

Math 830 ABSTRACT ALGEBRA

PROGRESS CHECK – VI

September 11 (Mon), 2006

Instructor: Yasuyuki Kachi

Line #: 17014.

• **Additive groups and their subgroups.**

Let G be an additive group. Recall that the binary operation of G is written additively, that is, the binary operation defined on G takes a pair of elements (x, y) of G into $x + y$. Recall that we denote its identity element by 0 . Recall also that we denote the inverse element of $x \in G$ as $-x$.

Definition. (Additive subgroups).

Let G be an additive group. Let H be a nonempty subset of G ; $H \subseteq G$. H is said to be an (additive) subgroup of G , if it satisfies the two conditions:

(SG1) $x + y \in H$ whenever $x \in H$ and $y \in H$,

(SG2) $-x \in H$ whenever $x \in H$.

• **Properties of additive subgroups.**

Let G be an additive group, and H its additive subgroup. Then the following (1–3) hold:

(1) $0 \in H$.

(2) H itself forms an additive group with the same identity element 0 .

(3) Let K be an additive subgroup of H . Then K is an additive subgroup of G .

• In view of (3) above, if $G \supseteq H \supseteq K$ if H is a subgroup of G , and if K is a subgroup of H , then we call $G \supseteq H \supseteq K$ a chain of additive subgroups.

Example 1. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ is a chain of additive subgroups.

Example 2. $\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq 8\mathbb{Z} \supseteq 16\mathbb{Z} \supseteq \dots \supseteq 2^m\mathbb{Z} \supseteq \dots$

is a chain of additive subgroups. Similarly,

$$\mathbb{Z} \subseteq \frac{1}{2}\mathbb{Z} \subseteq \frac{1}{4}\mathbb{Z} \subseteq \frac{1}{8}\mathbb{Z} \subseteq \frac{1}{16}\mathbb{Z} \subseteq \dots \subseteq \frac{1}{2^m}\mathbb{Z} \subseteq \dots$$

is an (increasing) chain of additive subgroups.

Example 3. Recall that, for an arbitrary $m \in \mathbb{Z}$; $m > 0$,

$$\mathbb{R}^m = \left\{ (x_1, \dots, x_m) \mid x_1, \dots, x_m \in \mathbb{R} \right\}$$

forms an additive group, under the addition rule:

$$(x_1, \dots, x_m) + (y_1, \dots, y_m) = (x_1 + y_1, \dots, x_m + y_m).$$

We may identify \mathbb{R}^m as a subset of \mathbb{R}^{m+1} consisting of vectors

$$(x_1, \dots, x_m, 0), \quad x_1, \dots, x_m \in \mathbb{R}.$$

Then

$$\mathbb{R} \subseteq \mathbb{R}^2 \subseteq \mathbb{R}^3 \subseteq \dots \subseteq \mathbb{R}^m \subseteq \mathbb{R}^{m+1} \subseteq \dots$$

is an (increasing) chain of additive subgroups.

Example 4. Lattices. Let

$$H = \left\{ (m, n) \in \mathbb{R}^2 \mid m \in \mathbb{Z}, n \in \mathbb{Z} \right\} \subseteq \mathbb{R}^2.$$

This H forms an additive subgroup of \mathbb{R}^2 . We denote it by \mathbb{Z}^2 .

• In a similar vein, let

$$v_1 = (a_1, b_1) \in \mathbb{R}^2 \quad \text{and} \quad v_2 = (a_2, b_2) \in \mathbb{R}^2$$

be linearly independent vectors over \mathbb{R} . Then

$$\begin{aligned}
H &= \left\{ m v_1 + n v_2 \in \mathbb{R}^2 \mid m \in \mathbb{Z}, n \in \mathbb{Z} \right\} \\
&= \left\{ \left(m a_1 + n a_2, m b_1 + n b_2 \right) \in \mathbb{R}^2 \mid m \in \mathbb{Z}, n \in \mathbb{Z} \right\} \subseteq \mathbb{R}^2
\end{aligned}$$

forms an additive subgroups of G , which is isomorphic to \mathbb{Z}^2 as an additive group.

[I] Let

$$L = \left\{ \begin{bmatrix} m \\ n \end{bmatrix} \mid m \in \mathbb{Z}, n \in \mathbb{Z} \right\}.$$

This L forms an additive group under the usual addition:

$$\begin{bmatrix} m_1 \\ n_1 \end{bmatrix} + \begin{bmatrix} m_2 \\ n_2 \end{bmatrix} = \begin{bmatrix} m_1 + m_2 \\ n_1 + n_2 \end{bmatrix}.$$

$L \simeq \mathbb{Z}^2$. Consider $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$. Then the following two conditions are equivalent:

- (a) For $m, n \in \mathbb{R}$, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix} \in L$ if and only if $\begin{bmatrix} m \\ n \end{bmatrix} \in L$.
- (b) $a \in \mathbb{Z}, b \in \mathbb{Z}, c \in \mathbb{Z}, d \in \mathbb{Z}$, and $ad - bc \in \{1, -1\}$.

Definition. In view of [I] above, we define

$$GL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc \in \{1, -1\} \right\}.$$

Note $GL_2(\mathbb{Z}) \subseteq GL_2(\mathbb{R})$.

[II] Prove that $GL_2(\mathbb{Z})$ is a subgroup of $GL_2(\mathbb{R})$.

- **Representation of the additive groups \mathbb{R} , \mathbb{Q} , \mathbb{Z} .**

Let us consider

$$\mathbb{G}_a(\mathbb{R}) = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R}) \mid b \in \mathbb{R} \right\}.$$

Theorem 1. $\mathbb{G}_a(\mathbb{R})$ as a multiplicative group is isomorphic to \mathbb{R} as an additive group.

