Notes

October 20, 2014

if G is a group, and $A \subseteq G$ and $B \subseteq G$ then $AB = \{ab | a \in A, b \in B\} \subseteq G$.

proposition

let G be a group, then H, K subgroups of G. Assume that $h^{-1}kh \in K$ for all $h \in H$, $k \in K$ then HK is a subgroup of G that contain s both H and K, in fact, HK is the smallest subgroup of G that contains both H and K. Assumption only important if we are not dealing with abelian groups.

proof

$a, b \in HK$. Write $a = h_1k_1, b = h_2k_2$ with $h_i \in H, k_i \in K$ then $a \cdot b = h_1k_1h_2k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2 \in HK$
$a = hk, a^{-1} = (hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1}) \in HK$

examples

$S_3, H = \{(1), (12)\}, K = \{(1), (123), (132)\}, (12)(123) = (23) \in HK, (12)(132) = (13) \in HK$ so $HK = G$ and is therefore contained by G

$(\mathbb{Z}, +)$, $H = a\mathbb{Z}, k = b\mathbb{Z}$, let $d = (a, b)$

claim: $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. clearly $a\mathbb{Z} \subseteq d\mathbb{Z}$, $b\mathbb{Z} \subseteq d\mathbb{Z}$.

$a\mathbb{Z} + b\mathbb{Z}$ is the smallest subgroup that contains both $a\mathbb{Z}$ and $b\mathbb{Z}$. so $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$.

$d = \gcd(a, b)$ so we can write $d = ma + nb$. let $\alpha \in d\mathbb{Z}$ and write $\alpha = dt, t \in \mathbb{Z}$ then $\alpha = dt = mat + nbt \in a\mathbb{Z} + b\mathbb{Z}$. so $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$

thm subgroup gen by a subset

G is a group, if $a \in G < a >= \{a^i | i \in \mathbb{Z}\}$ is the smallest subgroupthat contains a.

proof

let $S \subseteq G$, let $< S >= \{\underbrace{a_1a_2 \dots a_k}_{\text{word}} | a_i \in S \text{ or } {a_i}^{-1} \in S, k \in \mathbb{N}\}$ then $< S >$ is a subgroup, $< S >= \cap \forall H$ where $S \subseteq H \subseteq G$, and H is a subgroup of G, $< S >$ is the smallest subgroup of Gthat contains S.

so it is closed under multiplication, identity is in it, and the inverse of all words are in it.

show containment both ways, one is clear because we have words of length 1 that span S and so S is one of the elements of our H intersection.

example

$a, b \in G, S = \{a, b\} \subseteq G, < S >= \{a_1a_2 \dots a_k | a_i \in \{a, a^{-1}, b, b^{-1}\}\}$
if $ab = ba$ then $< S >= \{a^ib^j | i \in \mathbb{Z}, j \in \mathbb{Z}\}$

maps

studied groups, subgroups. now we are going to talk about maps

if we have groups G_1, G_2 and $\varphi : G_1 \to G_2$ is a group homomorphism provided $x \to \varphi(x), y \to \varphi$ means that $\varphi(x * y) = \varphi(x) * \varphi(y)$ for all $x, y \in G_1$.

examples

identity: $x \to x$

$(\mathbb{R}, +) = G_1, (\mathbb{R}^+, \cdot) = G_2$. $\varphi(x) = e^x$. ie $\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y)$.

notation

let $\varphi : G_1 \to G_2$ be a group homomorphism, then $\ker \varphi = \{x \in G_1 | \varphi(x) = e\}$

homomorphism always takes the identity in G_1 to G_2.

$\varphi(e_1)\varphi(e_1)^{-1} = \varphi(e_1 e_1)\varphi(e_1)^{-1} = \varphi(e_1)\varphi(e_1)\varphi(e_1)^{-1} = e_2 = \varphi(e_1)$

prove that $\ker \varphi$ is a subgroup

now we say that φ is an isomorphism if φ is a group homomorphism and φ is bijective.

both of the previous examples are isomorphisms.

so from an algebraic point of view, there is no difference between addition on the reals and multiplication on the positive reals.

proposition

let φ be an isomorphism. the following are true

1. φ^{-1} which is the map from G_2 to G_1 is also an isomorphism.
2. if G_1 is abelian, then G_2 is abelian.
3. if G_1 is cyclic then so is G_2
4. if $a \in G_1$ then $\text{ord}(a) = \text{ord}(\varphi(a))$

