MATH206: ABSTRACT ALGEBRA II

2. Cosets and Lagrange's theorem

Recall that a congruence relation modulo n on the set $\mathbb{Z}$ of integers can be defined by $a \equiv b \bmod n$ if and only if $a - b \in n\mathbb{Z}$, where $n\mathbb{Z}$ is the subgroup of $\mathbb{Z}$ consisting of all multiples of n we now generalized this notion and define congruence in any group modulo one of its subgroup we are interested in the equivalence classes which we called cosets.

Definition: Let $(G, \cdot)$ be a group with subgroup H for $a, b \in G$. we say that a is congruent to b modulo H, and write $a \equiv b \bmod H$ if and only if $ab^{-1} \in H$

Proposition 2.1 The relation $a \equiv b \bmod H$ is an equivalence relation on G. The equivalence class

Containing a can be written in the form
$Ha = \{ha / h \in H\}$ and it is called a right coset of
H in G. The element a is called a representative
of the coset Ha.

Proof:

(i) Reflexive (ie related to its self)
$a \equiv a \bmod H$, thus $a \equiv a \bmod H$ and this relation is reflexive

(ii) if $a \equiv b \bmod H$, then $ab^{-1} \in H$ thus $(ab^{-1})^{-1} = ba^{-1}$. Hence
$b \equiv a \bmod H$, and the relation is symmetric

(iii) if $a \equiv b \bmod H$ and $b \equiv c \bmod H$, then $ab^{-1} \in H$ and $bc^{-1} \in H$
Hence $(ab^{-1})(bc^{-1}) = ac^{-1}$ and $a \equiv c \bmod H$ the relation
is transitive and therefore are equivalence relation.
This equivalence class containing a is

$\{x \in G / x \equiv a \bmod H\}$
$= \{x \in G / xa^{-1} \in H\}$
$= \{x \in G / xa^{-1} = h \text{ for some } h \in H\}$
$= \{x \in G / x = ha, h \in H\}$
$= \{ha / h \in H\} = Ha$

Exercise find the right cosets of
$H = \{(1), (1\,2\,3), (1\,3\,2)\}$ in S_3
$S_3 = \{(1), (1\,2), (1\,3), (1\,2\,3), (1\,3\,2), (2\,3)\}$
$H = \{(1), (1\,2\,3), (1\,3\,2)\}$
$H(1) = \{(1)(1), (1\,2\,3)(1), (1\,3\,2)(1)\}$
$H(2) = \{(1)(2), (1\,2\,3)(2), (1\,3\,2)(2)\}$

there are only two cosets

$H = \{(1), (123), (132)\}$

$H(12) = \{(12)\ (13)\ (23)\}$

Note that

$H(1) = H(123) = H(132)$

$H(12) = H(13) = H(23)$

U18ES2054

H

find the right cosets of $H = \{e, g^4, g^8\}$ in $C_{12} = \{e, g, g^2 \cdots g^{11}\}$

Solution

$H = \{e, g^4, g^8\}$

$Hg = \{g, g^5, g^9\}$

$Hg^2 = \{g^2, g^6, g^{10}\}$

$Hg^3 = \{g^3, g^7, g^{11}\}$

since $C_{12} = H \cup Hg \cup Hg^2 \cup Hg^3$ these are the only right cosets

Lemma 2.2 ; There is a bijection between any two right cosets of H in G. i.e any two right cosets contain the same number of elements.

Proof

Let Ha be a right coset of G we produce a bijection mapping between Ha and H from which it follow that there is a bijections between any two right cosets.

Define $\phi : H \longrightarrow Ha$ by $\phi(h) = ha$ then ϕ is clearly onto, Now suppose $\phi(h_1) = \phi(h_2)$ so that $h_1 a = h_2 a$

multiplying each since by a^{-1} on the right
$h_1 = h_2$ Hence ϕ is a bijection.

Theorem 2.3 (Lagrange's theorem)
If G is finite group and H is a subgroup of G then the order of $|H|$ divide the order of $|G|$

Proof

The right cosets of H in G form a partition of G so G can be written as a disjoint union $G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k$ for a finite set of element $a_1, a_2 \dots a_k \in G$
By Lemma 2.2 the number of element in each coset is $|H|$
Hence adding of all the elements in the above disjoint union, we see that $|G| = k|H|$ therefore $|H|$ divides $|G|$.

Defn: If H is a subgroup of G, the number of distinct right cosets of H in G is called the index of H in G and is written $[G:H]$

Corollary 2.4: If G is a finite group with subgroup H then $[G:H] = \frac{|G|}{|H|}$

Corollary 2.5: if a is an element of a finite group then the order of a ~~finite distinct~~ divides the order of G.

Proof

Let $\langle a \rangle = \{a^r / r \in \mathbb{Z}\}$ be the cyclic subgroup ~~gen~~ generated by a. Then the order of the subgroup $\langle a \rangle$ is the same as the order of the element a. Hence by

Lagrange's theorem the order of a divides the order of G.

Carrolary 2.6: Let the order of a Group G be n if a is an element of G then

$$a^n = e$$

Proof: if m is the order of a. then $n = mk$ for some k Hence $a^n = a^{mk} = (a^m)^k = e^k = e$

Carrolary 2.7: if G is a group of prime order, then G is cyclic.

proof: Let $|G| = p$ a prime number By Carrolary 2.5 every elemeat has order 1 or p. But the only element of order 1 is the identity. Therefore all the other elements have order p and there is atleast one, because $|G| \geq 2$ thus every non-identity element in G generates G. Hence G is cyclic. □

Remarks: the converse of lagrange's theorem is false as the following example shows. That is k is a divisor of the order of G, it does not necessarily follow that G has a subgroup of order k.

Example: A_4 is a group of order 12 having no subgroup of order 6

Solution

A_4 contains one identity elements, eight 3-cycles of the form (a b c) and three pairs of transposition

of the form $(ab)(cd)$, where a, b, c and d are
elements of $\{1, 2, 3, 4\}$

If a subgroup contains a 3-cycles (abc), it must also contain its inverses (acb) if a subgroup of order 6 exists, it must contain the identity and a product of two transpositions, because the odd number of non-identity elements cannot be made up of 3-cycles and their inverse. A subgroup of order 6 must also contain atleast two 3-cycles, because A_4 only contains four elements that are not 3-cycles.

Without loss of generality, suppose that a subgroup of order 6 contains the elements (abc) and $(ab)(cd)$ then it must contain the element $(abc)^{-1} = (acb)$, $(abc)[(ab)(cd)] = (bdc)$, $[(ab)(cd)](abc) = (acd)$, $(acd)^{-1} = (adc)$ which together with identity, gives more than six elements. Hence A_4 contains no subgroup of order 6.

We can also define the relation L on G so that $a \perp b$ if and only if $b^{-1}a \in H$. This relation is an equivalence relation, and the equivalence class containing a is the left coset

$$aH = \{ah \mid h \in H\}$$

Example: find the left and right cosets of $H = A_3$ and $K = \{(1)\ (12)\}$ in S_3

Solution

$H = A_3 = \{(1)(123)(132)\}$

$K = \{(1)(12)\}$

Right cosets

$H = \{(1), (123), (132)\}$

$H(12) = \{(1)(12), (123)(12), (132)(12)\}$

$= \{(12), (23), (13)\}$

Left cosets

$H = \{(1), (123), (132)\}$

$(12)H = \{(12)(1), (12)(123), (12)(132)\}$

$= \{(12), (13), (23)\}$ In this case ~~$L = R$~~

Right cosets

$K = \{(1)(12)\}$

$K(13) = \{(1)(13), (12)(13)\}$

$= \{(13), (123)\}$

$K(23) = \{(1)(23), (12)(23)\}$

$= \{(23), (132)\}$

Left Cosets

$K = \{(1), (12)\}$

$(13)K = \{(13)(1), (13)(12)\}$

$= \{(13), (132)\}$

$(23)K = \{(23)(1), (23)(12)\}$

$= \{(23), (123)\}$ $\therefore L \neq R$

~~2. Normal~~ In this case the L and R Cosets of K are not the same

3. Normal subgroups and Quotient Groups.

5. Normal Subgroups and Quotient Groups

Def: A subgroup H of a group G is called a normal subgroup of G if $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$

$H \trianglelefteq G$

Proposition 3.1: $Hg = gH$ for all $g \in G$, if and only if H is a normal subgroup of G

Proof:

Suppose $Hg = gH$ Then, for any element $h \in H$, $hg \in Hg = gH$

Hence $hg = gh$, for some $h \in H$ and $g^{-1}hg = g^{-1}gh = h \in H$

Therefore, H is normal subgroup.

Conversely, if H is normal in G let $hg \in Hg$ and $g^{-1}hg \in H$

i.e $g^{-1}hg = h_1$ for some $h_1 \in H$. Thus $g(g^{-1}hg) = gh_1$

i.e $hg = gh_1 \in gH$

Hence $Hg \subseteq gH$

Also $ghg^{-1} = (g^{-1})^{-1}hg^{-1} = h_2 \in H$

Hence $ghg^{-1} = h_2 \Rightarrow gh = h_2 g \in Hg$

Hence $gH \subseteq Hg$ and $Hg = gH$ ∎

Example: from our last example, A_3 is normal in S_3 whereas $K = \{(1), (12)\}$ is not normal in S_3

Proposition 3.2: Any subgroup of an abelian group is normal.

Proof

$\forall g \in G$, $h \in H$	$\forall g \in G$, $h \in H$
$g^{-1}hg \in H$	$g^{-1}hg = hg^{-1}g = h \in H$

Proof:

If H is a subgroup of an abelian group, G then $g^{-1}hg = hg^{-1}g = h \in H$ for all $g \in G$, $h \in H$. Hence H is normal. □

Theorem 3.3: If N is a normal subgroup of (G,·) the set of cosets $G/N = \{Ng \mid g \in G\}$ form a group, where the operation is defined by $(Ng_1)(Ng_2) = Ng_1g_2$. This group is called the quotient group or factor group of G by N

Proof:

The operation of multiplying two cosets, Ng_1 and Ng_2 is defined in terms of particular elements g_1 and g_2, of the cosets. for this operation to make sense, we have to verify that, if we choose different elements h_1 and h_2 in the same cosets, the product cosets Nh_1h_2 is the same as Ng_1g_2.

