

Math 830 ABSTRACT ALGEBRA
PROGRESS CHECK – VII

September 11 (Mon), 2006

Instructor: Yasuyuki Kachi

Line #: 17014.

• **Order comparison.**

Let G be a group, and $x \in G$. Recall that the order of x was defined as the smallest $m \in \mathbb{Z}$; $m > 0$ such that $x^m = 1$. Write $m = \text{ord } x$. The order of x is infinity, if there does not exist $m \in \mathbb{Z}$, $m > 0$ such that $x^m = 1$. Write $\text{ord } x = \infty$.

- We have seen that the order of an element of a finite group is always finite. More strongly, the following theorem holds:

Theorem 1. Let G be a finite group. Let $o(G)$ denote the order of G .

- (1) Let $x \in G$ be arbitrary. Then $\text{ord } x$ divides $o(G)$.
- (2) If there exists $x \in G$ such that $\text{ord } x = o(G)$, then
$$G \simeq \mu_m, \quad \text{where } m = o(G).$$
- (3) If $o(G) = p$ is a prime number, then $G \simeq \mu_p$.

Example 1. Let G be a group of order 24, $G \not\simeq \mu_{24}$. Then for $x \in G \setminus \{1\}$, the only possibility for $\text{ord } x$ is

$$2, \quad 3, \quad 4, \quad 6, \quad 8, \quad 12.$$

Example 2. Let G be a group of order 7. Then $G \simeq \mu_7$.

- The proof of the above Theorem 1 requires the notion of congruence ‘ \equiv_H ’ of a group G modulo its subgroup H . We will return to this topic later.

The following result is convenient.

Theorem 2. Let $f : G_1 \xrightarrow{\sim} G_2$ be a group isomorphism. Let $x \in G_1$. Then

$$\text{ord } x = \text{ord } f(x).$$

• **Application.** We are now ready to show that the two non-abelian groups of order 8, namely,

$$D = \left\{ \begin{array}{cccc} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, & \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, & \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, & \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, & \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \end{array} \right\}$$

(the dihedral group of order 8), and

$$Q = \left\{ \begin{array}{cccc} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{bmatrix}, & \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, & \begin{bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}, \\ \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, & \begin{bmatrix} -\sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{bmatrix}, & \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, & \begin{bmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{bmatrix} \end{array} \right\}$$

(the quaternionic group of order 8), are not isomorphic to each other.

• Indeed, to prove the statement, it suffices to simply list the orders of the eight elements of each group D, Q .

(1) The list of orders of the elements of D :

$$\begin{array}{cccc} 1, & 4, & 2, & 2, \\ 2, & 4, & 2, & 2 \end{array}$$

(this is in the order the matrices in D are listed in the above).

(2) The list of orders of the elements of Q :

$$\begin{array}{cccc} 1, & 4, & 4, & 4, \\ 2, & 4, & 4, & 4 \end{array}$$

(this is in the order the matrices in Q are listed in the above). If we compare these two tables, clearly D and Q cannot be isomorphic to each other.

• **The subgroup of G generated by two elements of G .**

We have defined the notion of a subgroup of a group G generated by one element $x \in G$. We may generalize this in the following. Let $x, y \in G$. We may consider such elements in G as

$$\begin{aligned} x, y, x^2, y^2, xy, (xy)^2 = xyxy, x^2y, xy^2, x^2y^2, x^{-1}, y^{-1}, \\ x^{-1}y, xy^{-1}, (xy)^{-1} = y^{-1}x^{-1}, x^{-1}yx, y^{-1}xy, xyx^{-1}, yxy^{-1}, \\ xyx^{-1}y^{-1}, xyx^{-1}y^{-1}x, xyx^{-1}y^{-1}xy, x^{-2}, y^{-2}, \dots \end{aligned}$$

Note that many of these may coincide.

Lemma. Let G be a group. For $x, y \in G$, let

$$H = \bigcup_{m=1}^{\infty} \left\{ x^{k_1} y^{\ell_1} x^{k_2} y^{\ell_2} \dots x^{k_m} y^{\ell_m} \in G \mid k_1, \dots, k_m, \ell_1, \dots, \ell_m \in \mathbb{Z} \right\}.$$

This H forms a subgroup of G .

• We may denote the above H by $\langle x, y \rangle$. The proof of Lemma is self-evident. Indeed, the multiplication of two elements in H clearly belongs to H ;

$$\left(x^{k_1} y^{\ell_1} \dots x^{k_m} y^{\ell_m} \right) \left(x^{k_{m+1}} y^{\ell_{m+1}} \dots x^{k_n} y^{\ell_n} \right) = x^{k_1} y^{\ell_1} \dots x^{k_n} y^{\ell_n}.$$

Moreover,

$$\left(x^{k_1} y^{\ell_1} \dots x^{k_m} y^{\ell_m} \right)^{-1} = y^{-\ell_m} x^{-k_m} \dots y^{-\ell_1} x^{-k_1}.$$

- Often the ambient group G coincides with the subgroup $\langle x, y \rangle$; $G = \langle x, y \rangle$.

Then we say that the group G is generated by the two elements x and y .

- Recall that the group G is generated by its single element x ; $G = \langle x \rangle$, if and only if either $G \simeq \mu_m$, or $G \simeq \mathbb{G}_a(\mathbb{Z})$ (the additive group \mathbb{Z}).

- There is no good analog of this statement for groups generated by two elements; $G = \langle x, y \rangle$.