1. need to prove $\varphi^{-1}(\alpha\beta) = \varphi^{-1}(\alpha)\varphi^{-1}(\beta)$ for all $\beta \in G_2$, but φ is injective so it is enough to prove that $\varphi(\varphi^{-1}(\alpha\beta)) = \varphi(\varphi^{-1}(\alpha)\varphi^{-1}(\beta) = \varphi(\varphi^{-1}(\alpha))\varphi(\varphi^{-1}(\beta)) = \alpha\beta$
2. assume G_1 is abelian
$$\alpha\beta = \varphi(\varphi^{-1}(\alpha)\,\varphi^{-1}(\beta))$$
3. hint: assume that $G_1 =< a >$ for some $a \in G_1$ and then prove that $G_2 =< \varphi(a)$
4. no hint

example

$$\mathbb{Z}_4 \not\equiv \mathbb{Z}_2 \times \mathbb{Z}_2$$

by contradiction, assume that there exists an isomorphism φ from z4 to z2+z2. $[1] \in \mathbb{Z}_4$ and $\text{ord}[1] = 4$ so then $\text{ord}\varphi([1]) = 4$. But all elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has no elements of order 4, so there is no isomorphisms. however, if $\gcd(m, n) = 1$ then $\mathbb{Z}_{mn} \equiv \mathbb{Z}_m \times \mathbb{Z}_n$

$$\varphi : [x]_{mn} \to [x]_m[x]_n$$

what does well defined mean?

same input gives same output, ie if $[x] = [y]$ then $\varphi[x] = \varphi[y]$

3.4 #13

$(\mathbb{R}^*, \cdot), C_2 = \{\pm 1\} \subseteq \mathbb{R}^*$. C_2 is a subgroup of $\mathbb{R}^*$. prove that $\mathbb{R}^* \cong \mathbb{R}^+ \times C_2$

we construct an isomorphism $\theta : \mathbb{R}^* \to R^+ \times C_2$.

$x \to (|x|, \frac{x}{|x|})$. prove that θ is a group homomorphism and bijective.

$\theta(xy) = (|xy|, \frac{xy}{|xy|}) = (|x|, \frac{x}{|x|})(|y|, \frac{y}{|y|}) = \theta(x)\theta(y)$

bijectivity is exercise, but a number is uniquely identified by sign and magnitude (absolute value)

example

prove that $\mathrm{ord}(aba^{-1}) = \mathrm{ord}(b)$ for every $a, b \in G$ where G is a group.

$m = \mathrm{ord}(x)$ means $x^m = e$ and $x^k = e$ means that $m|k$.

if given $n = ord(x)$ and $m = ord(y)$ then best way is to show that $m = n$ is $m|n$ and $n|m$. this all works for finit.

this question is trivial if the group is abelian.

so let $m = ord(aba^{-1}), n = ord(b)$

case 1

n is finite, $b^n = e$. consider $(aba^{-1})^n = aba^{-1}aba^{-1} \dots aba^{-1} = ab^n a^{-1} = aea^{-1} = e$ so $ord(aba^{-1})$ is finite, also $m|n$

$b^m = a^{-1} \underbrace{(aba^{-1})(aba^{-1}) \dots (aba^{-1})(aba^{-1})}_{m \text{ times}} a = a(aba^{-1})^m a = a^{-1}ea = e$ so $b^m = e$ and $n|m$

case 2

n is infinite. then we must prove that m is infinite. by contradiction, assume $m < \infty$.

then $b^m = a^{-1} \underbrace{(aba^{-1})(aba^{-1}) \dots (aba^{-1})(aba^{-1})}_{m \text{ times}} a = a(aba^{-1})^m a = a^{-1}ea = e$ so $b^m = e$.

and so the order is finite and we have our contradiction. so m must be finite then

consider

$ord(a^{-1}) = ord(a)$ and $ord(ab) = ord(ba)$

by previous part $ord(ba) = (abaa^{-1}) = ord(ab)$

3.2 # 25 from class

we note that if $x \in G$ has the required order, then $x^{-1} \in G$ also has the required order. note that the $x \neq x^{-1}$ because the order is greater than 2.

!3.3 #9

other things in mind

lets take a group G and H, K subgroups. then $|HK| = \frac{|H||K|}{|H \cap K|}$

recall: $HK = \{hk | h \in H, k \in K\}$

$$\begin{aligned} g &\in HK \\ g &= hk \\ h \in H \quad |H| &= m \\ k \in K \quad |K| &= n \end{aligned}$$

question? how many ways can $g = hk = h'k'$?

$$\begin{aligned} hk = h'k' &\to (h')^{-1}hk = k' \\ (h')^{-1}h &= k'k^{-1} \in H \cap K \end{aligned}$$

so $k' = \alpha k, h' = h\alpha^{-1}$

that is to say $hk = (h'\alpha)(\alpha^{-1}k')$ there are $|H \cap K|$ ways to choose alpha

october 15

read 3.6.2

3.6 #2

Write out the addition tables for $\mathbb{Z}_4$ and for $\mathbb{Z}_2 \times \mathbb{Z}_2$. Use cycle notation to write out the permutation determined by each row of each of the addition tables as in the discussion preceding Cayley's theorem.