In other words we have to show that multiplication of cosets is well defined.

Since h_2 is in the same coset as g_1, we have $h_1 \equiv g_1 \bmod N$. similarly $h_2 \equiv g_2 \bmod N$. we now show that $Nh_1h_2 = Ng_1g_2$ we have $h_1g_1^{-1} = n_1 \in N$ and $h_2g_2^{-1} = n_2 \in N$ and so $(h_1h_2)(g_1g_2)^{-1} = h_1h_2g_2^{-1}g_1^{-1} = (n_1g_1\, n_2g_2)g_2^{-1}g_1^{-1}$

$= n_1(g_1 n_2 g_1^{-1})$.

Now N is a normal subgroup, so $g_1n_2g_1^{-1} \in N$ and $n_1g_1g_1^{-1} \in N$

Hence $h_1h_2 = g_1g_2 \bmod N$ and $Nh_1h_2 = Ng_1g_2$. Therefore the operation is well defined

The operation is associative because

$$(Ng_1 \cdot Ng_2)Ng_3 = Ng_1g_2\,Ng_3$$
$$= N(g_1g_2)g_3$$
$$= Ng_1(g_2g_3)$$
$$= Ng_1\,Ng_2g_3$$
$$= Ng_1(Ng_2Ng_3).$$

Since $NgNe = Nge = Ng$ and

$Nea Ng = Ng$ the identity is $Ne = N$

The inverse of Ng is Ng^{-1} because

$Ng\,Ng^{-1} = Ngg^{-1} = Ne = N$ and also $Ng^{-1}Ng = N$.

Hence $(G/N, \cdot)$ is a group.

Note: The order of G/N is the number of cosets of N in G $|G/N| = [G : N] = \frac{|G|}{|N|}$

Examples 18/7/2018

1. Since A_3 is a normal subgroup of S_3 therefore S_3/A_3 is quotient group if we let $H = A_3$, there the elements of this group are the cosets H and $H(12)$

$$S_3/H = \{H, H(12)\}$$

2. $(Z_n, +)$ is the quotient group of $(Z, +)$ by the subgroup $nZ = \{nz \mid z \in Z\}$

Solution

since $(\mathbb{Z}, +)$ is abelian, every subgroup is norma
al. The set $n\mathbb{Z}$ can be verified to be a subgroup
and the relation $a \equiv b \bmod n\mathbb{Z}$ is equivalent to
$a - b \in n\mathbb{Z}$ and to $n/(a-b)$. Hence $a \equiv b \bmod n\mathbb{Z}$ is
the same relation as $a \equiv b \bmod n$. Therefore, $\mathbb{Z}_n$ is the
quotient group $\mathbb{Z}/n\mathbb{Z}$

Proposition 3.4: If H is a subgroup of index 2
in G, so that $[G:H] = 2$, then H is a normal
subgroup of G, and G/H is a cyclic group of
order 2.

$[G:H] = 2 \Rightarrow H, Hg \Rightarrow g^{-1}hg \in H \quad \forall g \in G, h \in H$

1. $g \in H \Rightarrow g^{-1}hg \in H \quad \because g, h \in H$
2. $g \notin H \Rightarrow g \in Hg$

$g^{-1}hg \notin H \Rightarrow g^{-1}hg \in Hg$

$\Rightarrow g^{-1}hg = h_1 g$

$\Rightarrow g^{-1}h = h_1$

$\Rightarrow g^{-1} = h_1 h^{-1} \Rightarrow g = h h_1^{-1} \Rightarrow g \in H.$

Proof

since $[G:H] = 2$, there are only two right cosets
of H in G one must be H and the other can
be written as Hg, where g is any element
of G that is not in H. To show that H is
a normal subgroup of G, we need to show that

$g^{-1}hg \in H$ for all $g \in H$ and $h \in H$.

Case 1 If g is an element of H it is clear that $g^{-1}hg \in H$ for all $h \in H$.

Case 2 If g is not an element of H, suppose that $g^{-1}hg \notin H$. In this case $g^{-1}hg$ must be an element of the other coset Hg, and we can write $g^{-1}hg = h_i g$, for some $h_i \in H$. It follows that $g = hh_i^{-1} \in H$ which contradicts the fact that $g \notin H$. Hence $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$ in other words, H is normal in G.

24/7/2018

Theorem 3.5: If G is a finite abelian group and the prime p divides the order of G, then G contains an element of order p and hence a subgroup of order p.

Proof:

We prove this result by induction on the order of G for a particular prime p. Suppose that all abelian groups of order less than k, where order is divisible by p, contains an element of order p. The result is clearly true for groups of order 1.

Now suppose G is a group of order k, if p divides k, choose any non-identity element $g \in G$. Let t be the order of the element g.

Case 1: If p divides t, say $t = pr$, then g^r is an element of order p. This follows because g^r is not the identity, but $(g^r)^p = g^t = e$ and p is a prime.

Case 2: on the other hand, if p does not divide t let K be the subgroup generated by g. Since G is abelian, K is normal, and the quotient group G/K has order $\frac{|G|}{t}$ which is divisible by p.

Therefore by the induction hypothesis G/K has an element of order p, say Kh. If u is the order of h in G, then $h^u = e$ and $(Kh)^u = Kh^u = K$ since Kh has order p in G/K, u is a multiple of p, and we are back to Case 1. The result follows from induction hypothesis.

Note: that theorem 3.5 is partial converse of lagrange's Theorem. It is a special case of the Sylor theorems.

Example: show that A_5 has no proper normal subgroup.

Solution

A_5 contains three types of non-identity elements, namely 5-cycles, 3-cycles and pairs of disjoint transposition, Suppose N is a normal subgroup of A_5 that contains more than one element.

Case 1: Suppose N contains the 3-cycles (abc) from the definition of normal subgroups $g^{-1}(abc)g \in N$. for all $g \in A_5$. if we take $g = (ab)(cd)$, we obtain

$$(ab)(cd)(abc)(ab)(cd)$$
$$= (adb) \in N$$

and also $(adb)^{-1} = (abd) \in N$. In a similar way we can show that N contains every 3-cycle. since every alternating group is generated by the set of three cycles, N must be the whole alternating group.

Case 2: Suppose N contains the 5-cycles $(abcde)$ Then

$$(abc)^{-1}(abcde)(abc)$$
$$= (acb)(abcde)(abc)$$
$$= (adebc) \in N$$

and $(abcde)(adebc)^{-1}$

$$= (abcde)(acbed)$$
$$= (aec)$$

we are back to case 1 and hence $N = A_5$

Case 3: suppose N contains the pair of disjoint trans. position $(ab)(cd)$. Then e is the element of $\{1, 2, 3, 4, 5\}$ not appearing in these transpositions we have $(abe)^{-1}(ab)(cd)(abe)$

$$= (aeb)(ab)(cd)(abe)$$
$$= (be)(cd) \in N$$

Also $(ab)(cd)(be)(cd) = (aeb) \in N$

and again we are back to ✱ case 1
Thus any normal subgroup of A_5 containing more than one element must be A_5 itself.

Def: A group without any proper normal subgroup is called a simple group.

Example: A_5 - above

Remarks:

1. Apart from the cyclic groups of prime order, which have no proper subgroups of any kind, simple groups are comparatively rare.
2. A_5 is of great interest to mathematicians because it is used in Galois theory to show that there is an equation of fifth degree that can not be solved by any algebraic formula.

4: Centraliser and Centre of a group

Def: Let a be a fixed element of G. Then the centraliser of a in G is the set

$$C_G(a) = \{x \in G \mid xa = ax\}$$

and the centre of the group G is the set

$$Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$$

Theorem 4.1 Let G be a group and $a \in G$. Then $C_G(a)$ is a subgroup of G, while $Z(G)$ is a normal subgroup of G.

proof: $C_G(a)$

It is clear that $a \in C_G(a)$. Thus $C_G(a) \neq \phi$. Let $x, y \in C_G(a)$, then $xa = ax$ and $ya = ay$. Note that

$ya = ay \Rightarrow yay^{-1} = a \Rightarrow ay^{-1} = y^{-1}a$

Therefore

$$\begin{aligned}(xy^{-1})a &= x(y^{-1}a) \\ &= x(ay^{-1}) \\ &= (xa)y^{-1} \\ &= (ax)y^{-1} \\ &= a(xy^{-1})\end{aligned}$$

Hence, $C_G(a)$ is a subgroup of G.

Now, for all $g \in G$, $eg = ge$, thus $e \in Z(G)$ i.e $Z(G) \neq \phi$

let $x, y \in Z(G)$, then $xg = gx$ and $yg = gy$ for all $g \in G$

and $$\begin{aligned}(xy^{-1})g &= x(y^{-1}g) \\ &= x(gy^{-1}) \\ &= (xg)y^{-1} \\ &= (gx)y^{-1} \\ &= g(xy^{-1})\end{aligned}$$

Thus $Z(G)$ is a subgroup of G.

Next, suppose $x \in Z(G)$ and $g \in G$ then

$g^{-1}xg = g^{-1}gx = ex = x \in Z(G)$

Hence $Z(G) \trianglelefteq G$.

Note: That the centre may be a proper or an improper

$H \subseteq G$ (i) $H \neq \emptyset$
(ii) $x, y \in H, xy^{-1} \in H$.

subgroup or a trivial subgroup. for Instance, if G is abelian, then $G = Z(G)$. Conversely if $G = Z(G)$, then every element $a \in G$, is in the centre $Z(G)$ i.e $ab = ba$. for every $b \in G$ Thus G is abelian for some groups the centre may be the trivial group $\{e\}$. for example if $G = S_3$ then $Z(G) = \{e\}$

Def: for every subset $A \subseteq G$ $N(A) = \{x \in G / xA = Ax\}$ is called the normaliser of A in G.

