 2019

Definition 2.3.1. Let I be a subset of the ring R, consider

1. I is an additive subgroup of R
2. If $a \in I$ and $r \in R$, then $ra \in I$
3. If $a \in I$ and $r \in R$, then $ar \in I$.

If 1 and 2 hold, then I is a left ideal of R if 1 and 3 hold, then I is a right ideal of R. If all satisfies then I is an ideal of R. Let $I \neq R$ then I is a proper ideal of R.

Let R be a ring and let $a \in R$, $a \in R$, then we know RaR is an ideal, aR is a left ideal and Ra is a right ideal.

If R is commutative, ideals = left ideals = right ideals.

Definition 2.3.2. Let $(a) = Ra$ for $a \in R$, then we call I principal if $I = (a)$ for some $a \in R$.

If R is not commutative then we call an ideal a two-sided ideal.

Definition 2.3.3. If R is an integral domain, and $a \in R - \{0\}$ and $b \in R$, we say $a \mid b$ if $b = ca$ for some $c \in R$. Note $a \mid b$ iff $b \in (a)$.

Remark 2.3.4. If $p, q \in R[x]$, and R is a domain, and $p \mid q$. Then $deg(q) \geq deg(p)$ if $q \neq 0$.

Definition 2.3.5. Let $f : R \to S$ be a ring homomorphism. Define $\ker f = \{a \in R | f(a) = 0\}$ and $im(f) = \{f(a) | a \in R\} \subset S$.

Proposition 2.3.6. *(1)* $\ker(f)$ *is a proper ideal of* R*. (ii)* $im(f)$ *is a subring of* S*.*

Remark 2.3.7. If I is an ideal of R, then $I = R$ iff $\exists$ a unit a in I

Definition 2.3.8. $f : R \to S$ a ring homomorphism is called a ring isomorphism if $\exists g : S \to R$ a ring homormophism such that $g \circ f = id_R$ and $f \circ g = id_S$.

Remark 2.3.9. A ring homomorphism $f : R \to S$ is an isomorphism iff f is bijective.

2.3.1 Quotient Rings

Let R be a ring with proper ideal I. We define a new ring $(R/I, +, \cdot)$ as follows. I is a normal subgroup of the abelian group R, so $(R/I, +)$ is the usual quotient group, i.e. $a, b \in R, (a + I) + (b + I) = (a + b) + I$. To define multiplication, let $a, b \in R$. Want to set $(a+I)(b+I) = ab+I$. Moreover, the map $\pi : R \to I$, $\pi(a) = a+I$ is a ring homomorphism by construction. And $\ker(\pi) = I$ by group theory.

2.4 Nov. 4, 2019

Remark 2.4.1. If R is a field, the only ideals are $\{0\}$ and R

Proof. Let $I \subset R$ be a nonzero ideal. Then $\exists a \in I - \{0\}$. So $\exists b \in R$ such that $ba = 1$, but so $1 \in I$, $I = R$ $\square$

Remark 2.4.2. If R is a division ring, then only two-sided ideals are $\{0\}$ and R

Proposition 2.4.3. *Let* $f : R \to S$ *be a ring homomorphism, and* R *is a division ring, then* R *is injective.*

Proof. $\ker(f)$ is an ideal of R, $\ker(f) \neq R$ since $\ker(f)$ is a proper ideal. Thus $\ker(f) = 0$, so f is injective. $\square$

2.4.1 Operation of Ideals

Addition: Let I, J be ideals. Then $I + J = \{x + y | x \in I, y \in J\}$ is an ideal. Further if $\{I_j\}$ is a family of ideals, and $\sum I_j = \{x_{j1} + \ldots + x_{jk} | x_{ji} \in I_{ji}\}$, then $\sum I_j$ is an ideal. This holds for left and right ideals.

Example 2.4.4. $R = \mathbb{Z}, I = m\mathbb{Z}, J = n\mathbb{Z}$. $I + J = m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}$.

If R is commutative, and $a_1, \ldots, a_n \in R$, then $(a_1, \ldots, a_n) = (a_1) + \ldots (a_n)$

Multiplication of ideals: Assume R is commutative (unnecessary). Let I, J be ideals. $IJ = I \cdot J = \{\sum x_k y_k | x_k \in I, y_k \in J\}$. IJ is an ideal.

Let $I = (a), J = (b)$, $IJ = \{\sum x_k y_k | x_k \in (a), j_k \in (b)\}$. $x_k = r_k a, y_k = s_k b$, so $\sum x_k y_k = \sum r_k s_k ab$. Thus $IJ \subset (ab)$. $(ab) \subset IJ$ is clear, so $(a)(b) = (ab)$.

2.4.2 Isomorphism Theorems + Chinses Remainder Theorem

Theorem 2.4.5 (Factor Theorem)**.** *Let R be a ring and I be an ideal. Then if S is a ring, there is an bijection between $\{f : R \to S | f(I) = 0\}$, f is a ring homomorphism, and $\{f : R/I \to S\}$ is a ring homomorphism.*

Proof. Hence $\pi : R \to R/I$, $\pi(a) = a + I$. We know π is a ring homomorphism. If $f : R/I \to S$ is a ring homomorphism, consider $f \circ \pi : R \to S$ is a ring homomorphism since $\bar{f}$ and π are ring homomorphisms. That $g : R \to S$ is a map with $I \subset \ker(g)$. Then define $\bar{g} : R/I \to S$ by $\bar{g}(a + I) = g(a)$. We checked that $\bar{g}$ is a ring homomorphism by construction. Thus by the same proof for groups, we prove the factor theorem. □

Theorem 2.4.6. *Let $f : R \to S$ be a ring homomorphism. Recall $im(f) = \{f(x) | x \in R\}$. Then $R/\ker(f) \cong im(f)$ via ring $\bar{f}$, where $\bar{f}(a + \ker(f)) = f(a)$.*

Proof. This is the same as proof of first isomorphism theorem of groups. □

Example 2.4.7. $\mathbb{R}[x]/(x^2 + 1)$ $\exists$ a ring homomorphism $er : \mathbb{R}[x] \to \mathbb{C}$ given $er(p) = p(i)$, where $i = \sqrt{-1}$. $\ker(er) = (x^2 + 1)$. Thus $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Theorem 2.4.8. *Let R be a ring, I, J be ideals. Let $J \subset I$, then $R/I \cong (R/I)/(I/J)$*

Proof. The proof is similar to that of the third isomorphism theorem of groups. □

Theorem 2.4.9. *Let R be a ring, $I \subset R$ ideal, and $S \subset R$ subring. Then $S + I$ is a subring of R. I is an ideal of $S + I$. $S \cap I$ is an ideal of S. If $I \subset R$ is proper, $I \subset S + I$ is proper, $S \cap I \subset I$ is proper, and $S/S \cap I \cong (S + I)/I$.*

Theorem 2.4.10 (Correspondence Theorem)**.** *let R be a ring with proper ideal I, Then $S \to S/I$ gives a bijection from R to all R/I. The inverse map is π^{-1} where π is the canonicle map.*

2.5 Nov. 6, 2019

Let $\{R_i\}$ be a family of rings. Let $\prod R_i = \{(x_i)|x_i \in R_i\}$, the Cartisian product of the R_i. Then $\prod R_i$ is a ring. If $x = (x_i)$, $y = (y_i) \in \prod R_i$, define multiplication and addition coordinate wise. $p_i(\prod R_i) \to R_i$, then each p_i is a ring homomorphism. There is a group homomorphism $J_i : R_i \to R$, but J_i is not a ring homomorphism.

