Math 320 H.W 9

Joseph C. McGuire

November 8, 2018

1 Problem (79)

Prove that every Abelian group of order 27 must have a subgroup of order 9.

Proof. Let G be an Abelian group such that $|G| = 27$. Then, by the Fundamental Theorem of Finite Abelian Groups, we have $G \approx \mathbb{Z}_{27}$. Then there exists an isomorphism $\phi : \mathbb{Z}_{27} \to G$. Also, note that $| < 3 > | = 9$ in $\mathbb{Z}_{27}$ and $< 3 >$ is a subgroup of $\mathbb{Z}_{27}$. Then, by Corollary 1 to Theorem 4.1, we have $| < 3 > | = |3| = 9$ in $\mathbb{Z}_{27}$. Hence by Theorem 6.2.4, $|\phi(3)| = 9$, hence $| < \phi(3) > | = 9$. By Theorem 3.4, $< \phi(3) >$ is a subgroup of G.
$\therefore$ Any finite Abelian group of order 27 has a subgroup of order 9. $\square$

2 Problem (80)

R ={s,t,u,v,w,x,y,z} is a finite ring under the +, * operations.

2.1 Which element equals 0 in this ring? Justify your answer.

$u = 0$, since under the $+$ operation, we have $u + a = a$, for all $a \in R$.

2.2 Does the ring have a unity element? If so, say which elements equal 1 and justify your answer.

$w = 1$, since under the operation * we have $w * b = b$, for all $b \in R$.

2.3 Find the elements -1 and 3 * 1 in R, and make it clear which is which.

Since $w = 1$, by part (2), and $u = 0$, by part (1), we want the element $a \in R$ such that $w + a = u$. Following the Cayley table the only such element that satisfies this condition is v. Hence $v = -1$ in R.

Next we will find the element $b \in R$ such that $w + w + w = b$, since by part (2) we have $w = 1$. Following the Cayley table, this gives us that $x = 3 * 1$.

2.4 What are the units of R? Explain how you know that your answer is right.

By the Cayley table, we have $v * v = w = 1$, $t * t = w = 1$, $w * w = w = 1$, and $x * x = w = 1$. Thus, the units in R are the element $\{v, t, w, x\}$.

3 Problem (81)

Let $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$. Prove that $\mathbb{Z}[\sqrt{3}]$ is a ring under the ordinary addition and multiplication of the real numbers.

Proof. First, note that $\mathbb{R}$ is a ring and $\mathbb{Z}[\sqrt{3}] \subseteq \mathbb{R}$. Then we will show $\mathbb{Z}[\sqrt{3}]$ is a ring by Theorem 12.3.

($\mathbb{Z}[\sqrt{3}]$ is nonempty)

Consider $1 + 3\sqrt{3}$, by definition of the set, we have $1 + 3\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$. Hence $\mathbb{Z}[\sqrt{3}] \neq \emptyset$.

($a - b \in \mathbb{Z}[\sqrt{3}]$) Let $a, b \in \mathbb{Z}[\sqrt{3}]$. Then for some $c, d, e, f \in \mathbb{Z}$, $a = c + d\sqrt{3}$ and $b = e + f\sqrt{3}$. Then consider the following:

$$\begin{aligned} a - b &= c + d\sqrt{3} - (e + f\sqrt{3}) \\ &= c + d\sqrt{3} - e - f\sqrt{3} \\ &= (c - e) + d\sqrt{3} - f\sqrt{3} \\ &= (c - e) + (d - f)\sqrt{3} \end{aligned}$$

Hence (a - b) $\in$ $\mathbb{Z}[\sqrt{3}]$. (ab $\in \mathbb{Z}[\sqrt{3}]$) Let $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$. Then for some $\gamma, \delta, \epsilon, \zeta \in \mathbb{Z}$, $\alpha = \gamma + \delta\sqrt{3}$ and $\beta = \epsilon + \zeta\sqrt{3}$. Then consider the following:

$$\begin{aligned} \alpha\beta = (\gamma + \delta\sqrt{3})(\epsilon + \zeta\sqrt{3}) = \alpha\epsilon + \gamma\zeta\sqrt{3} + \epsilon\delta\sqrt{3} + \delta\zeta(\sqrt{3})^2 \\ = \alpha\epsilon + \delta\zeta 3 + \gamma\zeta\sqrt{3} + \epsilon\delta\sqrt{3} = (\alpha\epsilon + \delta\zeta 3) + (\gamma\zeta + \epsilon\delta)\sqrt{3}. \end{aligned}$$

Since $(\gamma\zeta + \epsilon\delta), (\alpha\epsilon + \delta\zeta 3) \in \mathbb{Z}$, we have $\alpha\beta \in \mathbb{Z}[\sqrt{3}]$.