Proposition 4.2: for any subset A of G, $N(A)$ is a subgroup of G.

Proof:

for any $a \in A$, $aA = Aa$. Thus $N(A) \neq \emptyset$

Let $x, y \in N(A)$. Then $xA = Ax$ and $yA = Ay$.

Note also that $yA = Ay$

$\Rightarrow y^{-1}(yA)y^{-1} = y^{-1}(Ay)y^{-1}$

$\Rightarrow Ay^{-1} = y^{-1}A$ and

and $(xy^{-1})A = x(y^{-1}A)$

$= x(Ay^{-1})$

$= (xA)y^{-1}$

$= (Ax)y^{-1}$

$= A(xy^{-1})$

Hence $N(A)$ is a subgroup of G.

Note that when A is the singleton set $\{a\}$, the Normalizer of A ie $N(a)$ is the same as

the Centralizer of a, $C_G(a)$

$N(A) = \{x \in G \mid xA = Ax\}$

$N(a) = \{x \in G \mid xa = ax\}$

$= C_G(a)$ 25/7/2018

Theorem 4.3: Let $H \leq G$. Then $H \trianglelefteq N(H) \leq G$, and whenever $H \trianglelefteq J \leq G$, $J \leq N(H)$. where $N(H)$. where $N(H)$ is the normalizer of H in G

Proof

Certainly $H \subseteq N(H)$. since for all $h \in H$, $hH = Hh = H$, so $N(H) \neq \emptyset$. Let $x, y \in N(H)$, since $y^{-1}Hy = H$ it follows that $H = yHy^{-1}$, and so

$$(xy^{-1})^{-1}Hxy^{-1} = y(x^{-1}Hx)y^{-1}$$
$$= yHy^{-1}$$
$$= H$$

Hence $xy^{-1} \in N(H)$. Therefore $N(H) \leq G$ and $H \leq N(H)$. It is also clear from the definition of $N(H)$ that $H \trianglelefteq N(H)$

finally, if $H \trianglelefteq J \leq G$ and $x \in J$ then $x \in G$ and $x^{-1}Hx = H$ Hence by the definition of $N(H)$, $x \in N(H)$ Thus $J \leq N(H)$.

Corollary 4.4: Let $H \leq G$. Then $H \trianglelefteq G$ if and only if $N(H) = G$

Exercise

(1) Show that for any element a of a group G, $Z(G) \leq C_G(a)$.

2. what can you say about $N(a)$ and $N(H)$ for any $a \in H$, where H is a subgroup of G.

3. Can you relate $Z(G)$ and $N(H)$ for any subgroup H of a group G.

~~5 Conjugate~~

5. Conjugate classes and the class equation

Conjugate relation

Def: Let G be a group, $a \in G$ and $b \in G$. Then b is said to be conjugate to a, if $b = xax^{-1}$ for some $x \in G$

Proposition 5.1: Let G be a group, and $\sim$ the relation in G given by $b \sim a$ if and only if b is conjugate to a, Then $\sim$ is an equivalence relation in G

Proof:

(i) since $a = eae^{-1}$, a is conjugate to a. (reflexive)

(ii) if a is conjugate to b, then $a = xbx^{-1}$ for some $x \in G$. Then $b = x^{-1}ax$, i.e b is conjugate to a (Symmetric)

(iii) Let a be conjugate to b, and b conjugate to c. Then $a = xbx^{-1}$ and $b = ycy^{-1}$ for some $x, y \in G$.

Then $a = x(ycy^{-1})x^{-1}$

$= xycy^{-1}x^{-1}$

$= xyc(xy)^{-1}$

Thus a is conjugate to c Hence $\sim$ is an equivalence relation (transitive)

C(a) = conjugate class of a

Def: The equivalence classes under the relation $b \sim a$ if and only if $b = xax^{-1}$, $x \in G$ are called conjugate classes.

Proposition 5.2: Let G be a group Then any two distinct conjugate classes have no element in common and G is the union (disjoint) of all its conjugate classes.

Proof: 8/8/2018

This follows immediately from the property of equivalence classes. We will denote by $C(a)$, the conjugate class containing a. □

Proposition 5.3: Let G be a group and $a \in G$ Then $C(a) = \{a\}$ if and only if $a \in Z(G)$

Proof:

Suppose $C(a) = \{a\}$. Then, for any $b \in G$, $bab^{-1} \in C(a)$ $C(a) = \{a\}$ and so, $bab^{-1} = a$ or $ba = ab$. Thus $a \in Z(G)$

Conversely, let $a \in Z(G)$ and $b \in C(a)$. Then $b = xax^{-1}$ for some $x \in G$ since $a \in Z(G)$, $b = axx^{-1} = a$,

Thus, $C(a) = \{a\}$ □

Definition: $C(a)$ is called a trivial conjugate class if it contains just one element a.

Proposition 5.4 Let G be a finite group and $a \in G$ Then the number of elements in the conjugate class $C(a)$ is equal to the index of the normalizer $N(G)$ of a in G that is $|C(a)| = [G : N(a)] = \frac{o(G)}{o[N(a)]}$

Cardinality of $C(a)$

C(a) → i

$b = xax^{-1}$
b = conjugate of a

proof:

To show that $|C(a)| = [G : N(a)]$. We shall show that there is a bijective mapping from $C(a)$ into $G/N(a)$

Let $b \in C(a)$, then $b = xax^{-1}$ for some $x \in G$. This may not be unique that is be may also be equal to yay^{-1} for some $y \in G$. In such a case

$$b = xax^{-1} = yay^{-1}$$

which implies that $x^{-1}ya = ax^{-1}y$.

showing that $x^{-1}y \in N(a)$. And so $xN(a) = yN(a)$

Now, define a mapping $\theta : C(a) \longrightarrow G/N(a)$ by

$\theta b = xN(a)$ for all $b \in C(a)$ where $b = xax^{-1}$. We have just show that θ is well-defined. θ is also one-one, because if $xN(a) = yN(a)$, then $x^{-1}y \in N(a)$ and so, $x^{-1}ya = ax^{-1}y$ or $xax^{-1} = yay^{-1}$

Clearly, θ is onto, Thus, $C(a)$ and $G/N(a)$ have the same number of elements. □

4/8/2018

Theorem 5.5 (The class equation) (G:H)

Let G be a finite group. Then

$$|G| = |Z(G)| + \sum [G : N(a)] \quad [G : N(a)] > 1$$

where the summation runs over the set of representatives of distinct non-trivial conjugate classes. The above equation is called the class equation.

proof

C(a) - Ji

b = xax⁻¹
b = conjugate of a

proof:

To show that $|C(a)| = [G : N(a)]$. We shall show that there is a bijective mapping from $C(a)$ into $G/N(a)$

Let $b \in C(a)$, then $b = xax^{-1}$ for some $x \in G$. This may not be unique that is be may also be equal to yay^{-1} for some $y \in G$. In such a case

$$b = xax^{-1} = yay^{-1}$$

which implies that $x^{-1}ya = ax^{-1}y$.

showing that $x^{-1}y \in N(a)$. And so $xN(a) = yN(a)$

Now, define a mapping $\theta : C(a) \longrightarrow G/N(a)$ by $\theta b = xN(a)$ for all $b \in C(a)$ where $b = xax^{-1}$. We have just show that θ is well-defined. θ is also one-one, because if $xN(a) = yN(a)$, then $x^{-1}y \in N(a)$ and so, $x^{-1}ya = ax^{-1}y$ or $xax^{-1} = yay^{-1}$

Clearly, θ is onto, Thus, $C(a)$ and $G/N(a)$ have the same number of elements. □

4/8/2018

Theorem 5.5 (The class equation) (G:41)

Let G be a finite group. Then

$$|G| = |Z(G)| + \sum [G : N(a)] \quad [G : N(a)] > 1.$$

where the summation runs over the set of representatives of distinct non-trivial conjugate classes. The above equation is called the class equation.

proof

$G = C(a_1) \cup C(a_2) \cup \dots \cup C(a_k)$

G is a disjoint union of its distinct conjugate classes. By Proposition 5.3, there $|Z(G)|$ trivial conjugate classes and by propositions 5.4, each non-trivial conjugate class has $[G : N(a)]$ elements. Thus counting all the elements in all the conjugate classes we have $|G| = |Z(G)| + \sum_{[G:N(a)]>1} [G : N(a)]$

□

Proposition 5.6: Any group of order p^n where p is prime, has non-trivial centre.

Proof

Let G be a group of order p^n consider the class equation $|G| = |Z(G)| + \sum_{[G:N(a)]>1} [G : N(a)]$

since for each term of the summation, $[G : N(a)] > 1$ p divides each term of the summation. Hence p divides $\sum_{[G:N(a)]>1} [G : N(a)]$

Also, since p divides $|G| = p^n$, p divides $|G| - \sum_{[G:N(a)]>1} [G : N(a)] = |Z(G)|$

Hence $|Z(G)| \geq 1$ so that $Z(G) \neq \{e\}$

□

non-trivial $Z(G) \neq \{e\}$

Corollary 5.7: Any group of order p^2 is abelian, where p is a prime

Proof

By proposition 5.6, $Z(G) \neq \{e\}$. Hence $|Z(G)| = p$ or p^2. Suppose $|Z(G)| = p$. Then $Z(G)$ is a cyclic group of order p. Choose $a \in G$ such that $a \notin Z(G)$. Then $N(a)$ is a subgroup of G containing $Z(G)$ properly because $a \in N(a)$ and $a \notin Z(G)$. Hence $N(a) = G$. This implies $a \in Z(G)$ contrary to the choice of a. Thus $|Z(G)| = p$ is impossible. Hence $|Z(G)| = p^2$, that is $Z(G) = G$ showing that G is abelian. □

Recall Theorem 3.5 that if G is a finite abelian group and the prime p divides the order of G then contains an element of order p and hence a subgroup of order p. We now give a generalisation of this result.

