Math 331: HW 13 Solutions 7.8: 12, 17bc; 8.1: 6b, 18, 22;
Tuesday, 12 Dec 2006

7.8.12 Let G and H be the groups in Exercises 31 and 32 os Section 7.1. Use the First Isomorphism Theorem to prove that H is normal in G and that G/H is isomorphic to the multiplicative group $\mathbb{R}^*$ of nonzero real numbers. [*Hint:* Consider the map $f : G \to \mathbb{R}^*$ given by $f(T_{a,b}) = a$.]

Recall that from Exercise 7.1.31, for $a, b \in \mathbb{R}$ with $a \neq 0$, we define $T_{a,b} : \mathbb{R} \to \mathbb{R}$ by $T_{a,b}(x) = ax + b$ for $x \in \mathbb{R}$. The collection of all such functions forms a nonabelian group under composition. Note that for $a, b, c, d \in \mathbb{R}$ with $a, c \neq 0$, we have for $x \in \mathbb{R}$

$$T_{a,b} \circ T_{c,d}(x) = T_{a,b}(T_{c,d}(x)) = T_{a,b}(cx + d) = a(cx + d) + b = acx + ad + b = T_{ac,ad+b}(x);$$

hence, $T_{a,b} \circ T_{c,d} = T_{ac,ad+b}$. We use the hint to define a map $f : G \to \mathbb{R}^*$ given by $f(T_{a,b}) = a$. We prove that f is a homomorphism: let $u, v \in G$, then $u = T_{a,b}$ and $v = T_{c,d}$ for some $a, b, c, d \in \mathbb{R}$ with $a, b \neq 0$. Then

$$f(uv) = f(T_{a,b} \circ T_{c,d}) = f(T_{ac,ad+b}) = ac = f(T_{a,b})f(T_{c,d}) = f(u)f(v),$$

and so f is a homomorphism; note that f is surjective, since given $a \in \mathbb{R}^*$, we have $T_{a,0} \in G$ and $a = f(T_{a,0})$. The kernel of f is given by the collection of all $T_{a,b}$ with $a = 1$; hence, the kernel is $H = \{T_{1,b} \mid b \in \mathbb{R}\}$. Thus, H is a normal subgroup of G and by the First Isomorphism Theorem we have $G/H \cong \mathbb{R}^*$. ◆

7.8.17 (An exercise for those who know how to multiply 3×3 matrices.) Let G be the set of all matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

where $a, b, c \in \mathbb{Q}$. [Note by part (a), we may assume that G is a group.]

(b) Find the center C of G and show that C is isomorphic to the additive group $\mathbb{Q}$.

Let $A, X \in G$, then

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad X = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

for some $a, b, c, x, y, z \in \mathbb{Q}$. Then we have

$$AX = \begin{pmatrix} 1 & x + a & y + az + b \\ 0 & 1 & z + c \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad XA = \begin{pmatrix} 1 & a + x & b + xc + y \\ 0 & 1 & c + z \\ 0 & 0 & 1 \end{pmatrix};$$

so $AX = XA$ iff $az = xc$. It follows that A is in the center iff $az = xc$ for all $z, x \in \mathbb{R}$; but this is only possible if $a = c = 0$. Hence, the center C of G consists of all matrices A as above with $a = c = 0$. We define a map $f : \mathbb{Q} \to C$ by

$$f(b) = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

for $b \in \mathbb{Q}$. It is straightforward to see that f is bijective and since for $b, b' \in \mathbb{Q}$

$$f(b + b') = \begin{pmatrix} 1 & 0 & b + b' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = f(b)f(b'),$$

it follows that f is a homomorphism. Hence, f is an isomorphism and so $C \cong \mathbb{Q}$ as required. ◆

(c) Show that G/C is isomorphic to the additive group $\mathbb{Q} \times \mathbb{Q}$.

We apply the First Isomorphism Theorem to the map $g : G \to \mathbb{Q} \times \mathbb{Q}$ defined by

$$g\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = (a, c)$$

for $a, b, c \in \mathbb{Q}$. By construction g is surjective and the kernel of g coincides with C (since $(a, c) = (0, 0)$ iff $a = c = 0$). A straightforward computation shows that g is a homomorphism. Indeed with A, X in part (a) we have

$$g(AX) = (x + a, z + c) = (a, c) + (x, z) = g(A) + g(X).$$

Hence, by the First Isomorphism Theorem $G/C \cong \mathbb{Q} \times \mathbb{Q}$. ◆

8.1.6b Write $\mathbb{Z}_{15}$ as the direct sum of two of its subgroups.