Definition 2.5.1. Let I, J be ideals of a ring R, we say I, J are relatively prime if $I+J = R$.

Remark 2.5.2. If I, J are ideals of a commutative ring, then $IJ \subset I \cap J$. If $I + J = R$, then $IJ = I \cap J$.

Theorem 2.5.3 (Chinses Remainder Theorem)**.** *Let R be a ring with ideas $I_1, \dots I_n$. Assume that if $1 \leq i, j \leq n$ and $i \neq j$, then $I_i + I_j = R$. Consider the map $f : R \to R/I_1 \times \ldots \times R/I_n$, $f(a) = (a + I_1, \ldots, a + I_n)$, Then f is a ring homomorphism.* $\ker(f) = I_1 \cap \ldots \cap I_n$*, and f is surjective.*

Remark 2.5.4. As a consequence, $R/I_1 \cap \ldots \cap I_n \cong R/I_1 \times \ldots \times R/I_n$ by first isomorphism theorem. For $R = F[x]$ where F is a field, we will see that the CRT implies if $b_1, \ldots, b_n \in F, \exists f \in F[x]$ such that $f(a_i) = b_i, \forall i$ and $a_1, \ldots, a_n \in F, a_i \neq a_j$ if $i \neq j$.

2.5.1 Maximal ideals and prime ideals

Definition 2.5.5. Let R be a ring. A proper ideal I of R is called maximal if whenever $I \subset J$, J ideal of R, then $J = I$ or $J = R$.

Example 2.5.6. $R = \mathbb{Z}, I = p\mathbb{Z}$ is maximal iff p is prime.

Theorem 2.5.7. *Every proper ideal is contained in a maxiaml idea.*

Definition 2.5.8. Let S be a set. A partial order $\leq$ on S is a relation such that (i) $a \leq a, \forall a \in S$ (ii) $a \leq b$ and $b \leq a$, then $a = b$. (iii) $a \leq b \leq c$, then $a \leq c$.

A set S with partial order $\leq$ is called a partially ordered set or poset.

Remark 2.5.9. A subset of a poset is a poset.

2.6 Nov. 8, 2019

Definition 2.6.1. Let $(S, \leq)$ be a poset.

1. A subset T of S is called a chain (or totally ordered) if $\forall x, y \in T$, $x \leq y$ or $y \leq x$
2. An element $x \in S$ is called an upper bound of a subset T if $\forall y \in T, y \leq x$
3. And element x of S is called maximal if $y \in S$ and $x \leq y$ implies $x = y$

Lemma 2.6.2 (Zorn's Lemma)**.** *Let S be a nonempty poset. Then if every chain in S has an upper bound in S, then S has a maximal element.*

Zorn's lemma will be treated as an axiom, and is equivalent to the axiom of choice which says every product of nonempty sets is nonempty.

Theorem 2.6.3. *Let I be a proper ideal of a ring R, Then $\exists$ a maximal ideal M of R such that $M \supset I$.*

Proof. Let $S = \{$ proper ideals J of R such that $I \subset J\}$. We say $J_1 \leq J_2$ if $J_1 \subset J_2$. Then $(S, \leq)$ is a poset. Show every chain in S has an upper bound. Let $\{I_j\}$ be a chain in S. Let $\bar{I} = \cup I_j$. Then $\bar{I}$ is an ideal in S. Since $I_j \subset I, \forall j \in J$, then I is an upper bound for the chain in S. Hence, by Zorn's Lemma, $\exists M \in S$ such that if $N \in S$ and $M \subset N$, then $M = N$. Then if $M \subset K$, an ideal of R, then either $K = R$ or K is proper. If K is proper, then $I \subset M \subset K$ so $M = K$. So M is maximal. $\square$

Theorem 2.6.4. *Let R be a commutative ring with ideal I. Then I is a maximal ideal iff R/I is a field.*

Proof. Let I be a maximal ideal. Let $\bar{a} = a + I \in R/I - \{0\}$ so $a \neq I$. Consider the ideal $(a) + I$, $a \in (a) + I$, so $(a) + I \neq I$ and $I \subset (a) + I$. Since I is maximal, $(a) + I = R$. $1 = ra + x$, for some $r \in R, x \in I$. Thus $ra + I = 1 + I$. Thus $(r + I)(a + I) = ra + I = 1 + I$ in R/I. And $r + I$ is a unit of R/I. Hence R/I is a field.

Suppose R/I is a field. Then by discussion we had the only ideal of R/I are $0 + I$ and R/I. Let $J \in R$ be an ideal such that $I \subset J$, by the correspondence theorem, if $\pi : R \to R/I$ is $\pi(a) = a + I$, then $J = \pi^{-1}\pi(J)$. And every ideal of R/I is $\pi(I)$ for some $J \supset I$. Hence $J = \pi^{-1}\pi(0 + I)$ or $J = \pi^{-1}\pi(R)$, so $J = I$ or R, and I is maximal. $\square$

Example 2.6.5. F is a field, $R = F[x]$, M is the maximal ideal of R. Conclude $F[x]/M$ is a field. Note: If R is a ring, $R[x]/(x) \cong R$ so (x) is a maximal ideal of $R \iff R$ is a field.

Definition 2.6.6. A proper ideal P of a commutative ring R is called a *prime ideal* if $ab \in P$ for $a, b \in R$, then $a \in P$ or $b \in P$.

Example 2.6.7. If $R = \mathbb{Z}$ and $M > 0$, $m\mathbb{Z}$ is a prime ideal iff m is prime. Further $\{0\} = 0\mathbb{Z}$ is a prime ideal.

Theorem 2.6.8. *Let R be a commutative ring with proper ideal I, then I is prime iff R/I is a integral domain.*

Proof. If I is a prime ideal. Let $a + I, b + I \in R/I$. Suppose $(a + I)(b + I) = 0 + I$. Hence $ab + I = 0 + I$, $ab \in I$. So $a \in I$ or $b \in I$. By defintion of a prime, so $a + I = I$ or $b + I = I$. Thus R/I is an integral domain. The other way is clear. $\square$

Corollary 2.6.9. *If R is a commutative ring, then every ideal M is prime.*

Proof. R/M is a field, so is a integral domain. So M is prime. $\square$

Note: R is an integral domain iff (0) is a prime ideal.

Example 2.6.10. Let $R = \mathbb{Z}[x]$ $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ which is a domain but not a field. So (x) is a prime ideal but not maximal. But $(2, x)$ is a maximal and prime ideal.

2.6.1 $R[x]$

R be a ring, let $\phi : R \to S$ be a ring homomorphism. let $C_S(\phi(R))$ be the centralizer of $\phi(R)$. $C_S(\phi(R))$ is a subring.

Proposition 2.6.11 (Universal Properties)**.** *Let $\alpha \in C_S(\phi(R))$. Then $\exists!$ ring homomorphism $e_\alpha : R[x] \to S$ such that $e_\alpha(r) = \phi(r)$ if $r \in R$ and $e_\alpha(x) = \alpha$.*

2.7 Nov. 11, 2019

Example 2.7.1. Take $R = \mathbb{Q}$, $S = \mathbb{C}$, $\alpha = i = \sqrt{-1}$, then $e_\alpha : \mathbb{Q}[x] \to \mathbb{C}$, $e_\alpha(\sum r_j x^j) = \sum r_j i^j$

Definition 2.7.2. A polynomail g in $R[x]$ is called *monic* if its leading coefficient is 1, i.e., if $\deg(g) = d \geq 0$ and $g = a0 + a_1 x + \ldots + x^d$.

