Prof. Alexandru Suciu

MATH 3175 **Group Theory** **Summer 2, 2022**

Solutions for Assignment 2

---

1. Let R be a ring. An element $x \in R$ is called an *idempotent* if $x^2 = x$. (For instance, both 0 and 1 are idempotents.)

(i) Let x be an idempotent, $x \neq 1$. Show that x is a zero-divisor.

Since x is idempotent, we have $x(x-1) = x^2 - x = 0$. Moreover, since $x \neq 1$, we have $x - 1 \neq 0$. Thus, x is a zero-divisor.

(ii) The ring R is called a *Boolean ring* if every element in R is an idempotent. Show that in such a ring, the following identities hold:

$$x = -x \qquad \text{for all } x \in R, \tag{1}$$

$$xy = yx \qquad \text{for all } x, y \in R. \tag{2}$$

Since $x + x$ is idempotent, we have $(x + x)^2 = x + x$, and so $x^2 + x + x + x^2 = x + x$, or $x^2 + x^2 = 0$. But x is also idempotent, and so we have $x + x = 0$, that is, $x = -x$.

Since $x + y$ is idempotent, we have $(x + y)^2 = x + y$, and so $x^2 + xy + yx + y^2 = x + y$. But x and y are also idempotent, and so we have $x + xy + yx + y = x + y$, that is, $xy + yx = 0$. From the previous computation, we know that $yx = -yx$. Thus, we conclude that $xy = yx$.

2. For the ring $R = \mathbb{Z}_{12}$:

(i) List all the invertible elements, zero-divisors, and idempotents.

- Invertible elements: 1, 5, 7, 11.
- Zero-divisors: 0, 2, 3, 4, 6, 8, 9, 10.
- Idempotents: 0, 1, 4, 9.

(ii) Are there any elements which are neither zero-divisors nor invertible?

No

(iii) Are there any zero-divisors which are not idempotent?

Yes: 2, 3, 6, 8, and 10.

3. Let $(G, \cdot, e)$ be a group. An element $a \in G$ is said to have finite order if there is a positive integer n such that $a^n := a \cdot a \cdots a$ (multiplication done n times) is equal to the identity e. The smallest such n is called the *order* of a, and is denoted by $\operatorname{ord}(a)$ (or $o(a)$, or $|a|$). If no such n exists, we say a has infinite order, and write $\operatorname{ord}(a) = \infty$.

(i) Show that, for all $a, b \in G$,

(1) $\operatorname{ord}(a) = \operatorname{ord}(a^{-1})$.

If $a = e$, then $a^{-1} = e$, and there is nothing to prove; so assume $a \neq e$.

If $\operatorname{ord}(a) = n$, for some $n > 1$, write $k := \operatorname{ord}(a^{-1})$. Note that $(a^{-1})^n = e$, and so $k | n$. Suppose $k < n$; then $(a^k)^{-1} = (a^{-1})^k = e$, and so $a^k = e$, contradicting $\operatorname{ord}(a) = n$. Therefore, $k = n$, and thus $\operatorname{ord}(a^{-1}) = \operatorname{ord}(a)$.

If $\mathrm{ord}(a) = \infty$, then $\mathrm{ord}(a^{-1}) = \infty$, too, since otherwise $(a^{-1})^n = e$ for some $n > 0$, which would imply $(a^n)^{-1} = e$, and so $a^n = e$, contradicting $\mathrm{ord}(a) = \infty$.

(2) $\mathrm{ord}(ab) = \mathrm{ord}(ba)$.

If $ab = e$, then $b = a^{-1}$ and $ba = e$, and there is nothing to prove; so assume $ab \neq e$.

First suppose $\mathrm{ord}(ab) = n$, for some $n > 1$, and write $k \coloneqq \mathrm{ord}(ba)$. Since $(ab)^n = e$, we have that $(ab)^{n-1} = (ab)^{-1} = b^{-1}a^{-1}$. Therefore, $(ba)^n = b(ab)^{n-1}a = b(b^{-1}a^{-1})a = e$. Thus, $k|n$. Suppose $k < n$; then $(ab)^k = a(ba)^{k-1}b = a(ba)^{-1}b = e$, and so $(ab)^k = e$, contradicting $\mathrm{ord}(ab) = n$. Therefore, $k = n$, and thus $\mathrm{ord}(ba) = \mathrm{ord}(ab)$.

Now suppose $\mathrm{ord}(ab) = \infty$, and assume $\mathrm{ord}(ba) = n$, for some integer $n > 1$. Then $(ab)^n = a(ba)^{n-1}b = a(ba)^{-1}b = e$, contradicting $\mathrm{ord}(ab) = \infty$. Therefore, $\mathrm{ord}(ba) = \mathrm{ord}(ab) = \infty$.

(ii) Assume now that the orders of a and b are finite and coprime, and that $ab = ba$. Show that $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$.

Write $\mathrm{ord}(a) = m$ and $\mathrm{ord}(b) = n$, where, by assumption, $\gcd(m, n) = 1$. Since $ab = ba$, we have: $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e^n e^m = e$. Setting $k \coloneqq \mathrm{ord}(ab)$, this implies $k|mn$. Suppose $k < mn$; then $e = (ab)^k = a^k b^k$, and so $b^k = (a^k)^{-1}$, which implies by part (i)(1) that $\mathrm{ord}(a^k) = \mathrm{ord}(b^k)$. But $\mathrm{ord}(a^k)|\,\mathrm{ord}(a) = m$ and $\mathrm{ord}(b^k)|\,\mathrm{ord}(b) = n$, contradicting the assumption that $\gcd(m, n) = 1$. Therefore, $k = mn$, that is, $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$.

4. For each of the following groups, list all their elements, together with their orders:

(i) $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, with orders $\{1, 12, 6, 3, 4, 12, 2, 3, 12, 4, 6, 12\}$.

(ii) $\mathbb{Z}_{12}^\times = \{1, 5, 7, 11\}$, with orders $\{1, 2, 2, 2\}$.

(iii) $\mathbb{Z}_6 \times \mathbb{Z}_2 = \{(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), (0,1), (1,1), (2,1), (3,1), (4,1), (5,1)\}$, with orders $\{1, 6, 3, 2, 3, 6, 2, 6, 6, 2, 6, 6\}$.

(iv) $S_3 \times \mathbb{Z}_2 = \{((), 0), ((12), 0), ((13), 0), ((23), 0), ((123), 0), ((132), 0), ((), 1), ((12), 1), ((13), 1), ((23), 1), ((123), 1), ((132), 1)\}$, with orders $\{1, 2, 2, 2, 3, 3, 2, 2, 2, 2, 6, 6\}$.

5. Let G be the set of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, with $a, b \in \mathbb{R}$ and $a \neq 0$.

(i) Show that G is a group under matrix multiplication.

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c^{-1} & -dc^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac^{-1} & -adc^{-1} + b \\ 0 & 1 \end{pmatrix}.$$

Thus, G is a subgroup of $\mathrm{GL}(2, \mathbb{R})$; in particular, a group.

(ii) Is G abelian?

No: $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$ is not equal to $\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix}$.

(iii) Find all the elements of G that commute with $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$.

$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ if and only if $\begin{pmatrix} 2a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2a & 2b \\ 0 & 1 \end{pmatrix}$,

which only happens if $b = 2b$, that is, $b = 0$.