

## Math 830 ABSTRACT ALGEBRA

### PROGRESS CHECK – V

September 8 (Fri), 2006

**Instructor:** Yasuyuki Kachi

**Line #:** 17014.

- **Additive Groups.**

Let  $G$  be an abelian group. Often it is more convenient to denote its binary operation in an additive fashion. That is, instead of writing  $xy$  in juxtaposition, write  $x + y$  for the result of applying the binary operation for two elements  $x$  and  $y \in G$ . We also use the notation  $0$ , instead of  $1$ , for the identity element of  $G$ .

- Thus, we arrive at the definition of additive groups, as follows.

An additive group  $G$  is a set  $G$ , with a distinguished element  $0 \in G$ , endowed with a binary operation  $G \times G \longrightarrow G$ , which takes a pair  $(x, y) \in G \times G$  into an element  $x + y \in G$ , satisfying the following axioms (AG0–3):

$$(AG0) \quad x + y = y + x,$$

$$(AG1) \quad x + (y + z) = (x + y) + z,$$

$$(AG2) \quad 0 + x = x,$$

$$(AG3) \quad x + (-x) = 0 \quad \text{for a suitable } -x \in G.$$

**Example 1.** The most elementary but the most important example of an additive group is the additive group of integers;  $G = \mathbb{Z}$ . The usual additive structure on  $\mathbb{Z}$  makes  $\mathbb{Z}$  into an additive group.

**Example 2.** The usual additive structure on the set of rational numbers  $\mathbb{Q}$  makes  $\mathbb{Q}$  into an additive group.

**Example 3.** The usual additive structure on the set of real numbers  $\mathbb{R}$  makes  $\mathbb{R}$  into an additive group.

**Example 4.** The usual additive structure on the set of complex numbers  $\mathbb{C}$  makes  $\mathbb{C}$  into an additive group.

**Example 5.** The usual additive structure on the set of quaternionic numbers  $\mathbb{H}$  makes  $\mathbb{H}$  into an additive group. Recall that  $\mathbb{H}$  is defined as the following set of matrices:

$$\mathbb{H} = \left\{ \begin{bmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{bmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}.$$

Alternatively,

$$\mathbb{H} = \left\{ aI + bX + cY + dZ \mid a, b, c, d \in \mathbb{R} \right\},$$

where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{bmatrix},$$
$$Y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}.$$

• Note that,  $\mathbb{Q}$  as an additive group is different from  $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$  as a multiplicative group. Similarly,  $\mathbb{R}$ ,  $\mathbb{C}$ , and  $\mathbb{H}$  as additive groups are different from  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ ,  $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ , and  $\mathbb{H}^* = \mathbb{H} \setminus \{0\}$ , as multiplicative groups, respectively. However, see page 6– (Representation of additive groups).

**Example 6.** The usual additive structure on the set of vectors in  $\mathbb{R}^2$  makes  $\mathbb{R}^2$  into an additive group:

$$(a, b) + (c, d) = (a + c, b + d) \quad \left( a, b, c, d \in \mathbb{R} \right).$$

**Example 7.** More generally, the usual additive structure on the set of vectors in  $\mathbb{R}^n$  makes  $\mathbb{R}^n$  into an additive group.

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n) \\ \left( a_i, b_i \in \mathbb{R} \right).$$

- Recall that the additive structure of  $\mathbb{C}$  is defined as

$$\left( a + \sqrt{-1}b \right) + \left( c + \sqrt{-1}d \right) = \left( a + c \right) + \sqrt{-1} \left( b + d \right),$$

for  $a, b, c, d \in \mathbb{R}$ . From the group structure point of view, this addition rule is “essentially the same” as the addition rule of vectors in  $\mathbb{R}^2$  :

$$(a, b) + (c, d) = (a + c, b + d).$$

- We may more precisely rephrase the above observation, as follows.

**Fact.** The two additive groups  $\mathbb{C}$  and  $\mathbb{R}^2$  are isomorphic to each other :

$$\mathbb{C} \simeq \mathbb{R}^2.$$

*Proof.* Indeed, define the mapping  $f : \mathbb{C} \longrightarrow \mathbb{R}^2$  as

$$f \left( a + \sqrt{-1}b \right) = (a, b) \quad \left( a, b \in \mathbb{R} \right).$$

Clearly  $f$  is bijjective . Moreover, for two elements  $\alpha, \beta \in \mathbb{C}$ ,

$$f(\alpha + \beta) = f(\alpha) + f(\beta).$$

Indeed, if we write  $\alpha = a + \sqrt{-1}b$ ,  $\beta = c + \sqrt{-1}d$ , where  $a, b, c, d \in \mathbb{R}$ ,

then

$$\begin{aligned} f(\alpha + \beta) &= f\left((a + c) + \sqrt{-1}(b + d)\right) \\ &= (a + c, b + d) \\ &= (a, b) + (c, d) \\ &= f(\alpha) + f(\beta). \quad \square \end{aligned}$$