+	[0]	[1]	[2]	[3]	(1)
[0]	[0]	[1]	[2]	[3]	(1)
[1]	[1]	[2]	[3]	[0]	(1234)
[2]	[2]	[3]	[0]	[1]	(13)(24)
[3]	[3]	[0]	[1]	[2]	(1432)

+	([0], [0])	([0], [1])	([1], [0])	([1], [1])	(1)
([0], [0])	([0], [0])	([0], [1])	([1], [0])	([1], [1])	(1)
([0], [1])	([0], [1])	([0], [0])	([1], [1])	([1], [0])	(12)(34)
([1], [0])	([1], [0])	([1], [1])	([0], [0])	([0], [1])	(13)(24)
([1], [1])	([1], [1])	([1], [0])	([0], [1])	([0], [0])	(14)(23)

last time

$\varphi : G \to \text{Sym}(G)$

rigid motions of a regular n-gon

place the first vertex, then the second. we have n options for the first vertex, and 2 options for the second. and the rest are fixed. so we can do $2n$ rigid motions for any n-gon.

observation, rigid motions give us permutations, but for $n > 3$ we can't get all the permutations. $2 \cdot 4 < 4!$.

the rigid motions form a group.

goal: describe this group

a =counterclockwise rotation by $\frac{2\pi}{n}$ radians or $\frac{360}{n}^\circ$. order of a is n, that is to say, rotating n times gives us our original vertex placement.

a^i =rotation by $\frac{2\pi}{n} \cdot i$.

b =reflection about line L this will leave one or two vertices unchanged, depending on the parity of n.

$b = (2, n)(3, n-1)\dots$.

$b^2 = e$.

consider $\{b, ab, a^2b, \dots, a^{n-1}b\}$. remember a, b are functions so $ab = a \circ b$

$a^i b = a^j \Rightarrow a^i = a^j \Rightarrow a^{j-i} = e$ but $a^{j-1} = e$ iff $n|j-i$.

$a^i b$ =the flip about the line L_i that makes $\frac{\pi i}{n}$ with L, this means that $\text{ord}(a^i b) = 2$ because it's just a flip.

now we have n rotations and n flips. note that no flip can be a rotation because a flip changes orientation.

D_n denotes $\{e, a, a^2, \dots, a^{n-1}, b, ba, ba^2, \dots, ba^{n-1}\}$ which is the dihedral group with 2n elements. $a^n = e$ and $b^2 = e$.

notice that the order of the group reflects the symmetry of the geometric representation. a completely assymetric object with have only the e rigid motions, while a circle will have infinitely many.

what is ba? it's $a^{-1}b = a^{n-1}b$

october 20

assnmnt: 3.6 #21,23,25 if odd, has identity, if even, identity and half rotation $(r^{n/2})$ $a^j b = ba^j \to a^j b = a^{-j} b \to a^j = a^{-j} \to a^{2k} = e \to n|2j$

last time started homomorphisms

definition

$\varphi : G_1 \to G_2$ is group homomorphism then $\text{Im}\varphi = \varphi(G_1)$ is a subgroup of G_2 and $\text{Ker}(\varphi) = \{x \in G_1 : \varphi(x) = e_2\} = \varphi^{-1}(\{e_2\})$ beause $\{e_2\} \leq G_2$ is a normal subgroup, $\text{Ker}(\varphi) \leq G_1$ is a normal subgroup

equivalence relation defines a group homomorphism

on $G_1/\sim$ define the operation $[x][y] = [xy]$. is this well defined?

$[x] = [x']$ and $[y] = [y']$. $\varphi(x) = \varphi(x')$, and $\varphi(y) = \varphi(y')$ and so $\varphi(x)\varphi(y) = \varphi(x')\varphi(y')$ and homomorphism definition gives us $\varphi(xy) = \varphi(x'y')$.

claim , with this operation $G_1/\sim$ is a group. $[e_1]$ is identity. $[x]$ is inverse of $[x^-1]$.

let $\pi(x) = [x]$. claim π is a group homomorphism.

$\pi(xy) = [xy] = [x][y] = \pi(x)\pi(y)$.

why does $[xy] = [x][y]$

thrm

Let $\varphi : G_1 \to G_2$ be a group homomorphism. then $G_1/\sim \cong \varphi(G_1)$

proof:

$G_1 \sim\to \varphi(G_1)$

$[x] \to \varphi(x)$

$\overline{\varphi}([x]) = \varphi(x)$ claim: $\overline{\varphi}$ is a group homomorphism $\bar{(}[x][y]) = \overline{\varphi}([xy]) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}([x])\bar{(}[y])$

claim: surjectivity is clear claim: $\overline{\varphi}$ is injective. $\overline{\varphi}([x]) = \overline{\varphi}([x]) \to \varphi(y) = \varphi(x) \to x \sim y \to [x] = [y]$

assignment for next time

$\varphi : \mathbb{Z}_m \to \mathbb{Z}_n$ where φ is group homomorphism. hint: $\varphi(0) = 0$ and $\varphi([1]) = [k]$ then $\varphi([j]) = \varphi([jk])$. take $Z_2 \to \mathbb{Z}_4$ then $\varphi([1]) \neq [1]$