Sample Solution.

MATH 307 Quiz 4 Time allowed: 20 min Name: _____

1. How many homomorphisms from $\mathbf{Z}_6$ to $\mathbf{Z}_4$, and how many of them are surjective? Prove your results.

$k=0,1,2,3$.

Let $\phi([1]) = [k]$ in $\mathbb{Z}_4$. Then $\phi([x]) = [kx]_4$.

To be well-defined, $[x]=[y]$ in $\mathbb{Z}_6$; i.e., $x-y=6q$, $q\in\mathbb{Z}$

we require $[kx]=[ky]$ in $\mathbb{Z}_4$ i.e., $kx-ky=4q$ is a multiple of 4. $\therefore$ k is even.

So $k=0$ or 2.

Then $\phi([a]+[b]) = \phi([a+b]) = [k(a+b)]$ equal to $\phi([a])+\phi([b]) = [ka]+[kb]$ //

So ϕ are homomorphisms in each case.

$k=0$ $\quad \phi(\mathbb{Z}_6) = \{[0]\} \subseteq \mathbb{Z}_4$

$k=2$ $\quad \phi(\mathbb{Z}_6) = \{[0],[2]\} \subseteq \mathbb{Z}_4$

None of them is surjective.

2. Suppose H, K are subgroups of G, and $HK = \{hk : h \in H, k \in K\}$.

(a) Show that HK may not be a subgroup of G. [Hint: Consider $G = S_3$.]

(b) Show that HK is a subgroup of G if H is normal.

(a) Consider S_3, $H = \{\varepsilon, (1,2)\}$, $K = \{\varepsilon, (1,3)\}$. ε is the identity

HK has 4 elements and cannot be a subgroup of S_3

because $|HK| = |H||K|/|H\cap K| = 4$.

(b) Assume H is normal.

i) $e\in H$, $e\in K \Rightarrow e\cdot e \in HK$, is non-empty.

ii) Let $h_1k_1, h_2k_2 \in HK$ with $h_1, h_2 \in H$, $k_1, k_2 \in K$.

Then $h_1k_1h_2k_2 = h_1(k_1h_2k_1^{-1})(k_1k_2) = (h_1\hat{h})(k_1k_2) \in HK$

where $\hat{h} = k_1h_2k_1^{-1} \in H$ as H is normal.

iii) Let $h_1k_1 \in HK$ with $h_1 \in H$, $k_1 \in K$.

Then $(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = (k_1^{-1}h_1^{-1}k_1)k_1^{-1} = \hat{h}k_1^{-1} \in HK$

where $\hat{h} = k_1^{-1}h_1^{-1}k_1 \in H$ as H is normal.

+, +·

Example $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$;

$\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq \mathbb{R}[x] \subseteq \mathbb{C}[x]$; → ✓ $\mathbb{Z}_p[x]$, $\mathbb{Z}_n[x]$ $n=a,b$ is NOT

$M_2(\mathbb{Z}) \subseteq M_2(\mathbb{Q}) \subseteq M_2(\mathbb{R}) \subseteq M_2(\mathbb{C})$;

$\mathbb{Z}[i]$.

are integral domain

Let ① $GL_2(\mathbb{R}) = \{ A \in M_2(\mathbb{R}) : \det(A) \neq 0 \}$ is NOT a subring of $M_2(\mathbb{R})$

② $\mathcal{A} = \{ A \in M_2(\mathbb{R}) : \det(A) = 0 \}$ is NOT a subring of $M_2(\mathbb{R})$

① $A, B \in GL_2(\mathbb{R}) \not\Rightarrow A+B \in GL_2(\mathbb{R})$ e.g. $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ ✓

$(GL_2(\mathbb{R}), +)$ not closed

no identity.

② $(\mathcal{A}, +)$ is not closed, $A = \begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix}$ & $B = \begin{bmatrix} 0 & 0 \\ 0 & -1 \end{bmatrix}$.

$$\mathbb{Z}[i] = \{ a_0 + a_1 i + a_2 i^2 + a_3 i^3 + \cdots + a_n i^n : n \in \mathbb{N} \cup \{0\}, a_0 \cdots a_n \in \mathbb{Z} \}$$

$$= \{ a_0 + a_1 i : a_0, a_1 \in \mathbb{Z} \}$$ Gaussian integers.

$\subseteq \mathbb{C}[i] = \mathbb{C}$.

