§3.3 # 3, 10

(3) If $H = \langle (12) \rangle$ and $K = \langle (13) \rangle$ then

$$HK = \{ (1), (12), (13), (132) \}$$

which is not a subgroup by Lagrange's Theorem, since $4 \nmid 6$.

(10) Let $n \in \mathbb{Z}$, $n > 2$. Then $H = \{ (\sigma, \tau) \in S_n \times S_n \mid \sigma(1) = \tau(1) \}$ is not a subgroup.

Proof: Closure under products fails. If $(\sigma, \tau) \in H$ and $(\sigma_1, \tau_1) \in H$ then $\sigma(1) = \tau(1)$ and $\sigma_1(1) = \tau_1(1)$. Then $(\sigma, \tau)(\sigma_1, \tau_1) = (\sigma\sigma_1, \tau\tau_1) \in H$ iff $\sigma\sigma_1(1) = \tau\tau_1(1)$. We know $\sigma_1(1) = \tau_1(1) = k$ for some k, but then we need $\sigma(k) = \tau(k)$ and this may fail. Example with $n > 2$: $((12), (123)) \in H$ since both send 1 to 2. Similarly $((12), (12)) \in H$. But $((12), (123))((12), (12)) = ((1), (13))$ and (1) sends 1 to 1 but (13) sends it to 3, so this product is not in H. //

Question: what if $n = 1$ or 2?

§3.4

(1) Show $\mathbb{Z}_{10}^\times \cong \mathbb{Z}_4$

Pf: $\mathbb{Z}_{10}^\times = \{a \in \mathbb{Z}_{10} \mid (a,10)=1\} = \{1,3,7,9\}$ since $3^2=9$, $3^3=7$, $3^4=1$ we may define an isomorphism by $\phi([n]_4) = [3^n]_{10}$. //

(5) Is $(\mathbb{C},+)$ isomorphic to $(\mathbb{C}^\times,*)$?

No: $(-1)^2=1$ so $o(-1)=2$ in $\mathbb{C}^\times$. But in $(\mathbb{C},+)$ if $\alpha \neq 0$ then $n\alpha \neq 0$ for all $n \neq 0$, so $o(\alpha)=\infty$. //

(6) Show $G_1 \times G_2 \cong G_2 \times G_1$

Pf: $\phi: G_1 \times G_2 \longrightarrow G_2 \times G_1$ by $\phi(g_1,g_2) = (g_2,g_1)$ is an isomorphism. //

(10) $\mathrm{Aff}(\mathbb{R}) \cong \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \,\middle|\, m \in \mathbb{R}^\times, b \in \mathbb{R} \right\}$ with matrix multiplication

Pf: Let $\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$. Then

$$\phi(f_{m,b} f_{n,c}) = \phi(f_{mn,\, mc+b}) = \begin{bmatrix} mn & mc+b \\ 0 & 1 \end{bmatrix} \quad \text{and}$$

$$\phi(f_{m,b})\phi(f_{n,c}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} n & c \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} mn & mc+b \\ 0 & 1 \end{bmatrix} \quad \text{so } \phi \text{ is a homomorphism}$$

Obviously, ϕ is 1-1 and onto. //

(13) Show $\mathbb{R}^\times \cong C_2 \times \mathbb{R}^+$

Pf: Let $\phi(r) = (\mathrm{sign}(r), \ln|r|)$ where $\mathrm{sign}(r) = r/|r|$. Then

$$\phi(r_1 r_2) = (\mathrm{sign}(r_1 r_2), \ln|r_1 r_2|) = (\mathrm{sign}(r_1)\mathrm{sign}(r_2), \ln|r_1| + \ln|r_2|)$$

$$= \phi(r_1)\phi(r_2), \quad \text{so } \phi \text{ is a homomorphism.}$$

Since $\phi^{-1}(\varepsilon, a) = \varepsilon e^a$, ϕ is 1-1 and onto. //

(15) For $a \in G$, let $\phi_a: G \to G$ by $\phi_a(x) = axa^{-1}$. Show ϕ is an isomorphism.

Pf: $\phi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \phi(x)\phi(y)$ so ϕ is a homomorphism.

$\phi_{a^{-1}}\phi_a = 1 = \phi_a\phi_{a^{-1}}$ since $a^{-1}axa^{-1}(a^{-1})^{-1} = x$, so ϕ is 1-1 and onto. //

(16) Let G be a group and $\phi: G \to G$ be $\phi(x) = x^{-1}$. Show

(a) ϕ is 1-1 and onto, and

(b) ϕ is an isomorphism iff G is abelian.

Pf: (a) $\phi(\phi(x)) = (x^{-1})^{-1} = x$ so $\phi\phi = 1$, so ϕ is 1-1 and onto.