• Similarly, we have the following:

**Fact.** The three additive groups  $\mathbb{H}$ ,  $\mathbb{C}^2$ , and  $\mathbb{R}^4$  are isomorphic to each other :

$$\mathbb{H} \simeq \mathbb{C}^2 \simeq \mathbb{R}^4.$$

**Fact.** Let  $M_{m,n}(\mathbb{R})$  denote the set of matrices with entries in  $\mathbb{R}$  of size  $m$  by  $n$ :

$$M_{m,n}(\mathbb{R}) = \left\{ \left[ \begin{array}{ccc} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{array} \right] \mid a_{ij} \in \mathbb{R} \right\}.$$

We introduce the usual additive structure on the set  $M_{m,n}(\mathbb{R})$ :

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} + \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{bmatrix} = \begin{bmatrix} a_{11} + b_{11} & \cdots & a_{1n} + b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & \cdots & a_{mn} + b_{mn} \end{bmatrix}.$$

Then  $M_{m,n}(\mathbb{R})$  is an additive group.  $M_{m,n}(\mathbb{R})$  is isomorphic to  $\mathbb{R}^{mn}$ :

$$M_{m,n}(\mathbb{R}) \simeq \mathbb{R}^{mn}.$$

• **Cyclic groups as additive groups.**

Let us consider the congruence  $\equiv_3$  in  $\mathbb{Z}$ . Namely,  $\equiv_3$  is an equivalence relation on the set  $\mathbb{Z}$ , defined as follows:

$$x \equiv_3 y \iff x - y \in 3\mathbb{Z}.$$

Then there are exactly three equivalence classes:

$$\begin{aligned} [0]_3 &= \{ 3x \mid x \in \mathbb{Z} \} = 3\mathbb{Z}, \\ [1]_3 &= \{ 1 + 3x \mid x \in \mathbb{Z} \} = 1 + 3\mathbb{Z}, \quad \text{and} \\ [2]_3 &= \{ 2 + 3x \mid x \in \mathbb{Z} \} = 2 + 3\mathbb{Z}. \end{aligned}$$

We may define the additive structure on the quotient set

$$\left( \mathbb{Z} / \equiv_3 \right) = \left\{ [0]_3, [1]_3, [2]_3 \right\}$$

as

$$\begin{aligned} [0]_3 + [0]_3 &= [0]_3, & [0]_3 + [1]_3 &= [1]_3, & [0]_3 + [2]_3 &= [2]_3, \\ [1]_3 + [1]_3 &= [2]_3, & [1]_3 + [2]_3 &= [0]_3, \\ [2]_3 + [2]_3 &= [1]_3. \end{aligned}$$

**Fact.** The set  $\mathbb{Z} / \equiv_3$  forms an additive group. We denote the group by  $\mathbb{Z} / 3\mathbb{Z}$ .

• More generally, let  $m \in \mathbb{Z}$ ,  $m > 1$ , be arbitrary. Let us consider the congruence  $\equiv_m$  in  $\mathbb{Z}$ . Namely,  $\equiv_m$  is an equivalence relation on the set  $\mathbb{Z}$ , defined as follows:

$$x \equiv_m y \iff x - y \in m\mathbb{Z}.$$

Then there are exactly  $m$  equivalence classes:

$$[k]_m = \left\{ k + mx \mid x \in \mathbb{Z} \right\} = k + m\mathbb{Z},$$

for  $k = 0, 1, \dots, m-1$ .

We may define the additive structure on the quotient set

$$\left( \mathbb{Z} / \equiv_m \right) = \left\{ [0]_m, [1]_m, \dots, [m-1]_m \right\}$$

as

$$[k]_m + [\ell]_m = [k + \ell]_m.$$

Note that, depending upon the values  $k$  and  $\ell$ , the sum  $k + \ell$  may be greater than  $m - 1$ . Then, by the definition of the congruence classes,  $[k + \ell]_m$  is understood as  $[k + \ell - m]_m$ .

**Fact.** The set  $\mathbb{Z}/\equiv_m$  forms an additive group. We denote the group by  $\mathbb{Z}/m\mathbb{Z}$ .

- **Representations of additive groups  $\mathbb{R}$  and  $\mathbb{Q}$ .**

Recall that, for two real numbers  $x$  and  $y \in \mathbb{R}$ , we have the exponential law :

$$\exp(x + y) = (\exp x)(\exp y),$$

or,

$$e^{x+y} = e^x e^y.$$

Thus, the function  $\exp$  translates the additive structure on  $\mathbb{R}$  to the multiplicative structure on  $\mathbb{R}$ . Since

$$f = \exp : \mathbb{R} \longrightarrow (\mathbb{R}^*)_+, \quad f(x) = \exp x = e^x,$$

is a bijection, where  $(\mathbb{R}^*)_+ = \{x \in \mathbb{R} \mid x > 0\}$ , we may contend that  $f$  is a realization of the additive group  $\mathbb{R}$  as a subgroup  $(\mathbb{R}^*)_+$  of the multiplicative group  $\mathbb{R}^*$ .

