HOMEWORK 9: SOLUTIONS - MATH 341
INSTRUCTOR: George Voutsadakis
Caution: These solutions were written speedily. They may contain mistakes!

Problem 1 *(a) Find up to isomorphism all Abelian groups of order 32 that have exactly two subgroups of order 4.*

(b) Let p be a prime. Determine how many Abelian groups there are of order p^5.

Solution:

(a) There are in total seven groups up to isomorphism of order $32 = 2^5$:

$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2, \quad \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2, \quad \mathbf{Z}_4 \times \mathbf{Z}_4 \times \mathbf{Z}_2,$$

$$\mathbf{Z}_8 \times \mathbf{Z}_2 \times \mathbf{Z}_2, \quad \mathbf{Z}_8 \times \mathbf{Z}_4, \quad \mathbf{Z}_{16} \times \mathbf{Z}_2, \quad \mathbf{Z}_{32}.$$

The first group has $\binom{5}{2}$ subgroups of order 4, the second has more than $\binom{3}{2} = 3$ subgroups of order 4, the third has also at least 3 sugroups of order 4, and the same holds for the 4th and the 5th groups in the list because $\mathbf{Z}_4$ and $\mathbf{Z}_8$ both contain subgroups of order 2 and 4. $\mathbf{Z}_{32}$ has a unique subgroup of order 4. So the only choice for exactly two subgroups of order 4 is the group $\mathbf{Z}_{16} \times \mathbf{Z}_2$. In fact these two subgroups are

$$H = \{(0,0),(4,0),(8,0),(12,0)\} \quad \text{and} \quad K = \{(0,0),(8,0),(0,1),(8,1)\}.$$

(b) There are 7 subgroups up to isomorphism of order p^5 :

$$\mathbf{Z}_p \times \mathbf{Z}_p \times \mathbf{Z}_p \times \mathbf{Z}_p \times \mathbf{Z}_p, \quad \mathbf{Z}_{p^2} \times \mathbf{Z}_p \times \mathbf{Z}_p \times \mathbf{Z}_p, \quad \mathbf{Z}_{p^2} \times \mathbf{Z}_{p^2} \times \mathbf{Z}_p,$$

$$\mathbf{Z}_{p^3} \times \mathbf{Z}_p \times \mathbf{Z}_p, \quad \mathbf{Z}_{p^3} \times \mathbf{Z}_{p^2}, \quad \mathbf{Z}_{p^4} \times \mathbf{Z}_p, \quad \mathbf{Z}_{p^5}.$$

■

Problem 2 *(a) Let p and q be distinct primes and G an Abelian group of order $|G| = n$, where both p and q divide n. Show that G contains a cyclic subgroup of order pq.*

(b) Let G_1 and G_2 be finite Abelian groups. Show that G_1 and G_2 have the same number of elements of order n for all n, if and only if $G_1 \cong G_2$.

Solution:

(a) Since $p \backslash n$ and $q \backslash n$, by the fundamental theorem of finite abelian groups, the given group G must have two direct factors of the form $\mathbf{Z}_{p^k}$ and $\mathbf{Z}_{q^l}$, with $k, l \geq 1$. Now $\langle p^{k-1} \rangle$ is a subgroup of $\mathbf{Z}_{p^k}$ of order p and $\langle q^{l-1} \rangle$ is a subgroup of $\mathbf{Z}_{q^l}$ of order q. Therefore, since $(p,q) = 1$, the group $\langle p^{k-1} \rangle \times \langle q^{l-1} \rangle$ is isomorphic to a cyclic subgroup of G of order pq.

(b) If $G_1 \cong G_2$, then G_1 and G_2 have the same number of elements of order n for all n, by Proposition 2.2.23 (4) on page 84. Suppose conversely, that $G_1 \ncong G_2$. Then, by the fundamental theorem of finite abelian groups, there exist a prime p, such that the direct factors of G_1 corresponding to p are not the same as the direct factors of G_2 corresponding to p. Suppose that k is the highest power such that the number m of direct factors $\mathbf{Z}_{p^k}$ in G_1 and the number n of direct factors $\mathbf{Z}_{p^k}$ in G_2 are different. Then, it is not difficult to see that the number of elements of order p^k in G_1 and in G_2 are not the same.

■

Problem 3 *(a) Let R be a ring. The* **center** *of R is defined as follows: $Z(R) = \{x \in R : xy = yx \text{ for all } y \in R\}$. Show that $Z(R)$ is a subring of R.*

(b) Find the center $Z(\mathbf{H})$ of the ring $\mathbf{H}$ of quaternions.

Solution:

(a) We use the subring criterion. Suppose that $x, y \in Z(R)$. Then, for all $z \in R, xz = zx$ and $yz = zy$. Therefore

$$z(x - y) = zx - zy = xz - yz = (x - y)z,$$

whence $x - y \in Z(R)$. Finally, $z(xy) = (zx)y = (xz)y = x(zy) = x(yz) = (xy)z$ and $xy \in Z(R)$, as well. Thus $Z(R)$ is a subring by the subring criterion.