Theorem 5.8 (Cauchy's Theorem)

Let G be a finite group of order n, and p be a prime dividing n. Then G has an element of order p and hence a subgroup of order p.

Proof:

We have already proved the theorem when G is abelian (see proof of theorem 3.5)

We shall now consider the case when G is not necessarily abelian.

The proof is again by induction on $n = |G|$. Assume that the theorem is true for all groups of order less than $|G| = n$, and assume further that for all proper subgroups H of G, p does not divide $|H|$. Consider the class equation

$$|G| = |Z(G)| + \sum_{[G:N(a)]>1} [G:N(a)]$$

since $|G| = |N(a)|[G:N(a)]$ and since $N(a)$ is a proper of G for all $a \notin Z(G)$ p does not divide $|N(a)|$ for all $a \notin Z(G)$. Hence, p provides $[G:N(a)]$ whenever $[G:N(a)] > 1$. Hence, p provides the summation $\sum_{[G:N(a)]>1} [G:N(a)]$

Since p divides $|G|$ it follows that p divides $|Z(G)|$. Now, $Z(G)$ is an abelian group, and since p divides $|Z(G)|$ by Theorem 3.5 (or first part of this theorem) $Z(G)$ contains an element of order p. Hence G contains and element of order p.

□

Exercise

1. find the conjugate classes of S_3 and verify the class equation.

2. find also the conjugate classes of S_4 and verify the class equation.

3. If G is a finite group with just 2 conjugate classes show that $|G| = 2$.

4. show that any subgroup H of order p^{n-1} in a group of order p^n is normal.

5. Let $\delta = (1\ 2\ 3\ \cdots\ n) \in S_n$. find the number of elements in the conjugate class of δ

6. Homomorphism of groups

Def: Let G and G' be any two groups A mapping $\theta: G \to G'$ is called a group homomoplism if it satisfies the condition

$$\theta(ab) = \theta(a)\,\theta(b) \quad \text{for all } a, b \in G$$

Examples

1. Let $G = \mathbb{Z}$, the group of integers under addition, and let $G' = \{1, -1\}$, the multiplicative group of 1 and -1. The mapping $\theta: G \to G'$ defined by

$$\theta(n) = \begin{cases} 1 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd} \end{cases}$$

is a group homomoplism, since

$$\theta(\overset{\text{odd}}{m} + \overset{\text{odd}}{n}) = 1 = (-1)(-1) = \theta(m)\,\theta(n)$$

$$\theta(\overset{\text{odd}}{m} + \overset{\text{even}}{n}) = -1 = -1 \times 1 = \theta(m)\,\theta(n)$$

$$\theta(\overset{\text{even}}{m} + \overset{\text{even}}{n}) = 1 = 1 \times 1 = \theta(m)\,\theta(n)$$

for all $m, n \in \mathbb{Z} = G$

$\theta(m+n) = \theta(m)\,\theta(n)$

2. Let $G = \mathbb{R}$ be the group of real number under addition and $G' = \mathbb{R}^+$ be the group of positive real numbers under multiplication. The mapping

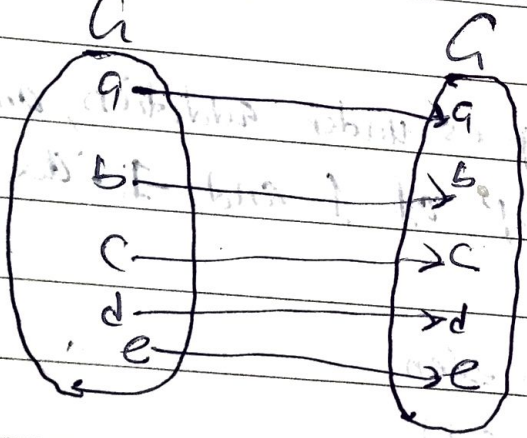
$$\theta : G \longrightarrow G'$$

given by $\theta(x) = 2^x$, is a group homomorphism, since for all $x, y \in \mathbb{R}$

$$\theta(x+y) = 2^{x+y} = 2^x \cdot 2^y = \theta(x)\,\theta(y)$$

3. for any two groups G and G', the mapping $\theta : G \to G'$ give by $\theta(a) = e'$ (the identity in G') is a group homomorphism, called the trivial homomophism

4. for any group G the identity mapping $I_G : G \to G$ is a group homomophism called the identity homomophism



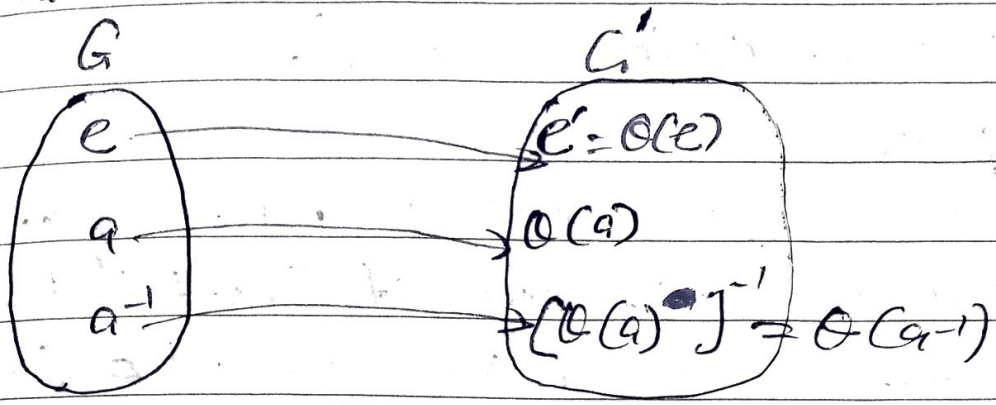
$$\theta(ab) = ab$$
$$= \theta(a)\,\theta(b)$$

5. Let $G = \mathbb{Z}$ and $G' = \mathbb{Z}_n$. The mapping $\theta : G \to G'$ defined by $\theta(a) = \bar{a}$ is a group homomophism.

Def: A group homomophims $\theta : G \to G'$ which is one-to-one is called a monomophism. θ is called an epimorphism if it is onto G', and a bijective

homomorphism is called isomorphism

proposition 6.1 Let $\theta: G \longrightarrow G'$ be a group homomorphism then (i) $\theta(e) = e'$ and (ii) $\theta(a^{-1}) = [\theta(a)]^{-1}$ for all $a \in G$



Proof:

(i) $\theta(e) = \theta(e \cdot e)$

$\theta(e) = \theta(e)\theta(e)$

multiply, on the left, both sides by $[\theta(e)]^{-1}$

$[\theta(e)]^{-1}\theta(e) = [\theta(e)]^{-1}\theta(e)\theta(e)$

$e' = e'\theta(e) = \theta(e)$

(ii) $\theta(e) = \theta(a \cdot a^{-1}) = \theta(a)\theta(a^{-1})$ that is

$\theta(e) = \theta(a)\theta(a^{-1})$ so multiplying both sides by $[\theta(a)]^{-1}$ we have $[\theta(a)]^{-1}\theta(e) = [\theta(a)]^{-1}\theta(a)\theta(a^{-1})$

that is $[\theta(a)]^{-1} = \theta(a^{-1})$ □

proposition 6.2 Let $\theta: G \longrightarrow G'$ be an epimorphism Then if G is abelian so is G'.

Proof:

Let $a', b' \in G'$ since θ is onto, there exist $a, b \in G$ such that $\theta(a) = a'$ and $\theta(b) = b'$. Now

$a'b' = \theta(a)\theta(b) = \theta(ab) = \theta(ba) = \theta(b)\theta(a)$

$= b'a'$

And so G' is abelian.

Proposition 6.3 Let $\theta: G \to G'$ be a homomophism of G onto G'. If G is cyclic, so is G'.

Proof

Let $G = \langle a \rangle$ be a cyclic group generated by a. the show that $\theta(a) = a'$ is a generator of G'. Let b' be any element in G'. since θ is onto there exists $b \in G$ such that $b' = \theta(b)$. Now $b = a^r$ for some $r \geq 1$ so that

$b' = \theta(b) = \theta(a^r)$

$= \theta(a)^r$

Thus, $G' = \langle \theta(a) \rangle$, that is G' is cyclic.

28/8/2018 □

Theorem 6.4 let θ be a group homomorphism of G into G'. If H is a subgroup of G then $\theta(H)$ is a subgroup of G', and if H is normal in G, then $\theta(H)$ is normal in $\theta(G)$. Going the other way, if K is a subgroup of G' then $\theta^{-1}(K)$ is a subgroup of G, and if K' is normal in $\theta(G)$, then $\theta^{-1}(K')$ is normal in G. [ie under a homomorphism, subgroups correspond to subgroups and normal subgroups correspond to normal subgroups]

Proof

Let H be a subgroup of G, and let $\theta(a)$ and $\theta(b)$

be any two elements in $\theta(H)$. Then $a, b \in H$, and

$$\theta(a)\theta(b)^{-1} = \theta(a)\theta(b^{-1}) = \theta(ab^{-1}),$$

But since $H \leq G$ and $a, b \in H$, we have $ab^{-1} \in H$, so that $\theta(a)\theta(b^{-1}) = \theta(ab^{-1})$ is in $\theta(H)$. Thus $\theta(H)$ is a subgroup of G'.

Now, suppose H is normal in G, and let $\theta(g) \in \theta(G)$ and $\theta(h) \in \theta(H)$. Then $\theta(g)\theta(h)\theta(g)^{-1} = \theta(g)\theta(h)\theta(g^{-1})$

$$= \theta(ghg^{-1})$$

Since H is normal in G, $ghg^{-1} \in H$ and so $\theta(g)\theta(h)\theta(g)^{-1} = \theta(ghg^{-1}) \in \theta(H)$.

Thus $\theta(H)$ is normal in $\theta(G)$

Going the other way, let K' be a subgroup of G'. Suppose $a, b \in \theta^{-1}(K')$. Then $\theta(a), \theta(b) \in K'$ so that $\theta(a)\theta(b)^{-1} \in K'$ or $\theta(ab^{-1}) \in K'$. Thus $ab^{-1} \in \theta^{-1}(K')$ and $\theta^{-1}(K')$ is a subgroup of G.