Subring check: ① non-empty, ② $a, b \in S \Rightarrow a-b \in S$ ③ $a, b \in S \Rightarrow ab \in S$

Subgroup test for $(S, +)$.

① $0 = 0 + 0i \in \mathbb{Z}[i]$ ✓

② Let $a_1 + ia_2$, $b_1 + ib_2 \in \mathbb{Z}[i]$ with $a_1, a_2, b_1, b_2 \in \mathbb{Z}$

② Then $(a_1 + ia_2) - (b_1 + ib_2) = (a_1 - b_1) + i(a_2 - b_2) \in \mathbb{Z}[i]$

③ $(a_1 + ia_2)(b_1 + ib_2) = (a_1 b_1 - a_2 b_2) + i(a_1 b_2 + a_2 b_1) \in \mathbb{Z}[i]$

($a_1 b_1 - a_2 b_2 \in \mathbb{Z}$, $a_1 b_2 + a_2 b_1 \in \mathbb{Z}$)

x^2-3x+2

$(x-1)(x-2)=0$

$\mathbb{R}$

$ab=ac$

$\mathbb{Z}_4$

$2\cdot 2=2\cdot 0$

$2(2-0)=0$

Chapter 13 Integral Domains

Definitions (a) A nonzero element a in a commutative ring R is a zero divisor if there is a nonzero element b such that $ab = 0$.

(b) An integral domain is a communtative ring with unity and no zero-divisors.

(c) A field is a commutative ring R such that $(R^*, \cdot)$ is a group.

Examples $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}_n$, $M_2(\mathbb{Z})$, $\mathbb{Z}[x]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Z}_3[i]$, external direct product $R_1 \oplus R_2$.

Example: In $\mathbb{Z}_4$, 2 is a zero divisor.

Example: In $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

$(1,0)\cdot(0,1) = (0,0)$

Example: $D_2(\mathbb{Z}_2)$

$= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}$

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ are zero divisors

In $\mathbb{Z}_m \oplus \mathbb{Z}_n$, $m, n > 1$

$(1,0)(0,1) = (0,0)$

Prop: For a finitely generated Abelian group G.

G has no zero divisor $\iff G \cong \mathbb{Z}$ or $\mathbb{Z}_p$, p prime

(b) $\mathbb{Z}$, $\mathbb{Z}_p$ are integral domain

$D_n(R) = \left\{ \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix} : a_i \in R \right\}$

$\cong R \oplus R \oplus \cdots \oplus R$ (n times)

$\mathbb{Z}$ not a field / only an integral domain.

$\mathbb{R}$ is a field

$\mathbb{Z}_n$ is an integral domain $\iff$ n is a prime

$\mathbb{Z}_n$ is a field $\iff$ n is a prime.

$3 \in \mathbb{Z}_7^*$

$3 \cdot 5 = 15 = 1$ in $\mathbb{Z}_7$

$3 \cdot b = 1$

$\not\exists b$

$\mathbb{Z}_n$, n prime $(\mathbb{Z}_n^*, \cdot)$ is a field because $k \neq 0$ in $\mathbb{Z}_n$.

$\gcd(k, n) = 1$, $\exists\, x, y \in \mathbb{Z}$ s.t. $kx + ny = 1$.

$\therefore kx = 1$ in $\mathbb{Z}_n$

$\therefore [k][x] = [1]$ in $\mathbb{Z}_n$

In $\mathbb{Z}_6$, 2, 3, 4 are zero divisors
1, 5 are not zero divisors
0

Theorem 13.1 If $a \in R$ is not a zero divisor and $ab = ac$, then $b = c$. Consequently, if R is an integral domain and $a \in R$ is nonzero such that $ab = ac$, then $b = c$.

$ab = ac$, a is not a zero divisor in R.

Then $ab - ac = a(b-c)$ $\Rightarrow$ $b - c = 0$, i.e., $b = c$

In $\mathbb{Z}_4$

$2 \cdot 3 = 2 \cdot 1$

$\Rightarrow 3 = 1$.

Remark: $AB = AC$ $A, B, C \in M_n(\mathbb{R})$

A^{-1} exists

Then

$B = C$

$0 = A(B-C)$ / $A^{-1}0 = A^{-1}A(B-C)$

Theorem 13.2 A finite integral domain is a field.

Corollary If p is a prime, then $\mathbb{Z}_p$ is a field.