Consider the two subgroups $\langle 3\rangle = \{0, 3, 6, 9, 12\}$ and $\langle 5\rangle = \{0, 5, 10\}$. Then we have $\langle 3\rangle \cap \langle 5\rangle = \{0\}$. Moreover, $\mathbb{Z}_{15} = \langle 3\rangle + \langle 5\rangle$ as can be seen from the following table

$+$	0	3	6	9	12
0	0	3	6	9	12
5	5	8	11	14	2
10	10	13	1	4	7

Hence by Theorem 8.3, $\mathbb{Z}_{15}$ may be written as the (internal) direct sum $\langle 3\rangle \oplus \langle 5\rangle$.

◆

8.1.18 Let $\mathbb{C}^*$ be the multiplicative group of nonzero complex numbers and $\mathbb{R}^{**}$ be the multiplicative group of positive real numbers. Prove that $\mathbb{C}^* \cong \mathbb{R}^{**} \times \mathbb{R}/\mathbb{Z}$, where $\mathbb{R}$ is the additive group of real numbers.

Let $f : \mathbb{R} \to \mathbb{C}^*$ be given by $f(t) = e^{2\pi it}$ for $t \in \mathbb{R}$. Then f is a homomorphism, since for all $s, t \in \mathbb{R}$ we have

$$f(s + t) = e^{2\pi i(s+t)} = e^{2\pi is}e^{2\pi it} = f(s)f(t).$$

Note that $f(t) = e^{2\pi it} = 1$ iff $t \in \mathbb{Z}$; hence the kernel of f is $\mathbb{Z}$. Then by the First Isomorphism Theorem, there is an isomorphism $\overline{f} : \mathbb{R}/\mathbb{Z} \to \operatorname{Im} f$ such that $\overline{f}(\mathbb{Z} + t) = f(t)$. Now define the map $\varphi : \mathbb{R}^{**} \times \mathbb{R}/\mathbb{Z} \to \mathbb{C}^*$ by

$$\varphi(r, \mathbb{Z} + t) = r\overline{f}(\mathbb{Z} + t) = re^{2\pi it}.$$

Since $\mathbb{C}^*$ is abelian, φ is a homomorphism. Since $\operatorname{Im} f = \{z \in \mathbb{C} \mid |z| = 1\}$, we have $\mathbb{R}^{**} \cap \operatorname{Im} f = \{1\}$; hence, the kernel of φ is trivial (i.e. $K_\varphi = \{1\}$) and so φ is injective. To see that φ is surjective, let $z \in \mathbb{C}^*$. Then since $z/|z| \in \operatorname{Im} f$, we have $z/|z| = \overline{f}(\mathbb{Z} + t)$ for some $\mathbb{Z} + t$. Hence,

$$z = |z|\overline{f}(\mathbb{Z} + t) = \varphi(|x|, \mathbb{Z} + t).$$

Hence, φ is surjective and thus φ yields the desired isomorphism.

◆

8.1.22 Let G and H be finite cyclic gropus. Prove that $G \times H$ is cyclic if and only if $(|G|, |H|) = 1$.

Let $m = |G|$ and $n = |H|$, then $G \cong \mathbb{Z}_m$ and $H \cong \mathbb{Z}_n$; so $G \times H \cong \mathbb{Z}_m \times \mathbb{Z}_n$. So if suffices to prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic iff $(m, n) = 1$.

Suppose that $(m, n) = 1$. Let $k \in \mathbb{Z}$; if $m \mid k$ and $n \mid k$, then $mn \mid k$ (this was proved in the first part of the course and the proof follows easily from expressing 1 as an integer linear combination of m and n). We claim that the order of $(1, 1)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$ is mn. Observe first that

$$(mn)(1, 1) = (n(m \cdot 1), m(n \cdot 1)) = (0, 0).$$

Now suppose that $k(1, 1) = (0, 0)$ for some $k > 0$. Then, $k \cdot 1 = 0$ in $\mathbb{Z}_m$ and $\mathbb{Z}_n$. Hence, $m \mid k$ and $n \mid k$; thus, $mn \mid k$ by the above fact. It follows that $mn \leq k$ and so the order of $(1, 1)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$ is mn as claimed. Since $\mathbb{Z}_m \times \mathbb{Z}_n$ has mn elements, $\mathbb{Z}_m \times \mathbb{Z}_n = \langle(1, 1)\rangle$ and so it is cyclic with generator $(1, 1)$.

Now suppose that $d = (m, n) \neq 1$. Then $m = m'd$ and $n = n'd$ for some positive integers m', n'. Then $k = m'n'd < mn$ and

$$k(a, b) = (n'ma, m'nb) = (0, 0)$$

for all $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Hence, there is no element of order mn so $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. Thus $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic iff $(m, n) = 1$.

◆