To see this, it suffices to observe

$$(*) \quad \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b' \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b + b' \\ 0 & 1 \end{bmatrix}.$$

[III] Use the formula (*) to prove

$$\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}^m = \begin{bmatrix} 1 & mb \\ 0 & 1 \end{bmatrix} \quad (m \in \mathbb{Z}).$$

- $\mathbb{G}_a(\mathbb{R})$ provides another representation of the additive group \mathbb{R} . The representation of \mathbb{R} which we already know is the one through

$$\exp : \mathbb{R} \longrightarrow \mathbb{R}^*, \quad \exp x = e^x.$$

Recall that the image of this mapping is

$$(\mathbb{R}^*)_+ = \{x \in \mathbb{R}^* \mid x > 0\}.$$

The disadvantage of this representation is that the image of \mathbb{Q} under the same mapping is not in \mathbb{Q}^* . Indeed, $e = \exp 1$ is an irrational number.

- We may be tempted to consider such alternative as

$$f : \mathbb{Q} \longrightarrow \mathbb{R}^*, \quad f(r) = 2^r.$$

However, the image is still not in \mathbb{Q}^* . Indeed, $2^{1/2}$ is an irrational number.

Definition. We define

$$\mathbb{G}_a(\mathbb{Q}) = \left\{ \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{Q}) \mid r \in \mathbb{Q} \right\},$$

$$\mathbb{G}_a(\mathbb{Z}) = \left\{ \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{Z}) \mid m \in \mathbb{Z} \right\}.$$

Theorem 2.

- (1) $\mathbb{G}_a(\mathbb{Q})$ as a multiplicative group is isomorphic to \mathbb{Q} as an additive group.
- (2) $\mathbb{G}_a(\mathbb{Z})$ as a multiplicative group is isomorphic to \mathbb{Z} as an additive group.

Theorem 2 follows immediately from (*) in the previous page.

[IV] Define $\mathbb{G}_a(\mathbb{C})$ as a subgroup of $GL_2(\mathbb{C})$.

• **Order of elements. The cyclic subgroup generated by an element.**

Let G be an arbitrary group. Let $x \in G$. Consider the sequence

$$x^0 = 1, \quad x^1 = x, \quad x^2, \quad x^3, \quad x^4, \quad \dots \quad x^m, \quad \dots .$$

These are all elements of G . Sometimes $x^m = 1$ for some $m \in \mathbb{Z}; m > 0$. Sometimes x^m is never equal to 1 for any $m \in \mathbb{Z}; m > 0$.

Definition. For $x \in G$, the smallest $m \in \mathbb{Z}; m > 0$ such that $x^m = 1$ is called the order of the element $x \in G$. Write it $m = \text{ord } x$. If there does not exist $m \in \mathbb{Z}, m > 0$, such that $x^m = 1$, then we say that the order of the element $x \in G$ is infinity. Write $\text{ord } x = \infty$.

- Note that $\text{ord } x = 1$ if and only if $x = 1$.

Example. Let $G = GL_2(\mathbb{R})$.

$$\begin{aligned} \text{ord} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} &= 1. & \text{ord} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} &= \infty. & \text{ord} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} &= 4. \\ \text{ord} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} &= 2. & \text{ord} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} &= \infty. & \text{ord} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} &= 2. \\ \text{ord} \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} &= 8. & \text{ord} \begin{bmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{bmatrix} &= 6. \end{aligned}$$

• **Remark.** In general $\text{ord}(AB)$ is not determined solely from $\text{ord}(A)$ and $\text{ord}(B)$.

Example. $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$. Then $AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

We have $\text{ord}(A) = 4$, $\text{ord}(B) = 6$, and $\text{ord}(AB) = \infty$.

Formula.

(1) Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$. If $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc \notin \{1, -1\}$, then

$$\text{ord} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \infty.$$

(2) Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{C})$. If $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc \notin U$, then

$$\text{ord} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \infty.$$

• The proof of the above Formula relies essentially upon the fact that the determinant

$$\det : GL_2(\mathbb{R}) \longrightarrow \mathbb{R}^*, \quad \det : GL_2(\mathbb{C}) \longrightarrow \mathbb{C}^*,$$

satisfy

$$(\text{Hom}) \quad \det(AB) = (\det A)(\det B).$$

- The converse of the above Formula (1), (2) is not true.

Formula 2. Let $A = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$, where $\theta \in \mathbb{R}$. Then

$$\text{ord}(A) \neq \infty \quad \text{if and only if} \quad \theta \in \pi\mathbb{Q}.$$

Theorem 3. Let G be a finite group. Then an arbitrary element of G has a finite order.

Definition. Let G be a group, and $x \in G$. Define

$$H = \{x^k \in G \mid k \in \mathbb{Z}\} \subseteq G.$$

Theorem. In the above Definition, H forms a subgroup of G . Let $m = \text{ord } x$.

(1) If $m \neq \infty$, then

$$H = \{1, x, x^2, \dots, x^{m-1}\},$$

and $x^m = 1$. In particular, $H \simeq \mu_m$.

(2) If $m = \infty$, then

$$H = \{1, x, x^{-1}, x^2, x^{-2}, \dots, x^m, x^{-m}, \dots\},$$

where $x^k \neq x^\ell$ whenever $k \neq \ell$. In particular, $H \simeq \mathbb{G}_a(\mathbb{Z})$ (the additive group \mathbb{Z}).

[V] Give a concrete example of an infinite group G whose arbitrary element has finite order.