If K' is a normal subgroup of $\theta(G)$, then for $b \in \theta^{-1}(K')$ and $g \in G$, we have $\theta(gbg^{-1}) = \theta(g)\theta(b)\theta(g^{-1})$

$$= \theta(g)\theta(b)\theta(g)^{-1} \in K'$$

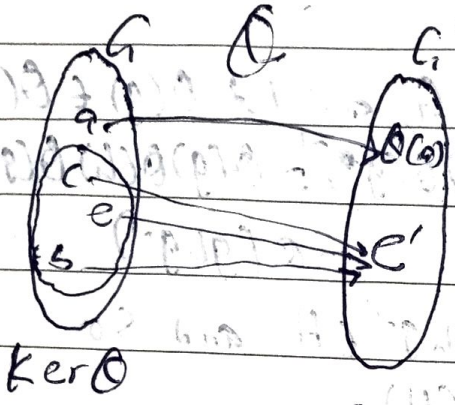
since $K' \trianglelefteq \theta(G)$. Therefore, $gbg^{-1} \in \theta^{-1}(K')$ so that $\theta^{-1}(K')$ is normal in G. □

Corollary 6.5 Let θ be a homomorphism from G into G'. Then $\text{im}\,\theta\,[= \theta(G)]$ is a subgroup of G'.

□

Definition: Let $\theta: G \longrightarrow G'$ be a group homomorphism. Then the **kernel** of the homomorphism θ, denoted by $\ker\theta$, is the set of all elements of G that are mapped to the identity element of G'. That is

$\ker\theta = \{g \in G / \theta(g) = e'$, the identity of $G'\}$



Theorem 6.6 Let $\theta: G \longrightarrow G'$ be a group homomorphism. Then $\ker\theta$ is a normal subgroup of G. Moreover θ is a monomorphism iff $\ker\theta = \{e\}$

Proof

Since $\theta(e) = e' \Rightarrow e \in \ker\theta$, i.e. $\ker\theta \neq \emptyset$. Let $a, b \in \ker\theta$ then $\theta(a) = \theta(b) = e'$. Now $\theta(ab^{-1}) = \theta(a)\theta(b^{-1})$

$= \theta(a)\theta(b)^{-1}$

$= e' \cdot e'^{-1} = e' \cdot e' = e'$

so that $ab^{-1} \in \ker\theta$. Thus, $\ker\theta$ is a subgroup of G.

if $a \in \ker\theta$ and $g \in G$, then

$\theta(gag^{-1}) = \theta(g)\,\theta(a)\,\theta(g^{-1})$

$= \theta(g)\,\theta(a)\,\theta(g)^{-1}$

$= \theta(g)\,e'\,\theta(g)^{-1} = \theta(g)\theta(g)^{-1} = e'$

$(a^2 = a)$ - Idempotent.

Hence, $gag^{-1} \in \ker\theta$, and $\ker\theta$ is normal in G

To prove the second part of the theorem suppose θ is one-one and let $a \in \ker\theta$. Then $\theta(a) = e' = \theta(e)$ since θ is one-one, we must have $a = e$ ie $\ker\theta = \{e\}$

Conversely, suppose that $\ker\theta = \{e\}$ and let $\theta(a) = \theta(b)$ for $a, b \in G$ Then

$$\theta(a)\theta(b)^{-1} = e'$$

and so, $ab^{-1} \in \ker\theta = \{e\}$. Thus we must have $ab^{-1} = e \Rightarrow a = b$ showing that θ is one-one

□

Corollary 6.7: A homomorphism $\theta: G \to G'$ of G onto G' is an isomorphism if and only if $\ker\theta = \{e\}$

□

Recall that a group is isomorphism is a bijective homomorphism. If there is an isomorphism between the group $(G, \cdot)$ $(H, *)$, we say that $(G, \cdot)$ and $(H, *)$ are isomorphic and write $G \cong H$.

Group homomorphism preserves identities and inverse. Certainly some but not all of the group structure is preserved. Our examples show that a homomorphic image of an infinite group may be finite, and a homomorphic image of a non-abelian group may be abelian

Example: Let M_2 be the multiplicative group of ~~non-sin~~ non-singular 2×2 matrices with real entries. We

define a mapping $\phi: M_2 \longrightarrow \mathbb{R}^*$, the multiplicative group of real numbers, by letting $A\phi = |A|$, where A is an element of M_2 and $|A|$ is its determinant. It follows from the well-known fact that $(AB)\phi = |AB| = |A||B| = (A\phi)(B\phi)$ and so, ϕ is a homomorphism.

Example: Let G be the multiplicative group of non-zero complex numbers and let H be the multiplicative group of matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, where a, b are real numbers not both zero. (Verify that H is a group)

Define $\phi: G \to H$ by

$$(a+ib)\phi = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Then $(a+ib)(c+id) = (ac-bd) + i(ad+bc)$

$$\therefore ((a+ib)(c+id))\phi = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$$

and $(a+ib)\phi \cdot (c+id)\phi = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$

$$= \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$$

And so, ϕ is a homomorphism

Now if $(a+ib)\phi = (c+id)\phi$, then

$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ from which $a=c$ and $b=d$ so $a+ib = c+id$ Also, any element $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ in H is an image $x+iy$ in G. Thus ϕ is onto and so, an isomorphism

$n+1=1 \in \mathbb{Z}_n$

Exercise: Show that the mapping $\theta: \mathbb{Z} \to \mathbb{Z}_n$ defined by $\theta(x) = \bar{x}$ and $\phi: M_2 \to \mathbb{R}^*$ defined by $\phi(A) = |A|$ are not isomorphisms.

Proposition 6.8: Any infinite cyclic group is isomorphism to $\mathbb{Z}$, and any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$

Proof 4/9/2018

Let $G = \langle a \rangle = \{ a^n / n \in \mathbb{Z} \}$ be any cyclic group generated by a. Definition a mapping $\theta: \mathbb{Z} \to G$ by $\theta(n) = a^n$ for all $n \in \mathbb{Z}$. Now

$\theta(m+n) = a^{m+n} = a^m a^n = \theta(m)\theta(n)$. Since G is an infinite cyclic group all the powers of a are distinct and so, θ is a one-one mapping Moreover θ is onto. Thus, θ is an isomorphism.

Now, suppose $G = \langle a \rangle = \{ e, a, a^2, \ldots, a^{n-1} \}$ is a finite cyclic group of order n. Then define $\phi: \mathbb{Z}_n \to G$ by $\phi(\bar{r}) = a^r$ for all $\bar{r} \in \mathbb{Z}_n$

$\phi(\bar{r} + \bar{s}) = \phi(\overline{r+s}) = a^{r+s} = a^r a^s = \phi(\bar{r})\phi(\bar{s})$

Moreover ϕ is one-one because if $\bar{r} \neq \bar{s}$, Then $r \neq s$ $(0 \leq r, s \leq n-1)$ and so, $a^r \neq a^s$. Thus $\phi(\bar{r}) \neq \phi(\bar{s})$. ϕ is clearly onto. Therefore ϕ is an isomorphism. □

Corollary 6.9: Any two cyclic groups of the same order are isomorphic.

Corollary 6.10 for each prime p, there is a unique (up to isomorphism) group of order p.

Proposition 6.11: Corresponding elements under a group isomorphism have the same order.

Proof

Let $\theta: G \to H$ be a group isomorphism, and let $\theta(g) = h$. Suppose that g and h have orders m and n respectively, where m is finite. Then

$h^m = (\theta(g))^m = \theta(g^m) = \theta(e_G) = e_H$ so n, the order of h, is also finite, and $n \leq m$, since n is the least positive integer with the property $h^n = e$.

Now, if n is finite,

$\theta(g^n) = \theta(g)^n = h^n = e = \theta(e)$.

Since θ is one-one, $g^n = e$, and hence m is finite and $m \leq n$. Therefore, either both m and n are finite and $m = n$, or both m and n are infinite. □

Theorem 6.12 Isomorphism between groups is an equivalence relation.

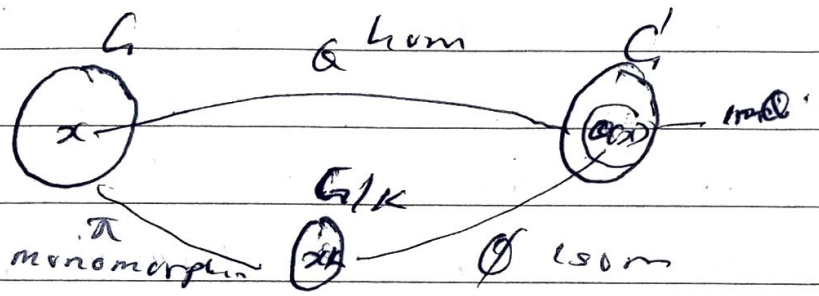
Proof

i. Clearly $G \cong G$, the identity mapping from G onto G, will do. (reflexive)

Let $\phi = \phi^{-1}$ be its inverse. Then ϕ is an isomorphism from H onto G and $H \cong G$. (symmetric)

iii) Suppose $G \cong H$ and $H \cong K$ and let $\phi_1 : G \to H$ and $\phi_2 : H \to K$ be the corresponding isomorphisms. The $\phi_1 \phi_2$ is an isomorphism from G to K so that $G \cong K$ (transitive) ∎

Theorem 6.13 (first isomorphism theorem)
Let $\theta : G \to G'$ be a group homomorphism of G into G'. Then $G/K \cong \text{im}\,\theta$, where K is the kernel of θ.