(b) ϕ is an isomorphism iff it is a homomorphism, by (a). Now $\phi(xy) = (xy)^{-1} = y^{-1}x^{-1}$ and $\phi(x)\phi(y) = x^{-1}y^{-1}$ so ϕ is an

16 (cont.)
isomorphism iff $x^{-1}y^{-1} = y^{-1}x^{-1}$ for all $x, y \in G$. ~~Next~~ If $a, b \in G$ let $x = a^{-1}$ and $y = b^{-1}$. We see that $ab = ba$ for all $a, b \in G$. //

17 Let $\phi : G_1 \to G_2$ be any group homomorphism, H a subgroup of G_1. Then $\phi(H)$ is a subgroup of G_2.
Pf: We must show $\phi(H)$ is closed under products and inverses. Suppose $a, b \in \phi(H)$. Then $a = \phi(x)$, $b = \phi(y)$ for some $x, y \in H$. Then $ab = \phi(x)\phi(y) = \phi(xy)$ so $ab \in \phi(H)$. Similarly $a^{-1} = \phi(x^{-1})$ so $a^{-1} \in \phi(H)$. Note that we are using $xy \in H$ and $x^{-1} \in H$ since H is a subgroup of G_1. //

19 Show that $\mathbb{C}^\times$ is isomorphic to the subgroup of $Gl_2(\mathbb{R})$ consisting of all matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $a^2 + b^2 \neq 0$.
Proof: We define an isomorphism $\phi(a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. This is clearly one-to-one and onto, so it suffices to show it is a homomorphism:

$$\phi \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \phi \begin{bmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{bmatrix}$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$= \phi(a + ib)\, \phi(c + id) \overset{?}{=} \phi(ac - bd + i(ad + bc)) \quad //$$

20 Show that G_1 is isomorphic to the subgroup $\{(x, e) \in G_1 \times G_2 \mid x \in G_1\} =: H$.
Pf: $\phi : G_1 \to H$ be $\phi(g) = (g, e)$. Then $\phi(g_1 g_2) = (g_1 g_2, e) = (g_1, e)(g_2, e) = \phi(g_1)\phi(g_2)$, so ϕ is a homomorphism. Clearly ϕ is 1-1 and onto.

22 Show that if $d = \gcd(a, b)$ and $l = \mathrm{lcm}(a, b)$ then $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_d \times \mathbb{Z}_l$.

Pf: The best way to organize this is start with the natural quotient maps: if $m \mid n$ then we have a homomorphism $\mathbb{Z}_n \xrightarrow{q} \mathbb{Z}_m$ by $q\,[k]_n = [k]_m$. Since $a \mid l$, $b \mid l$, $d \mid a$ and $d \mid b$ we have natural maps

$$\mathbb{Z}_l \xrightarrow{i} \mathbb{Z}_a \times \mathbb{Z}_b \xrightarrow{\pi} \mathbb{Z}_d$$

$$i([n]_l) = \begin{pmatrix} [n]_a \\ [n]_b \end{pmatrix} \quad \text{and} \quad \pi \begin{pmatrix} [n]_a \\ [m]_b \end{pmatrix} = [n]_d - [m]_d$$

The minus is chosen so that $\pi(i([n]_l)) = 0$. To get the isomorphism we want, we need two more homomorphisms going the opposite direction.

(CONT.)

§3.4

(22) (cont.) Since $d = \gcd(a,b)$ and $\ell = \operatorname{lcm}(a,b)$ we can write

$$\begin{array}{ll} a = a'd & 1 = xa' + yb' \text{ for some } x, y \in \mathbb{Z}, \text{ and} \\ b = b'd & d = xa + yb \end{array}$$

$$\ell = a'b'd = ab' = a'b .$$

Define

$$\mathbb{Z}_\ell \xleftarrow{\ r\ } \mathbb{Z}_a \times \mathbb{Z}_b \xleftarrow{\ s\ } \mathbb{Z}_d$$

by $\quad s([k]_d) = \begin{pmatrix} [kxa']_a \\ -[kyb']_b \end{pmatrix} \quad$ and $\quad r\begin{pmatrix} [n]_a \\ [m]_b \end{pmatrix} = [nyb' + mxa']_\ell .$

These are well defined since $dxa' = xa \equiv 0\ (a)$, $dyb' = yb \equiv 0\ (b)$, and $ayb' + bxa' = y\ell + x\ell \equiv 0\ (\ell)$.