(b) None of $i, -i, j, -j, k$ and $-k$ commutes with all other elements in the quaternion ring. Thus, the only elements that commute with every other element in the ring are the ones that correspond to real numbers, i.e.,

$$Z(\mathbf{H}) = \{a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} : a \in \mathbb{R}\}.$$

■

Problem 4 *(a) A* **Boolean ring** *is a ring with the property that $a^2 = a$ for all $a \in R$. Show that a Boolean ring is a commutative ring with $2a = 0$ for all $a \in R$.*

(b) For any set X, let $P(X) = \{A : A \subseteq X\}$ be the powerset of X. For any A and B in $P(X)$ define $A + B = \{x : x \in A \cup B, x \notin A \cap B\}, A \cdot B = A \cap B$. Show that under these two operations $P(X)$ is a ring with unity that is a Boolean ring.

Solution:

(a) We have

$$\begin{aligned} a+a &= (a+a)^2 \\ &= (a+a)(a+a) \\ &= a^2+a^2+a^2+a^2 \\ &= a+a+a+a, \end{aligned}$$

whence $a+a=0$, i.e., $2a=0$.

For commutativity,

$$\begin{aligned} a+b &= (a+b)^2 \\ &= (a+b)(a+b) \\ &= a^2+ab+ba+b^2 \\ &= a+ab+ba+b, \end{aligned}$$

whence $ab+ba=0$, which yields $ab=-ba$. But $2(ba)=0$, by our previous proof, whence $ba=-ba$, and, therefore $ab=ba$.

(b) Associativity of Addition:

$$\begin{aligned} (A+B)+C &= ((A\cap B^c)\cup(A^c\cap B))+C \\ &= (((A\cap B^c)\cup(A^c\cap B))\cap C^c)\cup(((A\cap B^c)\cup(A^c\cap B))^c\cap C) \\ &= (A\cap B^c\cap C^c)\cup(A\cap B\cap C^c)\cup(((A\cap B^c)^c\cap(A^c\cap B)^c)\cap C) \\ &= (A\cap B^c\cap C^c)\cup(A\cap B\cap C^c)\cup(((A^c\cup B)\cap(A\cup B^c))\cap C) \\ &= (A\cap B^c\cap C^c)\cup(A\cap B\cap C^c)\cup \\ &\quad (((A^c\cap(A\cup B^c))\cup(B\cap(A\cup B^c))\cap C)) \\ &= (A\cap B^c\cap C^c)\cup(A\cap B\cap C^c)\cup \\ &\quad (((A^c\cap A)\cup(A^c\cap B^c)\cup(B\cap A)\cup(B\cap B^c))\cap C) \\ &= (A\cap B^c\cap C^c)\cup(A\cap B\cap C^c)\cup(((A^c\cap B^c)\cup(B\cap A))\cap C) \\ &= (A\cap B^c\cap C^c)\cup(A\cap B\cap C^c)\cup((A^c\cap B^c\cap C)\cup(A\cap B\cap C)). \end{aligned}$$

Note that this is symmetric in A, B and C. Thus, we could reverse the equations grouping B and C first, to get $A+(B+C)=(A\cap B^c\cap C^c)\cup(A\cap B\cap C^c)\cup((A^c\cap B^c\cap C)\cup(A\cap B\cap C))$. Thus $A+(B+C)=(A+B)+C$.

The $\emptyset$ is the identity with respect to addition:

$$\begin{aligned} A+\emptyset &= (A\cap\emptyset^c)\cup(A^c\cap\emptyset) \\ &= (A\cap X)\cup\emptyset \\ &= A, \end{aligned}$$

and, similarly, for $\emptyset+A$.

The complement A is the inverse of A with respect to addition:

$$\begin{aligned} A+A &= (A\cap A^c)\cup(A^c\cap A) \\ &= \emptyset\cup\emptyset \\ &= \emptyset. \end{aligned}$$

Obviously, $+$ is also commutative.

The given multiplication is associative:

$$A(BC) = A(B \cap C) = A \cap (B \cap C) = (A \cap B) \cap C = (A \cap B)C = (AB)C.$$

It is also distributive with respect to addition:

$$\begin{aligned}
A(B+C) &= A \cap ((B \cap C^c) \cup (B^c \cap C)) \\
&= (B^c \cap A \cap C) \cup (A \cap B \cap C^c) \\
&= (A^c \cap A \cap C) \cup (B^c \cap A \cap C) \cup (A \cap B \cap A^c) \cup (A \cap B \cap C^c) \\
&= ((A^c \cup B) \cap (A \cap C)) \cup ((A \cup B) \cap (A^c \cup C^c)) \\
&= ((A \cap B)^c \cap (A \cap C)) \cup ((A \cap B) \cap (A \cap C)^c) \\
&= (A \cap B) + (A \cap C) \\
&= AB + AC.
\end{aligned}$$

For the Boolean property, it suffices to note that $A \cap A = A$.

■

Problem 5 *(a) Give an example of a commutative ring with no zero divisors that is not an integral domain.*

(b) Give an example of a ring with unity and no zero divisors that is not an integral domain.

Solution:

1. Check that $\langle 2\mathbf{Z}, +, \cdot \rangle$ is a commutative ring with no zero divisors that is not an integral domain since it does not have a multiplicative identity element.

2. The quaternion ring $\mathbf{H}$ is a ring with unity and without any zero divisors that is not an integral domain since it is not a commutative ring.

■