Proof:

Define a mapping $\phi : G/K \to \text{im}\,\theta$ by $\phi(aK) = \theta(a)$. We first show that ϕ is well-defined, so suppose $aK = bK$, then $a^{-1}b \in K$ and so, $\theta(a^{-1}b) = e'$, the identity in G'. Thus

$$e' = \theta(a^{-1}b)$$
$$= \theta(a^{-1})\theta(b)$$
$$e' = \theta(a)^{-1}\theta(b),$$

Hence, $\theta(a) = \theta(b)$, showing that θ is well-defined.
Now, let aK, bK be two elements of G/K. Then

$\phi(ak \cdot bk) = \phi(abk) = \theta(ab) = \theta(a)\theta(b)$
$= \phi(ak)\phi(bk)$. Thus ϕ is a homomorphism
ϕ is one to one because if $\phi(ak) = \phi(bk)$, then
$\theta(a) = \theta(b)$, i.e $\theta(ab^{-1}) = \theta(a)\theta(b)^{-1} = e'$.
This implies that $ab^{-1} \in k$ showing that $ak = bk$.
ϕ is onto because θ is onto $\text{im}\theta$. Thus, ϕ is
an isomorphism.

□

Example 18/9/2018

1. The mapping $\theta: \mathbb{Z} \to \mathbb{Z}_n$ defined by $\theta(x) = \bar{x}$ is a homomorphism and has $n\mathbb{Z}$ as its kernel. Therefore by the first isomorphism theorem, we have $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

2. Let a and b be the generators of the cyclic groups C_{12} and C_6, respectively. Define the homomorphism

$\theta: C_{12} \longrightarrow C_6$

by $\theta(a^r) = b^{2r}$. The kernel of θ is $k = \{e, a^3, a^6, a^9\}$ and so, $C_{12}/k \cong \text{im}\theta = \{e, b^2, b^4\}$. This isomorphism is obtained by mapping the cosets ka^r to b^{2r}

Theorem 6.14: (Cayley's theorem)

Every group is isomorphic to a group of permutation of a suitable set.

Proof

Let G be a group. Let a be a fixed element of G and define a mapping f_a of G into G by $xf_a = xa$

$f_a: G \to G$

$x \xrightarrow{\quad} xa$

$G \to H$
$a \to \rho_a$

for all $x \in G$. We first show that ρ_a is a permutation. First, ρ_a is one-one, for if $x\rho_a = y\rho_a$ then $xa = ya$ and by the cancellation law $x = y$. Secondly, ρ_a is onto G, for given $b \in G$ we have $(ba^{-1})\rho_a = ba^{-1}a = b$.

Now, we prove that $H = \{\rho_a : a \in G\}$ with the usual multiplication of mapping is a group.

For $\rho_a, \rho_b \in H$, $x(\rho_a \rho_b) = (x\rho_a)\rho_b = (xa)\rho_b = (xa)b = x(ab)$ $= x\rho_{ab}$. Hence $\rho_a \rho_b = \rho_{ab} \in H$. If then follows that H is a group with identity ρ_e and $\rho_a^{-1} = \rho_{a^{-1}}$

$\rho_a \rho_e = \rho_{ae} = \rho_a = \rho_{ea} = \rho_e \rho_a$

$\rho_a \rho_{a^{-1}} = \rho_{aa^{-1}} = \rho_e = \rho_{a^{-1}a} = \rho_{a^{-1}} \rho_a$

Lastly, we show that G is isomorphic to H let θ be the mapping from G to H such that $\theta(a) = \rho_a$ for all $a \in G$. Then θ is a homomorphism since

$$\theta(ab) = \rho_{ab} = \rho_a \rho_b = \theta(a)\theta(b).$$

The map θ is one-one since $\theta(a) = \theta(b)$ then $\rho_a = \rho_b$ and so $e\rho_a = e\rho_b$ implying that $a = b$.

Clearly, θ is onto. Hence θ is the required isomorphism. Therefore G is isomorphic to a group of permutations of a suitable set.

□

Definitions: An isomorphism of a group G onto itself is called an automorphism.

$G \xrightarrow{\text{hom}} G$ – endomorphism

Theorem 6.15 The set of all automorphisms of a group forms a group, called the group of automorphisms of G

$Aut(G)$ — group

$End(G)$ — monoid

Fermat's theorem

Recall that the mapping $\varphi: \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ defined by $\varphi(a) = a + n\mathbb{Z}$ is an isomorphism, i.e. $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

In particular for $\mathbb{Z}_p$, p a prime, the elements $\bar{1}, \bar{2}, \dots \bar{p-1}$ form a group of order $p-1$ under multiplication module p. since the order of any element in a group divides the order of the group, we see that for $b \neq \bar{0}$ and $b \in \mathbb{Z}_p$ we have

$$b^{p-1} = 1 \text{ in } \mathbb{Z}_p$$

Using the fact that $\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, we see at once that for any $a \in \mathbb{Z}$ not in the coset $0 + p\mathbb{Z}$, we have $a^{p-1} \equiv 1 \pmod{p}$. This gives us, at once the so-called little theorem of fermat.

Theorem (Little Theorem of fermat)

If $a \in \mathbb{Z}$ and p is a prime not dividing a, then p divides $a^{p-1} - 1$, that is $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$

Corollary If $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$ for any p

Proof:

The result follows from the theorem above if $a \not\equiv 0 \pmod{p}$. If $a \equiv 0 \pmod{p}$, then both sides reduce to 0 modulo p.

□ $\quad 0 \equiv 0 \pmod{p}$

Examples:

1. Show that $2^{11,213} - 1$ is not divisible by 11

Solution

By Little theorem of fermat,

$2^{10} \equiv 1 \bmod(11)$. So

$2^{11,213} - 1 \equiv (2^{10})^{1,121} \cdot 2^3 - 1$

$\equiv 1^{1,121} \cdot 2^3 - 1$

$\equiv 2^3 - 1$

$\equiv 7 \bmod(11)$

Thus the remainder of $2^{11,213} - 1$ when divided by 11 is 7 not 0 and so, $2^{11,213} - 1$ is not divisible by 11.

2. Show that for every integer n, the number $n^{33} - n$ is divisible by 15

Solution

Now, $15 = 5 \cdot 3$, we shall use Little theorem of fermat to show that $n^{33} - n$ is divisible by both 3 and 5 for any n. Note that $n^{33} - n = n(n^{32} - 1)$

If 3 divides n, then surely 3 divides $n(n^{32} - 1)$.

If 3 does not divide n, then $n^2 \equiv 1 \bmod(3)$ So,

$n^{32} - 1 \equiv (n^2)^{16} - 1 = 1^{16} - 1 \equiv 0 \bmod (3)$

And Hence 3 divides $n^{32} - 1$. Thus in all cases 3 divides $n^{33} - n$. Similarly, if 5 divides n, then 5 divides $n(n^{32} - 1)$. If 5 does not divides n, then $n^4 \equiv 1 \pmod 5$ so that $n^{32} - 1 \equiv (n^4)^8 - 1 \equiv 1^8 - 1 \equiv 0 \bmod$ and hence 5 divides $n^{32} - 1$

Thus, in all cases 5 divides $n^{33} - n$. If then follow that $n^{33} - n$ is divisible by 15 for all n.

7. ALGEBRAIC STRUCTURES

Ring $(R, +, \cdot)$

i $(R, +)$ abelian group.

ii $(R, \cdot)$ semigroup.

A. Rings and fields 19/9/2018

Definition: A ring is a non-empty set R together with two binary operations $+$ and $\cdot$, subject to the following conditions:

1. R is an abelian group with respect to $+$, ie
   i $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$
   ii $\exists\ 0 \in R$ such that $a + 0 = a = 0 + a$
   iii for each $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0 = (-a) + a$
   iv $a + b = b + a$ for all $a, b \in R$
2. R is a semigroup with respect to $\cdot$ ie

$a(bc) = (ab)c$, for all $a, b, c \in R$

3 Multiplication distribution over addition i.e

(i) $a(b+c) = ab + ac$

(ii) $(b+c)a = ba + ca$ for all $a, b, c \in R$

Definition: A ring R is called a ring with unity (or identity element) if there exists an element $1 \in R$ such that $a \cdot 1 = a = 1 \cdot a$ for all $a \in R$.

Definition: A ring R is said to be a commutative ring if $ab = ba$ for all $a, b \in R$

Examples

1. $R = \mathbb{Z}$, is a ring with respect to the usual addition and multiplication of integers. It is a commutative ring with unity. It is called the ring of integers.
2. $R = 2\mathbb{Z}$ is also a ring with addition and multiplication of integers. It is a commutative ring without identity.
3. $R = \mathbb{Z}_n$, the additive abelian group of residue classes modulo n, is a ring with multiplication defined by

$$\bar{i} \cdot \bar{j} = \bar{k}$$

where $ij \equiv k \pmod{n}$, $0 \leq k \leq n-1$

The multiplication is clearly associative and distributive over (addition) i.e $\bar{i}(\bar{j} + \bar{k}) = \bar{i}\bar{j} + \bar{i}\bar{k}$ and $(\bar{j} + \bar{k})\bar{i} = \bar{j}\bar{i} + \bar{k}\bar{i}$

This ring $\mathbb{Z}_n$ is commutative with identity.

4. Let $R = C[0,1]$ be the set of all real valued continuous functions on $[0, 1]$.

Define $+$ and $\cdot$ in R by

$$(f+g)(t) = f(t) + g(t) \quad \text{and}$$

$$(fg)(t) = f(t)g(t).$$

Then R is a ring with the constant function 1 as its identity element. R is also commutative.

5. Let R be the set of rational, or real or complex numbers. Then R is a ring with with the usual $+$ and $\cdot$. It is commutative with unity

6. Let $R = M_2(\mathbb{R})$ be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with a, b, c, d real. Then R is a ring with the usual addition and multiplication of matrices. It is a ring with identity but not commutative.

7. $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is a ring with the usual addition and multiplication of complex number. It is a commutative ring with identity $1 = 1 + 0\sqrt{-5}$.

8. Let R be the set of all subsets of a set X. Define $+$ and $\cdot$ in R by

$$A + B = A \setminus B \cup B \setminus A$$

and $AB = A \cap B$.

R is an abelian group with $+$ with $\emptyset$ (empty set) as the zero element and A is the inverse of A ($-A = A$).