Proposition 2.7.3. *Let $f, g \in R[x]$ with g monic, then $\exists h, r \in R[x]$ such that $f = hg + r$ with $\deg(r) < \deg(g)$ or $r = 0$ (division algorithm)*

Remark 2.7.4. If $g = a_0 + a_1 x + \ldots + a_d x^d$ with $a_d \in R^\times$ a unit, then $g = a_0 g_0$ where $g_i = \sum \frac{a_i}{a_0} x^i \in R[x]$. g_0 is monic so any $f = hg_0 + r$ then $f = \frac{h}{a_0} g + r$, so the division algorithm holds if $l(g) = a_d \in R^\times$. If F is a field, then division algorithm helds for any nonzero g.

Remark 2.7.5. Let $g \in R[x]$ be monic of degree d, then $R[x]/(g) = \{b_0 + b_1 x + \ldots + b_{d-1} x^{d-1} + (g(x))$

Example 2.7.6. $\mathbb{Q}[x]/(x^2+1) \cong \{a + bx + (x^2+1) | a, b \in \mathbb{Q}\}$

Example 2.7.7. $\mathbb{Z}[x]/(x^3 - x + 1) \cong \{a_0 + a_1 x + a_2 x^2 + (x^3 - x + 1) | a_0, a_1, a_2 \in \mathbb{Z}\}$

Example 2.7.8. $\mathbb{Q}[x]/(x^2+1) \cong \mathbb{Q}[i]$. pf: $e_i : \mathbb{Q}[x] \to \mathbb{C}$, $\alpha = i$, $R = \mathbb{Q}$, $S = \mathbb{C}$. e_i is a ring homomorphism. $\ker(e_i) = \{f \in \mathbb{Q}[x] | f(i) = 0\}$. $x^2 + 1 \in \ker(e_i)$. If $f \in \ker(e_i)$, then $f = h(x^2+1) + r$. where $\deg r < 2$. Then apply ring homomorphism, we find $r \in (x^2+1)$. Thus $\ker(e_i) = (x^2+1)$. Then we use the first isomorphism theorem to see $Q[x]/(x^2+1) \cong \mathbb{Q}[i]$.

Theorem 2.7.9 (Remainder Theorem)**.** *Let $f \in R[x]$ and let $\alpha \in R$*

1. *$\exists h \in R[x]$ such that $f = h(x - \alpha) + f(\alpha)$*
2. *Let R be an integral domain. Then $f(\alpha) = 0$ iff $x - \alpha \mid f$ in $R[x]$.*

Definition 2.7.10. Let R be an integral domain, and let $f \in R[x]$. We say α is a root of f if $f(\alpha) = 0$. If α is a root of f, we say α is a root of multiplicity m_α of $(x-\alpha)^{m_\alpha} \mid f$ in $R[x]$, but $(x - \alpha) \nmid f$.

Theorem 2.7.11. *Let R be a domain and let $f \in R[x]$ have degree $d \geq 0$, then f has at most d roots in R.*

2.8 Nov. 13, 2019

Definition 2.8.1. A ring R is called a principal ideal ring if every ideal is principal. A principal ideal domain (PID) is an integral domain that is a principal ideal ring.

Example 2.8.2. $\mathbb{Z}$ is a PID, since every ideal I is a subgroup. So $I = n\mathbb{Z} = (n)$. $\mathbb{Z}[x], \mathbb{Z}[\sqrt{-5}]$ are not PID's

Definition 2.8.3. R is a Euclidean domain if $\exists \psi : R - \{0\} \to \mathbb{Z}_{>0}$ such that if $b, a \in R$ and $a \neq 0$, then $\exists q, r \in R$ with $b = qa + r$ and $r = 0$ or $\psi(r) < \psi(a)$.

Example 2.8.4. $R = \mathbb{Z}$, $\psi(a) = |a|$. F is a field, $R = F[x]$. Let $\psi(p) = \deg(p)$ for $p \in R - \{0\}$. $F[x]$ is a Euclidean domain.

Theorem 2.8.5. *If R is a Eudclidean domain, then R is a PID.*

Proof. Let $I \subset R$ be an ideal. If $I = \{0\}$, $I = (0)$. If $I \neq \{0\}$, choose $a \in I - \{0\}$ so $\psi(a) \leq \psi(b), \forall b \in I - \{0\}$. Then $a \in I$, so $(a) \in I$. Show $I \in (a)$. If $b \in I, b = qa + r$, with $q \in R, r \in Q$ and $r = 0$, then $\psi(r) < \psi(a)$, contradiction to the choice of $\psi(a)$. Thus $r = 0$, $b = qa \in (a)$. □

Example 2.8.6. Let $d \in \{-2, -1, 2, 3\}$. Then $\mathbb{Z}[\sqrt{d}]$ is a Euclidean domain. And hence a PID. Esp $\mathbb{Z}[i]$ is a PID.

Proof. Let $\psi(\alpha) = |N(\alpha)|$ for $\alpha \in \mathbb{Z}[\sqrt{d}]$. If $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ and for $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Z}$, $N(\alpha) = \alpha\tau(\alpha)$ where $\tau(\alpha) = a - b\sqrt{d}$, then $N(\alpha\beta) = N(\alpha)N(\beta)$. Similarly, one can show the same result for $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$. Let $\alpha, \beta \in R = \mathbb{Z}[\sqrt{d}], \beta \neq 0$, then $\alpha/\beta \in \mathbb{Q}[\sqrt{d}]$. Thus $\frac{\alpha}{\beta} = x + y\sqrt{d}$ with $x, y \in \mathbb{Q}, \exists x_0, y_0 \in \mathbb{Z}$ such that $|x - x_0| \leq \frac{1}{2}$, $|y - y_0| \leq \frac{1}{2}$. Let $q = x_0 + y_0\sqrt{d}$, then $\frac{\alpha}{\beta} = q + r$. Thus $\alpha = q\beta + s\beta$ and we set $r = s\beta = \alpha - q\beta \in R$. To show $\psi(r) < \psi(\beta)$. But $\psi(r) = \psi(s\beta)$. So need to show $|N(s)| < 1$. If $\gamma = u + v\sqrt{d}$, by computation, $|N(s)| = \frac{1}{2} < 1$. □

Remark 2.8.7. Since R is a domain, if $a \in R - \{0\}$ and $b, c \in R$ and $ab = ac$, then $b = c$.

Definition 2.8.8.

1. Let $a, b \in R - \{0\}$. We say a and b are associates if $b = ua$, $u \in R^\times$
2. Let $a \in R - \{0\}$, $a \notin R^\times$. We say a is irreducible if $a = bc$ with b and $c \in R$, then b or c is a unit.
3. Let $a \in R - \{0\}$, $a \notin R^\times$. We say a is prime if whenever $a \mid bc$ with $b, c \in R$. Then $a \mid b$ or $a \mid c$.

Remark 2.8.9. Let $a, b \in R - \{0\}$.

