

Chapter 7.2 parts 1 & 2

7.2 Basic properties of groups.

Notation: instead of $a * b$ we write ab

Th 7.5 Let G be a group

(1) identity element in G is unique (only its existence is required in the definition)

(2) if $ab=ac$ then $b=c$

$$ba = ca \quad b = c$$

(3) The inverse for every element
is unique

$$e \in G$$

$$ea = ae = a$$

| justifies the notation a'
for the inverse of a
 $da = ad = e$

Rem $b=c$ does not mean ~~$b=c=0$~~
 $bc^{-1}=e$

$b=c$ means that b and c denote
the same element of the group

Cot 7.6

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

(2) $(a')^{-1} = a$

Pf $(ab)^{-1}$ is the unique inverse of ab

Thus if $b^{-1}a^{-1}$ is an inverse to ab , then $b^{-1}a^{-1}$ is the (unique) inverse for ab
 meaning $b^{-1}a^{-1} = (ab)^{-1}$

It is thus sufficient to show that $(b^{-1}a^{-1})(ab) = e$ & $(ab)(b^{-1}a^{-1}) = e$

Indeed: $(b^{-1}a^{-1})(ab) = b^{-1}a^{-1}ab = b^{-1}(a^{-1}a)b = b^{-1}e b = b^{-1}(eb) = b^{-1}b = e.$

Usual notation with integral powers

$$a^n = \underbrace{a \dots a}_{n \text{ times}} \quad a^{-n} = (a^{-1})^n \quad a^0 = e$$

| a - an element of the group
 n - an integer

Th 7.7 Usual rules apply:

$$a^m a^n = a^{m+n} \quad (a^m)^n = a^{mn}$$

| analogy with ring theory

Remark sometimes one uses + (addition) for group operation.

$\mathbb{Z}_x \oplus$

~~2.3=5~~

$$2+3=5$$

| p 198 - table of correspondences between multiplicative and additive notations

Take $a \in G$, group. Consider a, a^2, a^3, \dots

$$\text{Ex } G = \mathbb{Z} \quad a = 3$$

It may happen that the sequence is periodic:

$$a = e \quad a, a^2, a^3, \dots, a^{k-1}, \underbrace{e, a, a^2, \dots, a^{k-1}}, e, \dots$$

$$3, 6, 9, 12, \dots$$

$$\mathbb{Z}_5 \quad a = 2 \quad +$$

$$2, 4, 1, 3, 0 = e, 2, 4, \dots$$

Def The order of an element $a \in G$

is the smallest positive integer k such that

$$a^k = e$$

$$\mathbb{Z}_5 \setminus \{0\} \quad a = 2 \cdot$$

$$2, 4, 3, 1, 2, 4, \dots$$

$$e$$

If $a^k = e$ never happens then we say that
a has an infinite order

To 7.8 (1) If $a \in G$ has an infinite order,
then a^k for $k \in \mathbb{Z}$ are all distinct

(2) If there exist $i, j \in \mathbb{Z}$ such that $i \neq j$ and $a^i = a^j$
then a has finite order.

Remark If $a \in G$ is of infinite order, then G is infinite.

An infinite group may have elements of finite order

Ex: $\mathbb{R}^* \ni -1$ the order of -1 is 2: $-1 \neq 1 = e$ $(-1)^2 = 1 = e$

$\exists i$: the order of i is 4

Th 7.9 G - a group

$a \in G$ an element of order n

(1) If $a^k = e$, then $n | k$

(2) If $a^i = a^j$, then $i \equiv j \pmod{n}$

(3) If $n = td$ with $d \geq 1$, then a^t has order d

Pf (1) Euclid's Lemma $k = nq + r$ Wanted: $r = 0$
 $0 \leq r < n$

$$a^k = e$$

$a^{nq+r} = e$ $(a^n)^q a^r = e$ implies $a^r = e$ implies $r \geq n$
or $\boxed{r=0}$

(2) - simple

$$(a^t)^d = a^{td} = a^n = e$$

Is d the smallest positive integer with this property?

Let k have $(a^t)^k = e$
the property:

$$a^{t^k} = e$$

from (1): $u \mid t^k \quad td \mid t^k$ implies $d \mid k$ implies $d \leq k$

- Yes, d is the smallest with this property.

Prop (Exer 31a) Let G be a group, $a, b \in G$

Assume that $ab = ba$

Then $(ab)^{|a||b|} = e$.

Pf

$$(ab)^{|a||b|} = \underbrace{abab \dots ab}_{|a||b|} = a^{|a||b|} b^{|a||b|} = (a^{|a|})^{|b|} (b^{|b|})^{|a|} = e^{|b|} e^{|a|} = e$$

Prop (Exer 33) Let G be a group $a, b \in G$

Assume that $ab = ba$

Assume $(|a|, |b|) = 1$.

Then $|ab| = |a||b|$

Pf

$$(ab)^{|a||b|} = e \quad \text{by the previous proposition}$$

Th 7.9(1) implies that $|ab| \mid |a||b|$

The Fundamental Thm of Arithmetic allows us to write

$$|ab| = mn \text{ with } \frac{u|a|}{\cancel{m}} , \frac{n|b|}{\cancel{n}} \\ (m, n) = 1$$

$$(ab)^{\frac{|ab|}{|ab|}} = e$$

$$(ab)^{mn} = e \quad \text{take it to the power } |b|/n:$$

$$\left((ab)^{mn} \right)^{\frac{|b|}{n}} = e$$

$$(ab)^{\frac{u|b|}{|b|}} = e$$

$$a^{\frac{u|b|}{|b|}} b^{\frac{u|b|}{|b|}} = e$$

$$a^{\frac{u|b|}{|b|}} = e$$

$$b^{|b|} = e \text{ implies } b^{\frac{u|b|}{|b|}} = (b^{|b|})^u = e$$

Th 7.9(i) implies that $|a| \mid u|b|$

Since $(|a|, |b|) = 1$, we conclude that $\underline{|a| \mid u}$

We have $\begin{cases} u \mid |a| \\ |a| \mid u \end{cases} \text{ implies } u = |a|$

Similarly, we derive $u = |b|$.

Thus $|ab| = mn$ becomes $|ab| = |a||b|$ as required.

Cox 7.10 Let G be an abelian group.
 Let $c \in G$ be an element of maximal order. }
 Then for every $a \in G$,
 $|a| \leq |c|$

Pf Assume that there is $a \in G$ such that $|a| > |c|$.
 The Fundamental Thm of Arith implies that there is a prime p
 such that

$$|a| = p^r u \quad |c| = p^s n \quad r > s$$

$$(p, u) = 1 \quad (p, n) = 1$$

By Th 7.9(3), $|a^u| = p^r$ $|c^{p^s}| = n$ Note that $(p^r, n) = 1$

By the proposition (Exer 33), $|a^u c^{p^s}| = p^r n > p^s n = |c|$;
 that contradicts the maximality
 of $|c|$.