Example 3. We may consider the subgroup S of $G = GL_3(\mathbb{R})$ generated by

$$X = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \text{and} \quad Y = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Since we have the relations

$$X^2 = I, \quad Y^3 = I, \quad XY = Y^2X, \quad XY^2 = YX,$$

(and hence also

$$\begin{aligned} X^{-1} &= X, & Y^{-1} &= Y^2, & (Y^2)^{-1} &= Y, \\ (XY)^{-1} &= Y^2X, & (XY^2)^{-1} &= YX, \end{aligned}$$

it follows that

$$S = \langle X, Y \rangle = \{ I, X, Y, Y^2, XY, XY^2 \} \subseteq GL_3(\mathbb{R}).$$

[I] (1) Describe the subgroup of $GL_4(\mathbb{R})$ generated by

$$X = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \text{and} \quad Y = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

(2) Describe the subgroup of $GL_4(\mathbb{R})$ generated by

$$Z = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad \text{and} \quad W = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

• **Direct products.**

Let G_1 and G_2 be groups. Let

$$G = G_1 \times G_2 = \left\{ (x_1, x_2) \mid x_1 \in G_1, x_2 \in G_2 \right\},$$

We may introduce the group structure into G ; $G \times G \longrightarrow G$, as

$$(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2).$$

Clearly, the identity element of $G = G_1 \times G_2$ is $(1, 1)$, which we denote by 1 . Also clearly,

$$(x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1}).$$

$G = G_1 \times G_2$ clearly forms a group. We call $G = G_1 \times G_2$ the direct product of G_1 and G_2 .

Example 4. Kleinian group of order 4.

Let $G = \{1, a, b, c\}$ be a set, consisting of four elements. Define the group structure of G as follows.

$$\begin{array}{llll} 1 \ 1 = 1, & 1 \ a = a, & 1 \ b = b, & 1 \ c = c, \\ a \ 1 = a, & a \ a = 1, & a \ b = c, & a \ c = b, \\ b \ 1 = b, & b \ a = c, & b \ b = 1, & b \ c = a, \\ c \ 1 = c, & c \ a = b, & c \ b = a, & c \ c = 1. \end{array}$$

Fact. The above G forms an abelian group of order 4. G is isomorphic to $\mu_2 \times \mu_2$.

Proof. Let us denote $\mu_2 = \{1, -1\}$. Hence

$$\mu_2 \times \mu_2 = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\},$$

with the multiplicative structure

$$\begin{aligned} (1, 1)(1, 1) &= (1, 1), & (1, 1)(1, -1) &= (1, -1), \\ (1, 1)(-1, 1) &= (-1, 1), & (1, 1)(-1, -1) &= (-1, -1), \\ (1, -1)(1, 1) &= (1, -1), & (1, -1)(1, -1) &= (1, 1), \\ (1, -1)(-1, 1) &= (-1, -1), & (1, -1)(-1, -1) &= (-1, 1), \\ (-1, 1)(1, 1) &= (-1, 1), & (-1, 1)(1, -1) &= (-1, -1), \\ (-1, 1)(-1, 1) &= (1, 1), & (-1, 1)(-1, -1) &= (1, -1), \\ (-1, -1)(1, 1) &= (-1, -1), & (-1, -1)(1, -1) &= (-1, 1), \\ (-1, -1)(-1, 1) &= (1, -1), & (-1, -1)(-1, -1) &= (1, 1). \end{aligned}$$

Define a bijective mapping $f : \mu_2 \times \mu_2 \longrightarrow G$ as

$$f(1, 1) = 1, \quad f(1, -1) = a, \quad f(-1, 1) = b, \quad f(-1, -1) = c,$$

then clearly f satisfies the property

$$(\text{Hom}) \quad f(\alpha\beta) = f(\alpha)f(\beta) \quad \text{for each } \alpha, \beta \in \mu_2 \times \mu_2. \quad \square$$

Example 5. We may prove

$$\mu_2 \times \mu_2 \not\cong \mu_4.$$

Indeed, the orders of non-identity elements of $\mu_2 \times \mu_2$ are 2, whereas μ_4 has an element of order 4.

- Still, often it happens that

$$\boldsymbol{\mu}_k \times \boldsymbol{\mu}_\ell \simeq \boldsymbol{\mu}_{k\ell}.$$

Example 6. We may prove

$$\boldsymbol{\mu}_2 \times \boldsymbol{\mu}_3 \simeq \boldsymbol{\mu}_6.$$

Indeed, it suffices to show that the product

$$\boldsymbol{\mu}_2 \times \boldsymbol{\mu}_3 = \left\{ \begin{array}{l} (1, 1), \quad (1, \zeta_3), \quad (1, \zeta_3^2), \\ (-1, 1), \quad (-1, \zeta_3), \quad (-1, \zeta_3^2) \end{array} \right\}$$

has an element of order 6. Indeed, $x = (-1, \zeta_3)$ has order 6. Indeed,

$$x = (-1, \zeta_3) \neq (1, 1), \quad x^2 = (1, \zeta_3^2) \neq (1, 1),$$

$$x^3 = (-1, 1) \neq (1, 1), \quad x^4 = (1, \zeta_3) \neq (1, 1),$$

$$x^5 = (-1, \zeta_3^2) \neq (1, 1), \quad \text{and}$$

$$x^6 = (1, 1).$$

- To generalize Example 6, we may show the following.

Fact. Let k and ℓ be two integers, $k > 1$, $\ell > 1$. Assume that k and ℓ are co-prime. In other words, the only integer $m > 0$ that divides both k and ℓ is $m = 1$. Then

$$\boldsymbol{\mu}_k \times \boldsymbol{\mu}_\ell \simeq \boldsymbol{\mu}_{k\ell}.$$