1. $a \in R^\times \iff (a) = R$
2. a and b are associates $\iff (a) = (b)$

3. $a \mid b \in R \iff b \in (a)$

4. Let $a \mid b$. Then a and b are not associates $\iff$ $(b) \subset (a)$ but $(b) \neq (a)$.

Proposition 2.8.10. *If $x \in R$ is prime, then x is irreducible.*

Definition 2.8.11. Let R be any ring. We say R satisfies the ascending chain condition (acc) on ideals if for every sequence $I_1 \subset I_2 \subset \ldots I_n \subset \ldots$. $\exists n_0 \geq 0$ such that $I_n = I_{n_0}$ (increasing sequences stabilize). We say R satisfies acc on principal ideals if the above is true for chains $I_1 \subset I_2 \subset \ldots$ for principal ideals I_j. We say R is Notherian if it satisfies acc on ideals.

Theorem 2.8.12. *If R is a PID, then R is Noetherian.*

2.9 Nov. 15

2.9.1 Unique Factorization domain

Definition 2.9.1. A *Unique factorization domain* (UFD) is an integral domain R satisfying the following properties:

1. Every nonzero element $a \in R$ can be expressed as $a = up_1 \ldots p_n$, where u is a unit and the p_i's are irreducible

2. If a has another factorization, say $a = vq_1 \ldots q_m$,where v is a unit and the q_i's are irreducible, then $n = m$ and, after reordering if necessary, p_i and q_i are associates for each i.

Remark 2.9.2. Let $a \in \mathbb{Z}[\sqrt{d}$, d is square free integer < 0. Then if $N(a) = p$ is a prime in $\mathbb{Z}$, then α is irreducible ($N(a) = a\bar{a}$).

Theorem 2.9.3. *Let R be an integral domain*

1. *If R is a UFD, and $(a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset \ldots$ is an increasing chain with $a_i \in R$, then $\exists n_0 \geq 0$ such that if $n \geq n_0$, $(a_n) = (a_{n_0})$.*

2. *If R is a PID, then R is a UFD.*

2.10 Nov. 18, 2019

Proposition 2.10.1. *Let R be a UFD. Then if $a \in R$ is irreducible, a is prime.*

Remark 2.10.2. To prove that a PID is a UFD, we essentially showed that if R satisfies acc on principal ideals, then R is a UFD. Then converse is also true. R is a PID iff R is a UFD and every nonzero prime ideal is maximal. We essentially proved the converse is also true.

2.10.1 Rings of Fraction

Definition 2.10.3. Let $S \subset R$ be a subset, we say S is multiplicatively closed if $0 \notin S$, $1 \in S$, $a, b \in S$, then $ab \in S$.

Example 2.10.4. $a \in R$ is not nilpotent, so $a^n \neq 0, \forall n > 0$. Let $S = \{a^n | n \geq 0\}$, where $a^n = 1$. S is multiplicative closed since $a^n a^m = a^{m+n}$

Example 2.10.5. Let $P \subset R$ be a prime ideal. Let $S = R - P = \{a \in R | a \notin P\}$. Since P is prime, $a, b \notin P, ab \notin P$. S is multiplicatively closed.

Example 2.10.6. Let R be an integral domain. Then $S = R - \{0\}$ is multiplicatively closed since $(0) = \{0\}$ is a prime ideal.

Goal: Deinfe a new ring $S^{-1}R$ whose elements are written $\frac{a}{s}, a \in R, s \in S$. Consider the set $R \times S = \{(a, s) | a \in R, s \in S\}$. If $(a, s), (a_1, s_1) \in R \times S$, we say $(a, s) \sim (a_1, s_1)$ if $\exists t \in S$ such that $ts_1 a = tsa_1$. Claim, $\sim$ is an equivalent relation. This is easy to prove. We let $S^{-1}R =$ Equivalence classes of pairs (a, s) in $R \times S$. Write $a/s = [(a, s)]$ equivalent class in $S^{-1}R$ of (a, s).

Theorem 2.10.7. *$(S^{-1}R, +, \cdot)$ is a ring.*

Note: If $s \in S$, $\frac{0}{s} = \frac{0}{1}$. Set $0_{S^{-1}R} = \frac{0}{1}$. Associativity of multiplication and distributive property are routine.

Remark 2.10.8. If $a \in S$, and $s \in S$, then $\frac{a}{s}$ is a unit of $S^{-1}R$. Indeed, $\frac{s}{a} \in S^{-1}R$ since $a \in S$, and $\frac{a}{s}\frac{s}{a} = \frac{1}{1} = 1_{S^{-1}R}$

If R is a domain, and $S = R = \{0\}$. Then $S^{-1}R$ is a field. Indeed, let $r \in R$, $s \in S$. If $f \notin 0$, then $r \notin 0$, so $r \in S = R - \{0\}$. By (i), $\frac{r}{s} \in (S^{-1}R)^{\times}$, so $S^{-1}R$ is a field.

Notation: Let $Frac(R) = S^{-1}R$, $S = R - \{0\}$, and call $Frac(R)$ the fraction field of R.

Note: If R is a domain, we don't need the definition of $S^{-1}R$.

2.11 Nov. 20, 2019

2.11.1 Lattice

Define $S^{-1}R = \{\frac{r}{s} | r \in R, s \in S\}$ where $S \subset R$ is a multiplicative closed subset.

Proposition 2.11.1. *The map $f : R \to S^{-1}R$ given by $f(a) = a/1$ is a ring homomorphism, and $\ker(f) = \{r \in R | \exists s \in S$ such that $sr = 0\}$. If S has no zero devisors, then f is injective. Hence, f is injective if R is an integral domain.*

Example 2.11.2. let $R = \mathbb{Z}_6$, $S = (3)$, $f : R \to S^{-1}R$, $f(r) = r/1$, $\ker(f) = \{r \in \mathbb{Z}_6 | 3r = 0\} = \{0, 2, 4\}$

Note: Ideals of $S^{-1}R$ are essentially the ideals of R which doesn't meet S.

Remark 2.11.3. Let A be a ring and let $a \in A$, unit of A. Then $\exists b \in A$ such that $ba = 1$ and $b \in A^\times$. Since $A^\times$ is a group under multiplication, then the element b is unique since it is the inverse of a. Hence we can write $b = a^{-1}$

Theorem 2.11.4 (Universal Property of localization)**.** *Let R be a ring with multiplicatively closed set S. Let $\phi : R \to A$ be a ring homomorphism such that $\phi(s) \in A^\times, \forall s \in S$. Then $\exists!$ ring homomorphism $\bar{\phi} : S^{-1}R \to A$ such that $\bar{\phi} \circ f = \phi$. In fact, $\phi(\bar{r/s}) = \phi(s)^{-1}\phi(r)$.*

Let R be a ring (assume commutativity). Let $R[x_1, \dots, x_n] = \{\sum a_i x^i | a_i \in R\}$ If $p = \sum a_i x^i$, $q = \sum b_i x^i \in R[x_1, \dots, x_n]$, then we define addition and multiplication as we do in one variable polynomial. then $(R[x_1, \dots, x_n], +, \cdot)$. If $a_1, \dots, a_n \in S$, and $\phi : R \to S$ is a ring homomorphism, $\exists!$ evaluation ring homomorphism, $e_a : R[x_1, \dots, x_n] \to S$, such that $e_a(\sum a_i x^i) = \sum \phi(a_i) a^i$, where $a^i = a_1^{i_1} \dots a_n^{i_n}$. Verifying this is like te case $n = 1$, as a consequence, $R[x_1, \dots, x_n] \cong R[x_1, \dots, x_{n-1}][x_n]$. Hence $R[x_1, \dots, x_n] \cong R[x_1] \dots [x_n]$. Hence is R is a integral domain, $R[x_1, \dots, x_n]$ is likewise.