$\therefore$ By Theorem 12.3, $\mathbb{Z}[\sqrt{3}]$ is a subring of $\mathbb{R}$, hence a ring itself $\square$

4 Problem (82)

The set {0,2,4,6,8} under addition and multiplication modulo 10 has a unity. Find it, and show that it works.

We want the element of the above set such that for all $a \in \{0, 2, 4, 6, 8\}$, $ax \equiv a$(modulo 10), where x is our unity element. The only such element that this works with is 6 :

$$\begin{gathered} 0 * 6 \equiv 0 \text{ (modulo 10)} \\ 2 * 6 \equiv 12 \equiv 2 \text{ (modulo 10)} \\ 4 * 6 \equiv 24 \equiv 4 \text{ (modulo 10)} \\ 6 * 6 \equiv 36 \equiv 6 \text{ (modulo 10)} \\ 8 * 6 \equiv 48 \equiv 8 \text{ (modulo 10)} \end{gathered}$$

Thus 6 is the unity element of this specific set.

5 Problem (83)

5.1 Show that x = 3 is a solution to the equation $x^2 + 7 = 0$ in $\mathbb{Z}_8[x]$.

Take $x^2 + 7 = 0$ in $\mathbb{Z}_8[x]$, note that $7 \equiv -1$ (modulo 8). Hence $x^2 + 7 = 0$ iff $x^2 - 1 = 0$ in $\mathbb{Z}_8[x]$ iff $x^2 = 1$. If we take $x = 3$, then we get $x^2 = 9$ and $9 \equiv 1$ (modulo 8). Thus $x = 3$ is a solution to $x^2 + 7 = 0$ in $\mathbb{Z}_8[x]$.

5.2 The argument below seems to show that the <u>only</u> solution to $x^2 - 1 = 0$ in $\mathbb{Z}_8[x]$ are x = 1 and x = 7, which would contradict what you showed in part(a) above. Which implication in the argument is incorrect? Show that it is incorrect.

Step(ii) is incorrect, because in $\mathbb{Z}_8[x]$, $(x + 7)(x + 1) = 0$ doesn't imply that $x + 7 = 0$ or $x + 1 = 0$. Consider the case in part(a), where we had x = 3, then we have $(x + 7)(x + 1) = (3 + 7)(3 + 1) = (10)(4) \equiv 0$ (modulo 8). Hence our hypothesis is true, but $3 + 7 \equiv 10 \equiv 2$ (modulo 8) and $3 + 1 \equiv 4$ (modulo 8). So our conclusion is false. Thus in $\mathbb{Z}_8[x]$ $(x + 7)(x + 1) = 0 \nRightarrow x + 7 = 0$ or $x + 1 = 0$.

6 Problem (84)

Let R be a ring with unity 1, and let $a \in R$ be fixed. Prove that there can exist at most one element $b \in R$ such that $ab = ba = 1$.

Proof. Let R be a ring with unity 1 and $a \in R$ be fixed. Suppose, for sake of contradiction, that for some $b \in R$ and $c \in R$, where b and c are distinct in R, we have $ac = ca = 1$ and

$ab = ba = 1$. Then consider the following:

$$ca = 1$$
$$\text{iff } ca = 1 * 1, \text{ since 1 is the unity of R}$$
$$\text{iff } c(ba) = 1(b * 1), \text{ by left-multiplication}$$
$$\text{iff } c * 1 = b, \text{ by our assumption that } ab = ba = 1$$
$$\text{iff } c = b.$$

But this is a contradiction of our hypothesis that c and b were distinct. Thus there can exist at most one element $b \in R$ such that $ba = ab = 1$, for a fixed $a \in R$. □

7 Problem (85)

Find an integer n such that the ring $\mathbb{Z}_n$, need not have the following properties that the ring integers has:

7.1 $a^2 = a$ implies $a - 0$ or $a = 1$.