It is a commutative with identity X.

$AX = A \qquad \emptyset = X$

9. Let $R = \{a+bi+cj+dk \mid a,b,c,d \in R\}$ with $+$ given by

$(a+bi+cj+dk)+(a'+b'i+c'j+d'k)$

$=(a+a')+(b+b')i+(c+c')j+(d+d')k$.

Then R is an abelian group with $0 = 0+0i+0j+0k$ as zero element and $-a+bi-cj-dk$ as the additive inverse of $a+bi+cj+dk$.

Define $\cdot$ on R component wise using the rule

$i^2=j^2=k^2=-1$, $ij=k=-ji$, $jk=i=-kj$, $ki=j=-ik$

This multiplication is associative Thus R is a ring with unity $1 = 1+0i+0j+0k$

R is clearly not commutative. This ring is called the ring of quoternions.

The following results are direct consequence of the definition.

Proposition 7.1 Let R be a ring. Then

(i) $a0 = 0 = 0a$, $a \in R$

(ii) $a(-b) = (-a)b = -(ab)$, $a, b \in R$

(iii) $(-a)(-b) = ab$, $a, b \in R$

Proof

(i) $a0 = a(0+0) = a0 + a0$. If $a0 = b$ then $b = b+b$.

By the Cancellation Law, $b = 0$ ie $a0 = 0$.

Similary $0a = 0$

(ii) $0 = 0b = (a+(-a))b$

$= ab + (-a)b$

By uniqueness of inverses, $-(ab) = (-a)b$ similarly $-(ab) = a(-b)$.

(iii) $a + (-a) = 0 = (-a) + a$, showing that $a = -(-a)$. Replacing a by $(-a)$ in (ii), we have $(-a)(-b) = -((-a)b) = -(-(ab))$

$= ab$. □

25/9/2018

Definition: A commutative ring with identity $1 \neq 0$ in which every non-zero element has an inverse with respect to multiplication is called a field.

$(R, +, \cdot)$

$(R, +)$ – abelian group $(R, \cdot)$ – semigroup

$(R \setminus \{0\}, \cdot) \rightarrow$ abelian group $\Rightarrow$ Fields.

Examples

1. The rings of rational, real and complex numbers are all fields.

2. Let $R = \mathbb{Z}_p$, the ring of residue classes modulo p a prime. We have seen that R is a commutative ring with identity.

T. We have, for $\bar{a}$, for $\bar{a} \neq 0$ in $\mathbb{Z}_p$ a is relatively prime to p. Hence $\lambda a + \mu p = 1$

for some $\lambda, \mu \in \mathbb{Z}$

And so, in particular $\bar{\lambda}\bar{a} = \bar{1}$ that is, $\bar{a}$ has a multiplicative inverse. Thus $\mathbb{Z}_p$ is a field. It is a finite

$\bar{\lambda}\bar{a} + \bar{\mu}\bar{p} = \bar{1}$ $\bar{\lambda}\bar{a} + \bar{0} = \bar{1}$

$\Rightarrow \bar{\lambda}\bar{a} = \bar{1}$ { }

~~ring~~ field.

Definition: Let R be a ring with identity element. Then R is called a skew field (or division ring) if every non-zero element has a multiplicative inverse

* Integral Domain: is a ring that is no zero divisor.

Example: Let $R = \{a+bi+cj+dk \mid a,b,c,d \in \mathbb{R}\}$ be the ring of quaternions. R is a ring with identity $1 = 1+0i+0j+0k$. Let ~~$q \in R$~~ $q \in R$, $q \neq 0$. Then $q = a+bi+cj+dk$ ~~in that case~~ with atleast one of a, b, c, d non-zero.

Thus $a^2+b^2+c^2+d^2 \neq 0$. If we let

$$q' = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$$

Then $qq' = q'q = 1$. Therefore every non-zero element in R has an inverse under multiplication. Thus, R is a skew-field.

6. Vector Spaces and Modules

Definition: A non-empty V is called a vector space over a field f, if

(i) V is an abelian group with respect to an operation denoted by $+$

(ii) for each $a \in f$ and $v \in V$, an element $av \in V$ is defined,

Cadano - formular for solving cube equation

satisfying the following conditions:

(a) $a(v+v') = av + av'$, for all $a \in f$ $v, v' \in V$.

(b) $(a+b)v = av + bv$, for all $a, b \in f$, $v \in V$

(c) $a(bv) = (ab)v$ for all $a, b \in f$, $v \in V$

(d) $1v = v$, for all $v \in V$ where 1 is the identity in f

Examples

1. $F = R$, the field of real numbers and $V = R^n = \{(x_1, x_2 \cdots x_n) / x_i \in R\}$. Then V is an abelian group with respect to addition + defined by $(x_1, x_2, \cdots x_n) + (y_1, y_2, \cdots y_n)$
$= (x_1 + y_1, x_2 + y_2 \cdots x_n + y_n)$

The identity element is $0 = (0, 0, \cdots 0)$ and $(-x_1, -x_2 \cdots$ is the inverse of $(x_1, x_2 \cdots x_n)$. Define scalar multiplication by

$a(x_1, x_2 \cdots x_n) = (ax_1, ax_2 \cdots ax_n)$, $a \in F = R$.

This scalar multiplications satisfies the four condition fo a vector space. Thus R^n is a vector space over R

2. If we let F to be any field in example 1. and $V = F^n = \{(x_1, x_2 \cdots x_n) / x_i \in F\}$ with addition + and scal multiplication as in example 1. Then V is still a vector space over F.

3. Let $V = F[x]$ be the ring of polynomials in x over fi field. $F[x] = \left\{ \sum_{r=0}^{\infty} a_r x^r / a_r \in F \right\}$

V is an abelian group for +. Define scalar multip

$q = \sum_{r=0}^{\infty} b_r x^r$ $\quad p+q = \sum_{r=0}^{\infty} (a_r + b_r) x^r$

cation by $a(a_0+a_1x+\cdots+a_nx^n) = aa_0+aa_1x+\cdots+aa_nx^n$
then the axioms of a vector space are satisfied and
V is a vector space over f.

4. Let V be the set of all $m \times n$ matrices with entries from a field f. Then V is a vector space over f with matrix addition and scalar multiplication.

Proposition 7.2 Let V be a vector space over a field f, $v \in V$, $a \in f$. Then

(i) $a0 = 0$

(ii) $0v = 0$

(iii) $(-a)v = a(-v) = -(av)$

(iv) $av = 0 \Rightarrow a = 0$ or $v = 0$

Proof:

(i) Let $w = a0$. Then $w = a0 = a(0+0)$

$= a0 + a0 = w + w$. By cancellative laws for addition, we have $w = 0$

(ii) Let $w' = 0v = (0+0)v$

$= 0v + 0v = w' + w'$

Hence $w' = 0$

(iii) $0 = 0v = (a+(-a))v$

$= av + (-a)v$ By uniqueness of inverse we have $-(av) = (-a)v$. Similarly $a(-v) = -(av)$

(iv) Suppose $av = 0$ and $a \neq 0$. Since f is a field $a^{-1} \in f$ such that $aa^{-1} = 1 = a^{-1}a$. Now

unital

left R module

$V = 1V = (a^{-1}a)V = a^{-1}(aV) = a^{-1}0 = 0.$

Hence, either $a = 0$ or $V = 0$.

Definition: A non-empty set M is said to be a **left module over a ring R** if M is an abelian group under an operation $+$ such that for every $r \in R$, $m \in M$, there exists a unique element $rm \in M$ subject to the following conditions.

(i) $r(a+b) = ra + rb$, $r \in R$ $a, b \in M$

(ii) $(r+s)a = ra + sa$, $r, s \in R$, $a \in M$

(iii) $r(sa) = (rs)a$, $r, s \in R$, $a \in M$

(iv) $1a = a$. → if R has identity M - unital left R module

Example

1. Every vector space over f is a module over f.
2. Every abelian group is a left module over the ring of integers.

Solution

for any integer $n \in \mathbb{Z}$ and for any element $a \in G$ we defin na as follows:

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n\text{-times}} & n > 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{n\text{-times}} & n < 0 \\ 0 & n = 0 \end{cases}$$

It is easy to see that, for an integer $m > 0$

Ring of integer is called ring with unity - monoid

$-(ma) = m(-a) = \underbrace{(-a)+(-a)+\cdots+(-a)}_{m\text{-times}}$

$= -(\underbrace{a+a+\cdots+a}_{m\text{ times}})$

$r(a+b) = ra+rb$

① $m(a+b) = \underbrace{(a+b)+(a+b)+\cdots+(a+b)}_{m\text{-times}}$

$n>0$

$= \underbrace{a+a+\cdots+a}_{m\text{-times}} + \underbrace{b+b+\cdots+b}_{m\text{-times}}$