Let R be a UFD. Let $F = frac(r)$ and regard $R \subset F$ via $f : R \to F$. Let $\{p_i | i \in I\}$ be the nonzero principal prime ideals of r, for each p_1, choose a prime p_i of R such that $p_i = (p_i)$. p_i is unique up to a unit. If $(p_i) = (p_j)$, then $p_i = p_j$ by choice. Note each p_j is irreducible. Let $P = \{p_i | i \in I\}$. If $R = \mathbb{Z}, P = \{$ primes $p > 0\}$. If $R = k[x], k$ is a field, take $P = \{f | f$ monic irreducible polynomial$\}$.

Remark 2.11.5. Let $p \in P$, if $\alpha \in F^\times$, then $\alpha = p^e a/b$, with $a, b \in R$, $p \nmid a, p \nmid b$. And $e \in \mathbb{Z}$, e is independent of choices.

Definition 2.11.6. Set $ord_p(\alpha) = e$. $\forall \alpha \in F^\times, ord_p(\alpha) = 0$ except for a finite set of p, so we can define $c(\alpha) = \prod_{p \in P} p^{ord_p(\alpha)}$. Thus $e(\alpha) = u\alpha$, somce $u \in R^\times$. Set $ord_p(0) = \infty$, $\forall k \in \mathbb{Z}$.

2.12 Nov. 22, 2019

Definition 2.12.1. If $f \in R[x] - \{0\}$, then we say f is primitive if $c(f) = 1$.

Remark 2.12.2. Let $f \in F[x] - \{0\}$. Then $f = c(f) f_0$, where f_n is primitive and in $R[x]$

Theorem 2.12.3 (Gauss Lemma)**.** *Let R be a UFD, $F = frac(R)$ let $f, g \in F[x] - \{0\}$. Then $c(fg) = c(f)c(g)$.*

Proof. Let $f = c(f) f_0, g = c(g) g_0$ with f_0, g_0 primitive. Then $fg = c(f)c(g) f_0 g_0$, so $c(fg) = c(f)c(g)c(f_0 g_0)$. Suffices to show that if f_0, g_0 are primitive in $R[x]$, then $c(f_0 g_0) = 1$. Since f_0 is primitive in $R[x]$, $\exists$ prime p in P, $p \nmid f_0$. $\pi_p(f_0) \neq 0$. Similarly, $\forall p \in P$, $\pi_p(g_0) \neq 0$. But $\pi(f_0 g_0) = \pi(f_0)\pi(g_0) \neq 0$ since $R/(p)[x]$ is a domain. Thus $\forall p \in P, p \nmid f_0 g_0$, so $p \nmid c(f_0 g_0)$ so $c(f_0 g_0) = 1$. ◻

Proposition 2.12.4. *Let $f \in R[x]$ and assume $\deg(f) > 0$. Then f is irreducible in $R[x]$ iff R is primitive in $F[x]$.*

Theorem 2.12.5. *Let R be a UFD, then $R[x]$ is a UFD.*

Proof. Let $f \in R[x] - \{0\}$. But $f \in F[x] - \{0\}$, and $F[x]$ is a PID. So $f = af_1 \dots f_n$ with $a \in F^\times$, $t_1 \dots, t_d \in F[x] - \{0\}$ irreducible. By a remark, $t_i = c_1 f_i$ with $c_i = c(t_i)$, thus $f = ac_1 \dots c_d f_1 \dots f_d$. But each $f_i = \frac{1}{c_1} t_i$ is irreducible in $F[x]$ since $\frac{1}{c_i} \in F^\times$. And each f_i is primitive in $R[x]$, so each f_i is irreducible in $R[X]$. Thus $f = acf_1 \dots f_d$, with $c = c_1 \dots c_n$. But $c(f) = c(ac)c(f_1 \dots f_n)$, and by Gauss lemma and easy induction, $c(f_1, \dots f_n) = 1$. Thus $c(f) = c(ac) = uac$. So $ac \in R$. Since $ac \in R - \{0\}$, we can write $ac = uq_1 \dots q_d$ with $u \in R^\times, q_1, \dots, q_n$ irreducibles of R. Each irreducible $q_i \in R$. $\square$

Corollary 2.12.6. *If R is a UFD, then $R[x_1, \dots, x_n]$ is a UFD*

Proof. By induction. $\square$

Example 2.12.7. $\mathbb{Z}[x_1, \dots, x_n]$ and $F[x_1, \dots, x_n]$ are UFD's.

Note: $\mathbb{Z}[x_1, \dots, x_n]$ is not a PID if $n \geq 1$, and $F[x_1, \dots, x_n]$ is not a PID if $n \geq 2$.

2.13 Nov. 25

Theorem 2.13.1 (Eisenstein Criterion)**.** *Let R be a UFD with quotient field F,and let $f(X) = a_n X^n + \dots + a_1 X + a_0$ be a polynomial in $R[X]$, with $n \geq 1$ and $a_n \neq 0$. If p is prime in R, p divides a_i for $0 \leq i < n$, but p does not divide a_n and p^2 does not divide a_0, then f is irreducible over F. Thus,if f is primitive then f is irreducible over R.*

Example 2.13.2. Let p be a prime. Let $f(x) = 1 + x + \dots x^{p-1}$. Then f is irreducible in $\mathbb{Q}[x]$. To see this, we show that $f(x+1)$ is eisenstein, And $f(x)$ is irreducible in $\mathbb{Q}[x]$ iff $f(x+1)$ is irreducible in $\mathbb{Q}[x]$.

Proof. Let R be a commutative ring, and let $a \in R$. Let $T_a : R[x] \to R[x]$ be the unique ring homomorphism such that $T_a(r) = r, \forall r \in R$, and $T_a(x) = x + a$. If $b \in R$, then $T_a T_b(r) = r, \forall r \in R$ And $T_a T_b(x) = x + a + b$. $T_{a+b} = T_a \circ T_b$ on R and x, and sine these generate $R[x]$ as a ring, then $T_{a+b} = T_a \circ T_b$ on $R[x]$. But $T_0 = Id_{R[x]}$, so $T_a : R[x] \to R[x]$ is an isomorphism of $R[x]$. Hence $f(x) \in R[x]$ is irreducible iff $T_a f(x)$ is irreducible. $\square$

Example 2.13.3. Let $f = f(x, y) = y^5 - x^3 y^4 + x^2 y + 2xy$ in $\mathbb{C}[x, y]$. Then f is irreducible in $\mathbb{C}[x, y]$.

Proof. Regard $f \in R[y] = \mathbb{C}[x][y] = \mathbb{C}[x, y]$, where $R = \mathbb{C}[x]$. Then $f = y^5 + (-x^3)y^4 + (x^2)y + (2x)y$. R is a UFD, and x is irreducible in R. So x is prime in R. And f is Eisenstein for the prime x. Let $F = \mathbb{C}[x] = Frac(\mathbb{C}[x])$. Therefore, f is irreducible in $F[x] = \mathbb{C}(X)[y]$. But f is primitive in $R[y]$ since $a_5 = 1$, so f is irreducible in $R[y] = \mathbb{C}[x, y]$. $\square$

Example 2.13.4. $f = x_1^2 + x_2^2 + x_3^2$ is irreducible in $\mathbb{C}[x_1, x_2, x_3]$

Proof. Let $R = \mathbb{C}[x_2, x_3]$, so $\mathbb{C}[x_1, x_2, x_3] = R[x_1]$, $f = x_1^2 + a_0$. Note R is a UFD. Find a prmitive R so that f is Eisenstein for p. Our $a_0 = (x_2 + ix_3)(x_2 - ix_3)$, and $x_2 + ix_3$ is irreducible in R since it is prime. Then f is Eisenstein for $p = x_2 + ix_3$, and f is irreducible in $F[x_1]$ where $F = \mathbb{C}(x2, x_3)$. f is irreducible in $R[x_1]$. □

2.13.1 Characteristic of a ring

Let R be a ring. Consider the unique ring homoomrphism $\phi : \mathbb{Z} \to R$, $\phi(n) = n \cdot 1_R$. Then $\ker(\phi)$ is a proper ideal of $\mathbb{Z}$, so $\ker(\phi) = n\mathbb{Z}$, $n \neq 1$, $n \geq 0$

Definition 2.13.5. The characteristic $\mathrm{Char}(R)$ of R is n.