Together, these define isomorphisms $\phi = \begin{pmatrix} \pi \\ r \end{pmatrix}$ and $\psi = (s\ \ i)$

$$\mathbb{Z}_a \times \mathbb{Z}_b \underset{\psi}{\overset{\phi}{\rightleftarrows}} \mathbb{Z}_d \times \mathbb{Z}_\ell ,$$

$$\phi\begin{pmatrix} [n]_a \\ [m]_b \end{pmatrix} = \begin{pmatrix} [n-m]_d \\ [nyb' + mxa']_\ell \end{pmatrix} \quad \text{and} \quad \psi\begin{pmatrix} [k]_d \\ [j]_\ell \end{pmatrix} = \begin{pmatrix} [kxa' + j]_a \\ [-kyb' + j]_b \end{pmatrix}.$$

It is a simple calculation to show $\phi\psi$ and $\psi\phi$ are identity homomorphisms, so ϕ and ψ are inverse isomorphisms. (I.E. are isomorphisms inverse to one another.)

(25) If G is a group and $\phi: G \to S$ a 1-1 onto function then $(S, *)$ is a group if $s * t = \phi(\phi^{-1}(s)\,\phi^{-1}(t))$.

<u>Proof:</u> The product is the function $S \times S \xrightarrow{\phi^{-1} \times \phi^{-1}} G \times G \longrightarrow G \xrightarrow{\phi} S$, so closure is satisfied. For associativity,

$$s_1 * (s_2 * s_3) = \phi(\phi^{-1}(s_1)\,\phi^{-1}(s_2 * s_3)) = \phi(\phi^{-1}(s_1)\,\phi^{-1}(\phi(\phi^{-1}(s_2)\,\phi^{-1}(s_3))))$$

$$= \phi(\phi^{-1}(s_1)\,(\phi^{-1}(s_2)\,\phi^{-1}(s_3)))$$

(25) (cont.)

while $(s_1 * s_2) * s_3 = \phi((\phi^{-1}(s_1)\phi^{-1}(s_2))\,\phi^{-1}(s_3))$ similarly. These are equal by associativity of G. The element $\phi(e)$ is the identity:

$$s * \phi(e) = \phi(\phi^{-1}(s)\,\phi^{-1}(\phi(e)))$$

$$= \phi(\phi^{-1}(s)\,e) = \phi(\phi^{-1}(s)) = s$$

and similarly for $\phi(e) * s$. Finally, the inverse of s is $\phi(\phi^{-1}(s)^{-1})$ since

$$s * \phi(\phi^{-1}(s)^{-1}) = \phi(\phi^{-1}(s)\,\phi^{-1}(\phi(\phi^{-1}(s)^{-1})))$$

$$= \phi(\phi^{-1}(s)\,\phi^{-1}(s)^{-1}) = \phi(e),$$

the identity, and similarly on the other side. //

(26) Show that $\det : Gl_2(\mathbb{R}) \to \mathbb{R}^\times$ is a group homomorphism.

Proof: This is simply a calculation:

$$\det\left(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}\right) = \det\begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{pmatrix}$$

$$= (a_1b_1 + a_2b_3)(a_3b_2 + a_4b_4) - (a_3b_1 + a_4b_3)(a_1b_2 + a_2b_4)$$

$$= a_1a_4b_1b_4 + a_2a_3b_2b_3 - a_1a_4b_2b_3 - a_2a_3b_1b_4$$

$$= (a_1a_4 - a_2a_3)(b_1b_4 - b_2b_3)$$

$$= \det\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \det\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}. \quad //$$

(27) If $\phi : G_1 \to G_2$ is a homomorphism then $\ker\phi = \{g \in G_1 \mid \phi(g) = e\}$ is a subgroup of G_1

Pf: If $\phi(g_1) = e = \phi(g_2)$ then $\phi(g_1^{-1}) = \phi(g_1)^{-1} = e^{-1} = e$ and $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = ee = e$, so $\ker\phi$ is closed under inverses and products. //

§3.4

(28) A group homomorphism $\phi : G_1 \to G_2$ is an isomorphism iff $\ker \phi = \{e\}$ and $\phi(G_1) = G_2$.

Pf: Clearly $\phi(G_1) = G_2$ is the same as saying ϕ is onto.

Lemma: ϕ is 1-1 if and only if $\ker \phi = \{e\}$.

Pf: If $e \neq g \in \ker(\phi)$ then $\phi(g) = e = \phi(e)$ so ϕ is not 1-1. Conversely, if $\ker \phi = \{e\}$ and $\phi(x) = \phi(y)$ then $\phi(xy^{-1}) = ee^{-1} = e$ so $xy^{-1} \in \ker \phi$. Thus $xy^{-1} = e$, so $x = y$. Hence ϕ is 1-1. //

So 1-1 and onto is equivalent to $\ker \phi = \{e\}$ and $\phi(G_1) = G_2$. //