- The group  $(\mathbb{R}^*)_+$  contains a subgroup

$$G = \left\{ \exp x \in (\mathbb{R}^*)_+ \mid x \in \mathbb{Q} \right\} \subseteq (\mathbb{R}^*)_+.$$

We may contend that the additive group  $\mathbb{Q}$  is realized as this subgroup  $G$  of the multiplicative group  $\mathbb{R}^*$ .

- The above are called the (1-dimensional) representations of the additive groups  $\mathbb{R}$  and  $\mathbb{Q}$ .

- **The additive group  $\mathbb{R}/\mathbb{Z}$ .**

Let us consider the congruence  $\equiv_{\mathbb{Z}}$  in  $\mathbb{R}$ . Namely,  $\equiv_{\mathbb{Z}}$  is an equivalence relation on the set  $\mathbb{R}$ , defined as follows:

$$x \equiv_{\mathbb{Z}} y \iff x - y \in \mathbb{Z}.$$

Then the equivalence classes are of form:

$$[x]_{\mathbb{Z}} = \left\{ x + m \mid m \in \mathbb{Z} \right\} = x + \mathbb{Z},$$

for  $x \in [0, 1) = \left\{ x \in \mathbb{R} \mid 0 \leq x < 1 \right\}$ .

We may define the additive structure on the quotient set

$$\left( \mathbb{R} / \equiv_{\mathbb{Z}} \right) = \left\{ [x]_{\mathbb{Z}} \mid x \in [0, 1) \right\}$$

as

$$[x]_{\mathbb{Z}} + [y]_{\mathbb{Z}} = [x + y]_{\mathbb{Z}}.$$

Note that, depending upon the values  $x$  and  $y$ , the sum  $x + y$  may be greater than or equal to 1. Then, by the definition of the congruence classes,  $[x + y]_{\mathbb{Z}}$  is understood as  $[x + y - 1]_{\mathbb{Z}}$ .

**Fact.** The set  $\mathbb{R} / \equiv_{\mathbb{Z}}$  forms an additive group. We denote the group by  $\mathbb{R} / \mathbb{Z}$ .

- **Representations of the additive groups  $\mathbb{Z}/m\mathbb{Z}$  and  $\mathbb{R}/\mathbb{Z}$ .**

Let us recall that

$$U = \left\{ z \in \mathbb{C}^* \mid |z| = 1 \right\},$$

and

$$\boldsymbol{\mu}_m = \left\{ z \in \mathbb{C}^* \mid z^m = 1 \right\} = \left\{ 1, \zeta_m, \dots, \zeta_m^{m-1} \right\}$$

both form subgroups of the multiplicative groups  $\mathbb{C}^*$ . We contend that the additive group counterpart of  $U$  and  $\boldsymbol{\mu}_m$  are  $\mathbb{R}/\mathbb{Z}$  and  $\mathbb{Z}/m\mathbb{Z}$ , respectively. More precisely, we have the following:

**Fact.** (1) The mapping

$$f : \mathbb{R}/\mathbb{Z} \longrightarrow U, \quad f\left([x]_{\mathbb{Z}}\right) = \exp\left(2\pi x \sqrt{-1}\right)$$

is a well-defined bijection. Moreover,

$$f\left([x]_{\mathbb{Z}} + [y]_{\mathbb{Z}}\right) = f\left([x]_{\mathbb{Z}}\right) f\left([y]_{\mathbb{Z}}\right).$$

(2) The mapping

$$f : \mathbb{Z}/m\mathbb{Z} \longrightarrow \boldsymbol{\mu}_m, \quad f\left([k]_m\right) = \exp\left(\frac{2\pi k \sqrt{-1}}{m}\right)$$

is a well-defined bijection. Moreover,

$$f\left([k]_m + [\ell]_m\right) = f\left([k]_m\right) f\left([\ell]_m\right).$$

• **Summary.**

- (1)  $\mathbb{R}$  (the additive group)  $\simeq (\mathbb{R}^*)_+$  (the multiplicative group).
- (2)  $\mathbb{Q}$  (the additive group)  $\simeq \left\{ \exp x \mid x \in \mathbb{Q} \right\}$  (the multiplicative group).
- (3)  $\mathbb{R}/\mathbb{Z}$  (the additive group)  $\simeq U$  (the multiplicative group).
- (4)  $\mathbb{Z}/m\mathbb{Z}$  (the additive group)  $\simeq \boldsymbol{\mu}_m$  (the multiplicative group).