In R, $n \cdot a = 0, \forall a \in R$, since $n \cdot a = (1n)a = 0a = 0$. If R is an integral domain, then $\mathrm{Char}(R) =$ a prime or 0.

Example 2.13.6. $\mathrm{Char}(\mathbb{Z}/n\mathbb{Z}) = n, \forall n \neq 1$, $\mathrm{Char}(R[x]) = \mathrm{Char}(R)$.

Remark 2.13.7. If $\mathrm{Char}(R) = p$ is prime, and $a, b \in R$, and $ab = ba$, then $(a+b)^p = a^p + b^p$.

Chapter 3

Module Theory

3.1 Dec. 2, 2019

Definition 3.1.1. Let R be a ring, not necessarily commutative. A *(left) R-module* is an abelian group $(M, +)$ with a map $R \times M \to M$, with $(r, m) \mapsto r \cdot m$, such that $\forall s, r \in R$, $m, r \in M$,

1. $r(m + n) = rm + rn$
2. $(r + s)m = rn + sm$
3. $(rs)m = r(sm)$
4. $1m = m$

Remark 3.1.2. If R is a field, a R-module is the same as a vector space.

Remark 3.1.3. $\mathbb{Z}$ modules are same as abelian groups. Indeed, given a $\mathbb{Z}-$module $(M, +)$ is an abelian group structure. Conversely, if $(M, +)$ is an abelian group, we define a map $\mathbb{Z} \times M \to M$ by $(m, n) \mapsto mn = n + \ldots + n$ if $n > 0$, setting $0m = 0, \forall m \in M$ and if $n < 0$, set $nm = (-n)m$. Check this makes M a $\mathbb{Z}-$module.

Proposition 3.1.4. *let $0_R = 0$ in R, $0_M = 0$ in M. Then $\forall r \in R$, $m \in M$*

1. $r0_M = 0_M$
2. $0_R m = 0_M$
3. $(-r)m = r(-m)$
4. *if $r \in R^\times$ and $rm = 0_M$, then $m = 0_M$*

Let $R^n = \{(x_1, \ldots, x_n | x_i \in R\}$, R^n is an abelian group via component wise operations. If $r \in R, x = (x_1, \ldots, x_n) \in R^n$, let $rx = (rx_1, \ldots, rx_n)$ can check R^n is a $R-$module. If $n = 1, R^n = R$ which is a R-module by $(r, x) \mapsto rx$.

Definition 3.1.5. Let M be a R-module, a subset N of M is called a submordule if N is a subgroup of $(M,+)$, and $\forall r \in R, x \in N, rx \in N$. Can check N itself is a R-module.

Example 3.1.6. $R = \mathbb{Z}$, $N = \{(x_1, x_2) \in \mathbb{Z}^2 | x_1 + x_2 \in 2\mathbb{Z}\}$. Can check easily that N is a submodule.

Remark 3.1.7. If R is a ring, then the left ideals I of R are the submodules of R. Indeed, if $I \subset R$ is an left ideal, I is a subgroup of $(R,+)$, and if $r \in R$ and $x \in I$, then $rx \in I$ by definition of left ideal, so I is a submodule. Converse is similar. If R is commutative, submodules are the same as ideals.

Definition 3.1.8. Let M, N be R-modules, a map $f : M \to N$ is called a R-module homomorphism, if $f(x+y) = f(x) + f(y)$, $f(rx) = rf(x), \forall r \in R, x, y \in M$.

Remark 3.1.9. Let $Q \subset M$ be a submodule, $f : M \to N$ be an R-module homomorphism. Then $f(Q)$ is a submodule of N. Indeed, $f(Q)$ is a subgroup of N by 1.3. If $r \in R, y \in f(Q)$, $y = f(x)$, some $x \in Q$, so $ry = rf(x) = f(rx) \in f(Q)$.

Let $P \subset N$ be a submodule, and let $f : M \to N$ be a R-module homomorphism. Let $f^{-1}(P) = \{x \in M | f(x) \in P\}$. Then $f^{-1}(P)$ is a submodule of M, $f^{-1}(P)$ is a subgroup of M by group theory. And if $x \in f^{-1}(P)$, and $r \in R$, then $f(rx) = rf(x) \in P$ since P is a submodule, so $rx \in f^{-1}(P)$.

Remark 3.1.10. If M is a R-module, then $\{0\}$ and M are always submodules. Hence if $f : M \to N$ is a R-module homomorphism, then $Im(f) = f(M)$ is a submodule of N and $\ker(f) = f^{-1}(\{0\})$ is a submodule of M.

Notation: If M, N are R-modules, then $Hom_R(M, N) = \{f : M \to N | f$ is a R-module homomorphism$\}$.

Example 3.1.11. Let $R = F[x, y]$, F is a field, let $N = (x, y) = \{rx + sy | r, s \in R\} =$ ideal generated by x, y. We can define $f : R^2 \to N$ by $f(r, s) = rx + sy$. Can check that $f \in Hom_R(R^2, N)$, f is surjective.

Remark 3.1.12. If M is a R-module, and $v \in M$. Then $Rv = \{rv | r \in R\}$ is a submodule of M. Further, $f : R \to Rv$, $f(r) = rv$ is a R-module homomorphism.

Definition 3.1.13. $Ann_R(v) = \{r \in R | rv = 0\} = \ker(f)$.

3.1.1 Direct products and direct sums

Let $\{M_i\}$ be a family of R-modules. Let $\prod M_i = \{(x_i) | x_i \in M_i\} =$ set theory product of M. Define $\forall j \in I$, $p_j : \prod M_i \to M_j$, where $p_j((x_i)) = x_j$. If $I = \{1 \ldots, n\}, \prod M_i = M_1 \times \ldots \times M_n$.

Let $\bigoplus M_i = \{(x_i) \in \prod M | x_i = 0, \forall i$ outside of finite subset of $I\}$. If $I = \mathbb{Z}_{>0}$, and each $M_i = R$, then $\prod M_i = \{(x_i) | x_i \in R\}$ and $\bigoplus M_i = \{(x_1, \ldots, x_n, 0, \ldots) | x_i \in R, \exists n_0 > 0$ such that $x_n = 0 \forall n \geq n_0\}$

Note: $\forall I, \bigoplus M$ is a submodule of $\prod M_i$. Indeed, if $x = (x_i) \in \prod M_i$, set $supp(x) = \{i \in I | x_i \neq 0\}$, then $x \in \bigoplus M \iff supp(x)$ is finite. If $x, y \in \prod M$ and $r \in R$, then $supp(X + y) \subset supp(x) \cup supp(y)$, $supp(rx) \in supp(x)$. Hence $\bigoplus M$ is a submodule of $\prod M$. Further $\bigoplus M_i = \prod M_i$ iff I is finite.