7.2 $ab = 0$ implies $a = 0$ or $b = 0$.

7.3 $ab = ac$ and $a \neq 0$ implies $b = c$.

Let n = 12, then $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ under the operations + and * modulo 12. Then note that the conditions don't hold:

(a.) $4^2 \equiv 4$(modulo 12), but $4 \not\equiv 0$(modulo 12) and $4 \not\equiv 1$(modulo 12).

(b.) $3 * 4 \equiv 0$(modulo 12), but $3 \not\equiv 0$(modulo 12) and $4 \not\equiv 0$(modulo 12).

(c.) $3 * 4 \equiv 0 \equiv 3 * 8$(modulo 12), but $4 \not\equiv 8$(modulo 12) and $3 \not\equiv 0$(modulo 12).

No, 12 isn't a prime.

8 Problem (86)

8.1 In $\mathbb{Z}_6$, show that $4|2$.

$4|2$ in $\mathbb{Z}_6$ iff $2q \equiv 4$(modulo 6), s.t $q \in \mathbb{Z}_6$ iff $q \equiv 2$(modulo 6). Thus $4|2$ in $\mathbb{Z}_6$, since $4 * 2 \equiv 2$(modulo 6).

8.2 In $\mathbb{Z}_8$, show that $3|7$.

$3|7$ in $\mathbb{Z}_8$ iff $3q \equiv 7$(modulo 8) iff $3q \equiv -1$(modulo 8) iff $q \equiv -3$(modulo 8) iff $q \equiv 5$(modulo 8). Hence $3 * 5 \equiv 7$(modulo 8) and $3|5$ in $\mathbb{Z}_8$.

8.3 In $\mathbb{Z}_{15}$, show that $9|12$.

$9|12$ in $\mathbb{Z}_{15}$ iff $9q \equiv 12$(modulo 15) iff $9q \equiv -3$(modulo 15) iff $-6q \equiv -3$(modulo 15) iff $q \equiv -2$(modulo 15). Hence $13 * 9 \equiv 12$(modulo 15), and $9|12$ in $\mathbb{Z}_{15}$.

9 Problem (87)

Give an example of a non-commutative ring that has exactly 16 elements.

Consider the set $M_2(\mathbb{Z}_2) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_2\}$.

Then $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

and $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Hence $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

and $M_2(\mathbb{Z}_2)$ is itself a ring, since $M_2(\mathbb{Z}_2) \neq \emptyset$, by above, and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a-c & b-f \\ c-g & d-h \end{pmatrix} \in M_2(\mathbb{Z}_2)$$

and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} \in M_2(\mathbb{Z}_2)$.

thus since $M_2(\mathbb{Z}_2) \subseteq M_2(\mathbb{Z}_n)$, we have $M_2(\mathbb{Z}_2)$ is a subgroup of $M_2(\mathbb{Z}_n)$ by Theorem 12.3.

10 Problem (88)

Let $G_1, G_2, ..., G_n$ be groups and let H_i be a subgroup of G_i for each $n \in \mathbb{N}$. Prove that $H_1 \oplus H_2 \oplus ... \oplus H_n$ is a subgroup of $G_1 \oplus G_2 \oplus ... \oplus G_n$.

Proof. Let $G_1, G_2, ..., G_n$ be groups and $H_i \geq G_i$ for all $i \in \{1, 2, ..., n\}$. Then let $(a_1, ..., a_n), (b_1, ..., b_n) \in H_1 \oplus ... \oplus H_n$, then we have $(a_1, ..., a_n) * (b_1, ..., b_n) = (a_1 b_1, ..., a_n b_n)$, since $a_i b_i \in H_i$, since H_i is a subgroup of G_i. Next, note that for each a_i, there exists $a_i^{-1} \in H_i$, since H_i is a subgroup of G_i. Thus $(a_1, ..., a_n) * (a_1^-1, ..., a_n^-1) = (a_1 a_1^{-1}, ..., a_n a_n^{-1}) = (e_1, ..., e_n)$. Hence $H_1 \oplus ... \oplus H_n$ has inverses for all of its elements. Thus, by Theorem 3.2, $H_1 \oplus ... \oplus H_n$ is a subgroup of $G_1 \oplus ... \oplus G_n$. □