$= ma+mb$

$n<0$ then $m=-n$, $n>0$

$m(a+b) = -n(a+b)$

$= -(na+nb)$

$= -(na)+[-(nb)]$

$= (-n)a+(-n)b$

$= ma+mb$

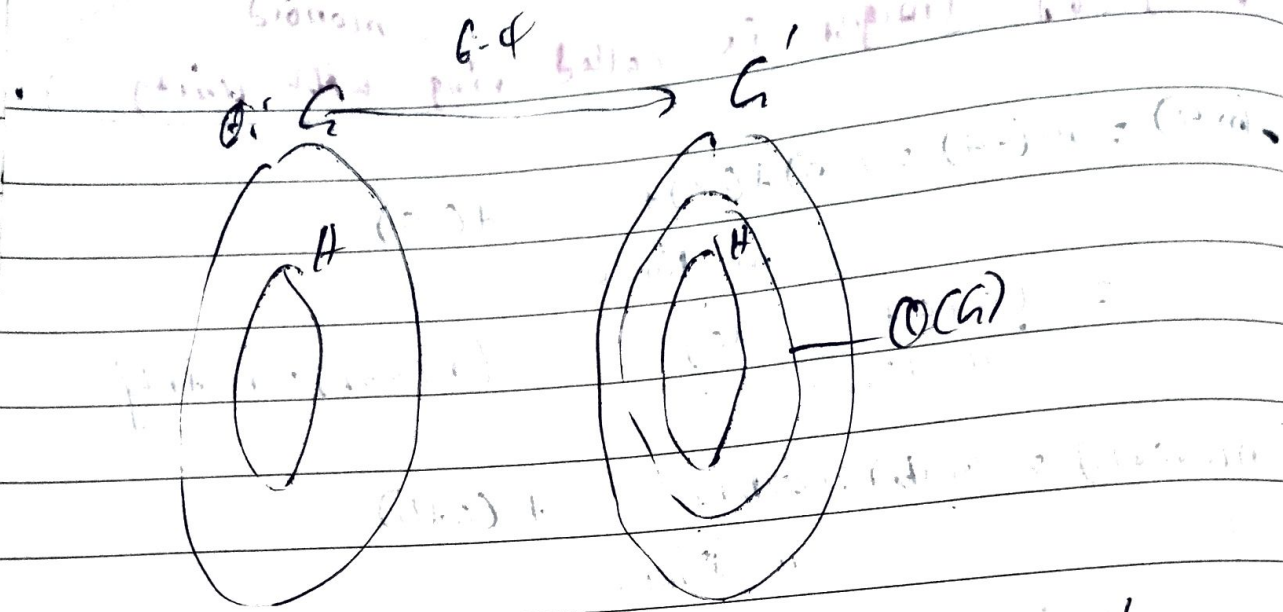
$m=0$

$m(a+b) = 0 = 0+0 = ma+mb$,

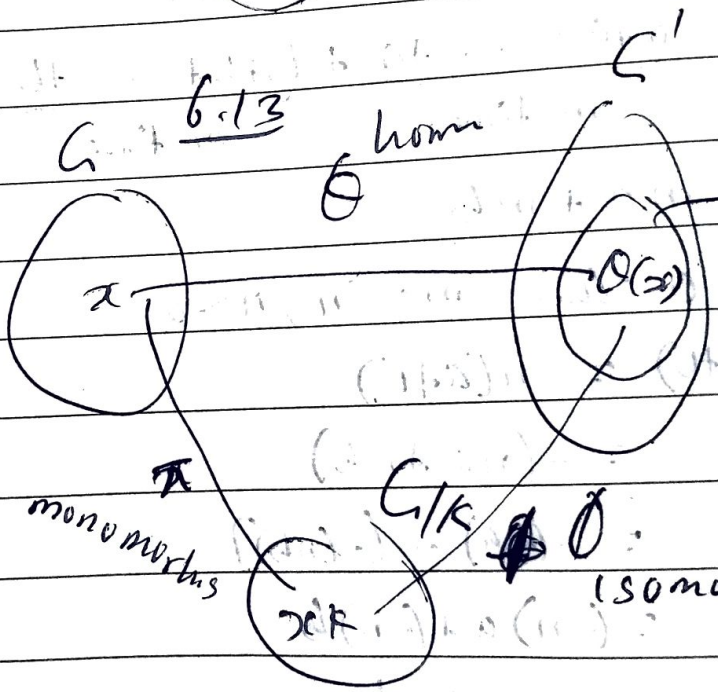
It is easy to show that conditions (ii) and (iii) are true

Hence G is a left $\mathbb{Z}$-modules

* Every ring is an example of modules over itself.



6.13



a set is said to be infinite if there is a proper subset that is equivalent to that set. A set is said to be finite if its can be put one to one correspondence with a set of N

$$n = (1\ 2\ -\ \text{---}\ n)$$

$$\downarrow$$

$$\mathbb{N}$$

Quotient Group

$G/N = \{Na : a \in G\}$

$G/N = \{Na_1, Na_2, \ldots, Na_n\}$

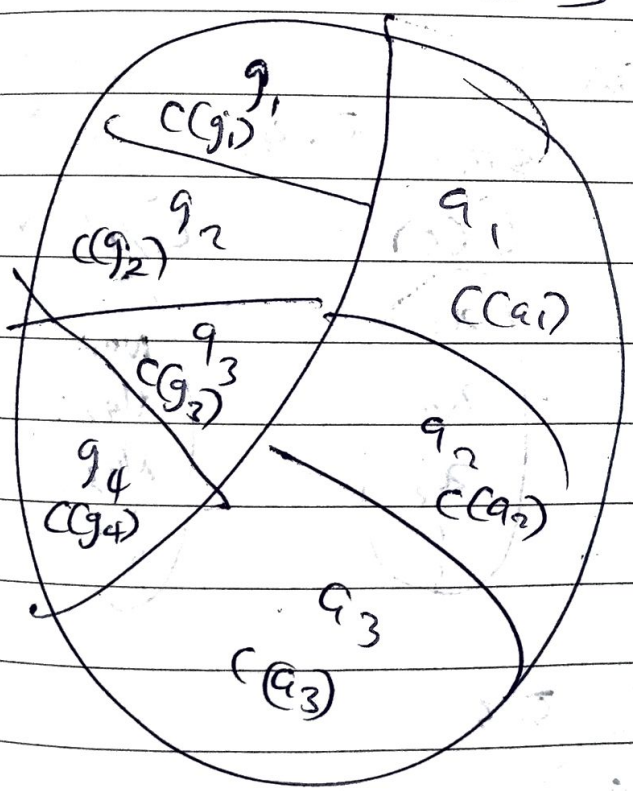
refle: $Na_1 = Na_1 \bmod N$

$Na_1 Na_i^{-1} = N(a_1 a_i^{-1}) = Ne = N$

Sym: $Na_1 = Na_2 \bmod N$

$Na_1 Na_2^{-1} = N(a_1 a_2^{-1})$

5.5



$|G| = \sum |C(a)|$

$|G| = |C(g_1)| + |C(g_2)| + |C(g_3)| + \sum |C(a_i)| = [G : N(a)]$

$|G| = |Z(G)| + \sum [G : N(a)]$

$[G : N(a)] > 1$

5.6

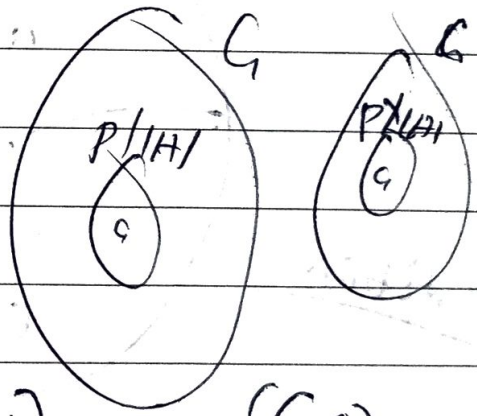
$[G : N(a)] = \frac{|G|}{|N(a)|} = \frac{p^n}{p^m}$

$p^{n-m} > 1$

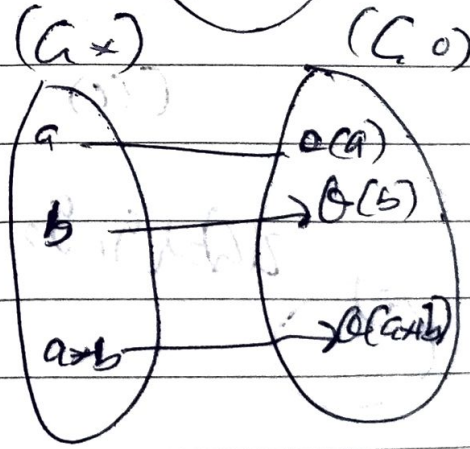
$O(a) = p$

$\langle a \rangle = \{a, a^2, a^3, \ldots, a^{p-1}, a^p = e\}$

Cyclic subgroup generated by a



Homo



$O(a*b) = O(a) \cdot O(b)$

$O(ab) = O(a)\,O(b)$

$5\mathbb{Z} = \{0, \pm 5, \pm 10, \pm 15, \ldots\}$

$\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$\bar{0} = 5\mathbb{Z}$

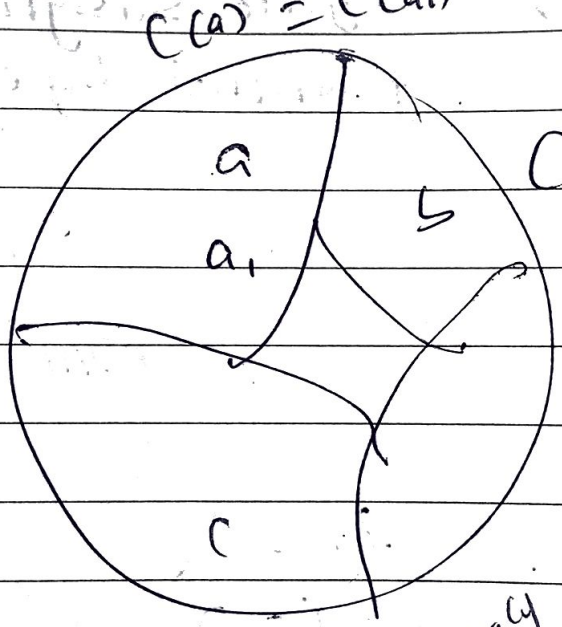
$\bar{1} = 5\mathbb{Z}+1$

$\bar{2} = 5\mathbb{Z}+2$

$\bar{3} = 5\mathbb{Z}+3$

$\bar{4} = 5\mathbb{Z}+4$

Collection of right coset $G/N(a)$



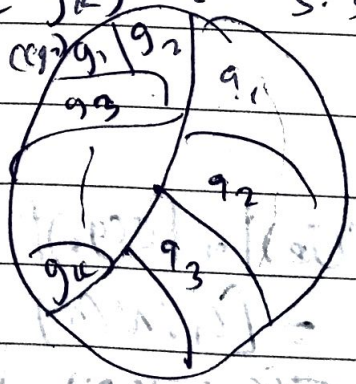
Partition

Conjugacy classes

5.3

$Z(G) = \{g_1, g_2, \ldots g_k\}$

5.5



5.4 size of normal subgroup, index