Universal property of $\prod M_i$. Suppose we are given a R-module N and $\forall j \in I$, we are given $f_j : N \to M_j$. Then $\exists! R-$module homomrophism $N \to \prod M_i$ such that $p_j \circ f_j, \forall j \in I$ if $y \in N, f(y) = (f_i(y))$

Universal property of $\bigoplus M_i$ for $j \in I$, define $q_j : M_j \to \bigoplus M_i$ by $q_j(x) = \{(X_j)|x_i = 0, x_j = x\}$ then q_j is a $R-$module homomorphism. Given $g_j : M_j \to N, \forall j$. Then $\exists!$ R-module homomrophism $g : N \to \bigoplus M_i$ such that $g \circ g_j = q_j$.

3.2 Dec.4, 2019

3.2.1 Quotient

Let M be a R-module, with submodule N. Then $M/N = \{x + N | x \in M\}$ is a R-module via action $(r, x + N) \to rx + N$, for $r \in R$, $x \in M$. Well-defined: if $x + N = y + N$, then $y = z + x$, where $z \in N$. And $r(y + N) = r(x + z) + N = rx + rz + N = rx + N = r(x + N)$. Checking M/N is a R-module is routine. $\pi : M \to M/N$, $\pi(x) = x + N$ is a R-module homomorphism. $\ker(f) = N$ and π is surjective.

Example 3.2.1. $R = \mathbb{Z}, M = \mathbb{Z}^2.N = \{(x, y)|x + y \in 2\mathbb{Z}\}$.

Remark 3.2.2. Let M, N, P be R-modules, let $f \in Hom_R(M, N), g \in Hom_R(N, P)$. Then $g \circ f \in Hom_R(M, R)$. Check is routine

3.2.2 Isomorphism Theorems

Let M, N, P be R-modules, $N \subset M$ is a submodule. Let $Hom_R(M, P)_N = \{f \in Hom_R(M, P)|N \subset \ker(f)$. Define $\pi^* : Hom_R(M/N, P) \to Hom_R(M, P)$ by $\pi^*(f) = f \circ \pi \in Hom_R(M, P)$ by last remark.

Theorem 3.2.3. *$\pi^* : Hom_R(M/N, P) \to Hom_R(M, P)_N$ is a bijection. In particular, if $g \in Hom_R(M, P)_N$ then $g = \pi^*(\bar{g})$, for unique $\bar{g} \in Hom_R(M/N, P)$, and $\bar{g}(x + N) = g(x), \forall x \in M$.*

Theorem 3.2.4 (First Isomorphism Theorem)**.** *If $f \in Hom_R(M, P)$ and $K = \ker(f)$, then $\bar{f} : M/N \to im(f)$ is a R-module isomorphism, where $\bar{f}(x + K) = f(x)$. If f is surjective, then M/K is isormophic to P.*

Let $\{M_i\}$ be a family of submodules of M. $\forall j \in I$, we have $\alpha_j : M_j \to M$, $\alpha_j(x) = x$. By universal property of $\bigoplus M$, we get $!R$-module homomorphism $\alpha : \bigoplus M_i \to M$, $\alpha((x)) = \sum x_i$. Let $\sum M_i = im(\alpha)$, so $\sum M = \{x_1 + \ldots + x_i\}$. Conclude that $\sum M_i$ is a submordule of M as image of R-modules.

If S is also a submodule of M, then $N + S = \{x + y|x \in N, y \in S\}$. As above, $N + S$ is a submodule. So is $N \cap S$.

Theorem 3.2.5 (Second Isomorphism Theorem). $(N+S)/N \cong S/(S \cap N)$

Theorem 3.2.6 (Third Isomorphism Theorem). *Let $N \subset S$ submodules of M. Then $M/N \cong (M/N)/(S/N)$. $S/N = \pi(S)$, $\pi : M \to M/S$.*

Theorem 3.2.7 (Correspondence theorem). *Let $S(M)$ be the submodules of M. Let $S_N(M)$ be the submodules P of M such that $N \subset P$; Let $\pi : M \to M/N$, $\pi(x) = x+N$. Then $\pi^{-1} : S(M/N) \to S_N(M), P \to \pi^{-1}(P)$ is bijective. Its inverse is $Q \to \pi(Q)$ for $Q \in S_N(M)$.*

Recall: If M is a R-module, and $r \in M$, $Ann_R(x) = \{r \in R | rx = 0\}$. $\phi_v : R \to Rv$, $\phi_v(r) = rv$ is a R-module homormophism and $\ker(\phi_v) = Ann_R(v)$. Note: $Ann_R(v)$ is a left ideal of R.

Let $Ann_R(M) = \{r \in R | ru = 0, \forall u \in M\} = \cap Ann_R(u).Ann_R(M)$ is a 2-sided ideal.

Lemma 3.2.8. *1. $R/Ann_R(v) \cong R_v$ as a R-module*

2. If R is commutative, $Ann_R(v) = Ann_R(Rv)$ so $R/Ann_R(Rv) \cong Rv$

Definition 3.2.9. A R-module M is *cyclic* if $\exists v \in M$ such that $M = Rv$.

Example 3.2.10. R ring, $I \subset R$ left ideal, then $R/I = R(1+I)$ is cyclic. $Ann_R(1+I) = J$.

Example 3.2.11. F field, $R = M(n, F)$. Take $M = F^n = \{(a_1, \ldots, a_n) | a_i \in F\}$. R acts on M by $(A, v) \to A(v)$. $M = Re_n$. $Ann_R(e_n) \neq Ann_R(M)$.

Definition 3.2.12. Let M be a R-module, let $S = \{x_i\}$ be a subset of M. We say M is linearly independent over R if for $n \geq 0$, $r_{i_1}, \ldots, r_{i_n}, r_{i_1}x_{i_1} + \ldots + r_{i_n}x_{i_n} = 0$ if each $r_{i_j} = 0$ where $i_1, \ldots, i_n \in I$. We say S spans M over r if $M = \sum Rx_i$. We say S is a basis over M if S spans M and S is linearly independent.

Remark 3.2.13. A maximal linearly independent set need not be a basis.

Example 3.2.14. $R = \mathbb{Z}$, $M = R$, $S = \{2\}$ is maximal linearly independent over $\mathbb{Z}$, but $2R = 2\mathbb{Z} \neq \mathbb{Z}$ so S doesn't span.

3.3 Dec. 6, 2019

Definition 3.3.1. M is a *finitely generated* R-module if $\exists$ a finite S that spans M over R.

Definition 3.3.2. We say M is a free R-module if M has a basis.

Remark 3.3.3. Let S be a R-basis of M. Let $R^{\oplus I} = \{(r_i) | r_i \in R$ and $r_i = 0$ for all i outside of a finite subset of $I\}$. $R^{\oplus I} = \bigoplus R_i$ we define $\alpha_S : R^{\oplus I} \to M$ by $\alpha((r_i)) = \sum r_i y_i$.

