Math 830 ABSTRACT ALGEBRA
QUIZ – III

August 23 (Wed), 2006

Instructor: Yasuyuki Kachi

Line #: 17014.

ID : ____________________ Name : ______________________________

- **Check List.**

☐ A group is a set G, with a distinguished element $1 \in G$, admitting a binary operation $G \times G \longrightarrow G$ taking (x, y) into xy, such that

(G1) $x\,(yz) = (xy)\,z$ holds in G,

(G2) $1\,x = x = x\,1$ holds in G,

(G3) $x\,x^{-1} = 1 = x^{-1}\,x$ holds in G for a suitable $x^{-1} \in G$.

☐ In the above, $1 \in G$ is called the identity of the group G.

☐ An abelian group is a group G such that

(GA) $xy = yx$ holds in G.

☐ The set $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ of non-zero complex numbers forms an abelian group.

☐ The set $U = \left\{ z \in \mathbb{C}^* \;\middle|\; |z| = 1 \right\}$ of complex numbers having absolute value 1 forms an abelian group.

☐ The set $\boldsymbol{\mu}_2 = \left\{ 1, -1 \right\}$ forms an abelian group.

☐ The set $\boldsymbol{\mu}_3 = \left\{ 1, \zeta_3, \zeta_3^2 \right\}$ forms an abelian group.

☐ The set $\boldsymbol{\mu}_4 = \left\{ 1, \zeta_4, \zeta_4^2, \zeta_4^3 \right\}$ forms an abelian group.

☐ The set $\boldsymbol{\mu}_6 = \left\{1,\ \zeta_6,\ \zeta_6^2,\ \zeta_6^3,\ \zeta_6^4,\ \zeta_6^5\right\}$ forms an abelian group.

☐ The set $\boldsymbol{\mu}_8 = \left\{1,\ \zeta_8,\ \zeta_8^2,\ \zeta_8^3,\ \zeta_8^4,\ \zeta_8^5,\ \zeta_8^6,\ \zeta_8^7\right\}$ forms an abelian group.

☐ More generally, the set $\boldsymbol{\mu}_m = \left\{1,\ \zeta_m,\ \zeta_m^2,\ \zeta_m^3,\ \cdots,\ \zeta_m^{m-1}\right\}$ forms an abelian group $\left(m > 1\right)$.

☐ A <u>subgroup</u> of a group G is a non-empty subset $H \subseteq G$, such that

(SG1) $xy \in H$, whenever $x,\ y \in H$,

(SG2) $x^{-1} \in H$, whenever $x \in H$.

☐ A subgroup H of a group G always contains the identity 1 of G. H forms a group by itself. The identity of H is the same as the identity 1 of G.

☐ $U \subseteq \mathbb{C}^*$. U is a subgroup of $\mathbb{C}^*$.

☐ $\boldsymbol{\mu}_m \subseteq U$. Indeed, $\left|\zeta_m^i\right| = 1 \quad \left(i \in \mathbb{Z}\right)$. $\boldsymbol{\mu}_m$ is a subgroup of U.

☐ $\boldsymbol{\mu}_m$ is a subgroup of $\mathbb{C}^*$.

☐ More generally, suppose $G \supseteq H \supseteq K$, where G is a group, H is a subgroup of G, and K is a subgroup of H. Then K is a subgroup of G.

☐ Let G be a group, and H its subgroup; $G \supseteq H$. If G is abelian, then H is abelian.

☐ The converse is not true: Let H be an abelian group. Let G be a group which contains H as its subgroup; $G \supseteq H$. Then G is not necessarily abelian.

☐ The following offers an example of a <u>non-abelian</u> group G which contains $H = \mathbb{C}^*$ as its subgroup. Let G be defined as

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a,\, b,\, c,\, d \in \mathbb{R},\ ad - bc \neq 0 \right\}.$$

Then G forms a group, with respect to the usual multiplication;

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{bmatrix}.$$

Indeed, G satisfies (G1–3), where $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{1}$ serves as the identity, and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

☐ Meanwhile, the above G is <u>non-abelian</u>. Indeed, one has

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

which shows that G does not satisfy (GA). Write $G = GL_2(\mathbb{R})$.

☐ Let $G = GL_2(\mathbb{R})$ be as above. Let H be defined as

$$H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \;\middle|\; a = d,\ b + c = 0 \right\}.$$

H forms a subgroup of G. Indeed, H satisfies (SG1–2).

☐ The above H is abelian.

☐ More precisely, <u>the group structure</u> of the multiplicative group $\mathbb{C}^*$ and <u>the group structure</u> of the above H are <u>identical</u>, in the following sense. For $a + \sqrt{-1}\,b \in \mathbb{C}^*$ where $a,\, b \in \mathbb{R}$, we set $\varphi\big(a + \sqrt{-1}\,b\big) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

□ Clearly $\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in H$. Hence φ gives rise to a mapping

$$\varphi : \mathbb{C}^* \longrightarrow H; \qquad \varphi\Big(a + \sqrt{-1}\,b\Big) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

It follows that φ has an inverse;

$$\varphi^{-1} : H \longrightarrow \mathbb{C}^*; \qquad \varphi^{-1}\left(\begin{bmatrix} p & q \\ r & s \end{bmatrix} \right) = p + \sqrt{-1}\,r.$$

Hence φ is a <u>bijective</u> mapping between $\mathbb{C}^*$ and H.

□ For two $\alpha, \beta \in \mathbb{C}^*$,

$$\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$$

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

$$\alpha\,\beta = \big(ac - bd\big) + \sqrt{-1}\,\big(ad + bc\big),$$

thus

$$\varphi(\alpha\,\beta) = \begin{bmatrix} ac - bd & -\big(ad + bc\big) \\ ad + bc & ac - bd \end{bmatrix},$$

whereas

$$\varphi(\alpha)\,\varphi(\beta) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac - bd & -\big(ad + bc\big) \\ ad + bc & ac - bd \end{bmatrix}.$$

□ In general, suppose G_1 and G_2 are two groups, and suppose there is a <u>bijective</u> mapping $\varphi : G_1 \longrightarrow G_2$ such that

$$\varphi(xy) = \varphi(x)\varphi(y) \qquad (x, y \in G)$$

holds. Then we say that the <u>two groups G_1 and G_2 are isomorphic to each other</u>.