Claim: α_S is a R-module isomorphism, i.e. a free R-module is exactly a module isomorphism to a direct sum of copies of R. Let $T \subset M$ be a subset. Define $\alpha_T : R^{\oplus I} \to M$ by $\alpha_T((r_i)) = \sum r_i y_i$. $Im(\alpha_I) = \sum Ry_i$, so α_T is surjective iff T spans M over R. $\ker(\alpha_T) = \{(r_i) | \alpha_T((r_i)) = 0\} = \{(r_i) | \sum r_i y_i$. Hence, α_T is injective iff $\sum r_i y_i = 0$ then $r_i = 0$ iff T is lineraly independent in R.

Example 3.3.4. Let $I = \{1 \ldots, n\}, S = \{x_{r_1}, \ldots, x_{r_n}\}, \alpha_S : R^n \to M, \alpha_S(r_1, \ldots, r_n) = \sum r_i x_i$. By above, if S is a basis of M, α_S is an isomoprhism. R^n has basis $\{e_1, \ldots, e_n\}$. A basis of M determines an isomorphism from R^n to M by $\alpha_S(e_i) = x_i$.

Proposition 3.3.5. *Let M be a R-module, with submorudles $\{M_i\}$, define $\alpha : \bigoplus M_i \to M$ by $\alpha((x_i)) = \sum x_i$ and note α is a R-module homomorphism by universal property $\bigoplus M_i$, $\alpha_i : M_i \to M_j$ and α is R-module homomorphism induced from then*

1. *α is surjective iff $M = \sum M_i$*
2. *α is injective iff $\forall j \in I, M_j \cap \sum_{i \neq j} M_i = 0$*
3. *α is an isomorphism iff $M = \sum M_i$ and (2) is satisfied.*

3.3.1 Linear Algebra over Integral Domains

Assume R is a domain, let $F = frac(R).R^n \subset F^n$ since $R \subset F$

Example 3.3.6. $\mathbb{Z}^n \subset \mathbb{Q}^n$

Remark 3.3.7. If $V \subset \mathbb{R}^n$, let $FV = \{\sum_{k=1}^{\infty} \alpha_k u_k | \alpha_k \in F, u_k \in V\}$. Then FV is a F-vector space over F. Indeed, F is closed under addition and F scalar multiplication. We call FV the F-vector space generated by V, and it is the smallest F-vector space containing V.

Definition 3.3.8. $rk(V) = rk_R(V) = \dim_F(FV)$ since $FV \subset F^n, \dim_F(FV) \leq n$, so $rk(V) \leq n$.

Lemma 3.3.9.
1. *Let $S = \{s_i\}$ be in R^n. Then S is linearly independent over R in R^n iff S is linearlyh independent over F in F^n*
2. *Let $M_1, \ldots, M_k$ be R submodules of R^n, then $M_1 + \ldots + M_k$ is direct in R^n iff $FM_1 + \ldots + FM_K$ is direct in F^n*

Lemma 3.3.10. *Let $M \subset R$ be a R-submodule, let $S \subset M$. Then S is a maximal linearly independent set for R iff S is a maximal linear independent set over F in FM.*

Lemma 3.3.11.
1. *If $S = \{x_1, \ldots, x_n\}$ spans M in R^n, then S spans FM in F^n*
2. *$F(M_1 + \ldots + M_k) = FM_1 + \ldots + FM_k$*

Consequence: If $M \subset R^n$ is a submodule and M is free with basis S, then by lemmas, FM is free with basis S, $rk(M) = \dim_F(FM) = |S|$. In particular if T is another basis of M, then $|T| = |S|$.

3.4 Dec. 9, 2019

Definition 3.4.1. Let M be a free R-module, and let $\alpha : M \to R^n$ be a R-module isomorphism. If $N \subset M$ is a submodule, let $rk(N) = rk(\alpha(N)) = \dim_F F\alpha(N)$.

Proposition 3.4.2. *Let $\alpha : M \to R^n$ and $\beta : M \to R^S$ be R-module isomorphism. Then $rk(\alpha(N)) = rk(\beta(N))$ by definition $rk(N)$ is independent of choices.*

Proof. Let $\gamma = \beta \circ \alpha^{-1} : R^n \to R^S$ be R-module isormophism. Let $S \subset \alpha(N)$ to be maximal R linearly independent. Then $\gamma(S) \subset \beta(N)$ is maximally R-linearly independent. By lemma 3 from last time, S is maximally linear independent set in $F\alpha(N)$ and $\gamma(S)$ is a maximal F-linear independent set in $F\beta(N), \ldots, rk(\alpha(N)) = |S| = |\gamma(S)| = rk(\beta(N))$. □

Remark 3.4.3. Let $N_1, N_2 \subset M$ be submodule of a free finitely generated R-module M. Assume $N_1 + N_2$ is directed. Then

1. $rk(N_1 + N_2) = rk(N_1) + rk(N_2)$
2. if N_1 is free with basis $x_1, \ldots, x_k$ N_2 is free with basis $y_1, \ldots, y_l$, then $N_1 + N_2$ is free with basis $x_1, \ldots, x_k, y_1, \ldots, y_l$

3.4.1 Linear maps

Let M, N be R-modules. Recall $Hom_R(M, N)$.

Claim: $Hom_R(M, N)$ is a R-module. If $f, g \in Hom_R(M, N)$, define $f + g : M \to N$ by $(f + g)(x) = f(x) + g(x)$ for $x \in M$ if $r \in R$, set $(r \circ f)(x) = r(f(x))$ for $x \in M$, $f \in Hom_R(M, N)$. Once can check this makes $Hom_R(M, N)$ into a R-module. One step is $(r \circ f)(ax) = a(r \circ f)(x)$.

Example 3.4.4. Let M be a free R-module with basis $x_1, \ldots, x_n$. Then if $x \in M, r = \sum r_i x_i$ for $!r_1, \ldots, r_n$. Define for $j = 1, \ldots, n, q_j : M \to R$ by $q_j(\sum r_j x_i) = r_j$.

We call $Hom_R(M, R) = M^{\checkmark}$ the dual R-module to M. Conclude M free of rank n implies $M^{\checkmark}$ is a free module of rank n.

Theorem 3.4.5. *Let R be a PID. let M be a free R module of rank n. Let $M' \subset M$ be a submodule. Then*

1. *M' is free of rank $q \leq n$.*
2. *if $M' \neq \{0\}$, $\exists$ a basis $x_1, \ldots, x_n$ of M and nonzero $r_1, \ldots, r_q \in R$ such that $r_1 x_1, \ldots, r_q x_q$ is a basis of M and $r_1 \mid r_2 \mid \ldots \mid r_q \in R$.*

Remark 3.4.6. If R is not a PID, this is false. Ex: $R = F[x, y], M' = (x, y)$. Then M is free of rank 1, but M' is not free. since any subset S with > 1 element is not r linearly independent, and $M' = Rv$ as M is not a principal ideal.

3.5 Dec. 11, 2019

Corollary 3.5.1. *Let N be a finitely generated R-module, with R a PID. Then $\exists n, q \in \mathbb{Z}_{>0}$, with $n \geq q$, and $a_1, \ldots, a_q \in R$ such that $a_1 \mid a_2 \mid \ldots \mid a_q$ such that $N \cong R/(a_1) \oplus \ldots \oplus R/(a_j) \oplus R^{n-q}$.*

Corollary 3.5.2. *If G is a finite abelian group. Then $\exists n_1 \mid n_2 \mid \ldots \mid n_q$ in $\mathbb{Z}$ such that $G \cong \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_q}$*

Remark 3.5.3. Solution to problem to Problem set 1. Let G be a finite abelian group, let $m = lcm(|a|_{a \in G})$, then $\exists b \in G$ such that $|b| = m$.