Chap 18 Ideals and homomorphisms

Let A be a ring. B is called a subring of A if B is closed w.r.t. addition, multiplication, and negatives.

Fact: If a nonempty subset $B \subseteq A$ is closed w.r.t. addition, multiplication, and negatives, then B with the operations of A is a ring.

Fact: If B is a nonempty subset of A, then B is a subring of A if and only if B is closed w.r.t. subtraction and multiplication.

Def: $B \subseteq A$, $B \neq \phi$. We say that B absorbs products (in A) if $\forall b \in B, \forall x \in A$ $xb$ and $bx$ are in B

Def: A nonempty subset B of a ring A is called an ideal of A if B is closed w.r.t. addition and negatives, and B absorbs products in A.

Ex of subrings: $\mathbb{Q}$ is a subring of $\mathbb{R}$.
$\mathbb{Z}$ is - - - of $\mathbb{Q}$ and of $\mathbb{R}$

Ex of ideals: $2\mathbb{Z} = \{\text{even integers}\}$ is an ideal of $\mathbb{Z}$.

In a commutative ring A with unity, $\forall a \in A$, the principal ideal generated by a, denoted by $(a)$ is the subset $\{x \cdot a \,;\, x \in A\} = (a)$   $2\mathbb{Z} = (2)$

---

$B \subset A$ is an ideal iff B is closed w.r.t. subtraction and B absorbs products in A

ideals are in rings as normal subgroups are in groups.

ideals play an important role in connection with homomorphism.

Def. A homomorphism from a ring A to a ring B is a function $f: A \to B$ satisfying

- $f(x_1 + x_2) = f(x_1) + f(x_2)$   $\forall x_1, x_2 \in A$.
- $f(x_1 x_2) = f(x_1) f(x_2)$

Ex: $f: \mathbb{Z}_{mn} \to \mathbb{Z}_n$ $\quad$ $f: \mathbb{Z} \to \mathbb{Z}_n$

$\bar{k}^{mn} \mapsto \bar{k}^n$ $\quad$ $k \mapsto \bar{k}^n$

$f: A \to B$ a ring homomorphism $\Rightarrow f(A)$ is a subring of $B$.

$\ker(f) = \{x \in A : f(x) = 0\}$ kernel of $f$ is an ideal of $A$.

Pf: $\ker(f)$ is closed under subtraction: $\cdot\ x, y \in \ker(f) \Rightarrow f(x-y) = f(x) - f(y) = 0 - 0 = 0$

$\Rightarrow x - y \in \ker(f)$

$\cdot \ker(f)$ is absorbs products in $A$: $\forall a \in A, x \in \ker(f)$.

$$f(a \cdot x) = f(a) \cdot f(x) = f(a) \cdot 0 = 0 \Rightarrow a \cdot x \in \ker(f)$$

So $\ker(f)$ is an ideal of $A$.

Exer: A.2 $B = \{x + 2^{\frac{1}{3}}y + 2^{\frac{2}{3}}z : x, y, z \in \mathbb{Z}\}$ is a subring of $\mathbb{R}$

Pf: $\cdot$ $B$ is closed under subtraction:

$$(x_1 + 2^{\frac{1}{3}}y_1 + 2^{\frac{2}{3}}z_1) - (x_2 + 2^{\frac{1}{3}}y_2 + 2^{\frac{2}{3}}z_2) = (x_1 - x_2) + 2^{\frac{1}{3}}(y_1 - y_2) + 2^{\frac{2}{3}}(z_1 - z_2) \in B$$

$\cdot$ $B$ is closed under multiplication:

$$(x_1 + 2^{\frac{1}{3}}y_1 + 2^{\frac{2}{3}}z_1)(x_2 + 2^{\frac{1}{3}}y_2 + 2^{\frac{2}{3}}z_2) = (x_1x_2 + 2y_1z_2 + 2z_1y_2) + 2^{\frac{1}{3}}(x_1y_2 + y_1x_2 + 2z_1z_2)$$
$$+ 2^{\frac{2}{3}}(x_1z_2 + z_1x_2 + y_1y_2) \quad \in B.$$

Exer B.2 List all ideals of $\mathbb{Z}_{12}$

ideals are subgroups of $(\mathbb{Z}_{12}, +)$. Any subgroup of a cyclic group is a cyclic group. For any integer $n$ with $n \mid 12$, there is a unique subgroup of order $n$. So possible subgroups of $\mathbb{Z}_{12}$ are:

$\{0\}$, $\langle \bar{2} \rangle$, $\langle \bar{3} \rangle$, $\langle \bar{4} \rangle$, $\langle \bar{6} \rangle$, $\mathbb{Z}_{12}$.

Easy to verify these subsets are indeed ideals which are call principal ideals:

$(0)$ $(\bar{2})$, $(\bar{3})$, $(\bar{4})$, $(\bar{6})$, $\mathbb{Z}_{12} = (\bar{1})$

Ex: B.9 Give an example of a subring of $\mathbb{Z}_3 \times \mathbb{Z}_3$ which is not an ideal

$B = ((1,1)) = \{(0,0), (1,1), (2,2)\}$ is a subring of $\mathbb{Z}_3 \times \mathbb{Z}_3$, but not an ideal:

$(1,0)\cdot(1,1) = (1,0) \notin B$.

C.4 If a subring B of an integral domain A contains 1, then B is an integral domain.

Pf: A $\underbrace{\text{ring}}_{\text{with unity}}$ is an integral domain iff it satisfies the cancellation property

If A satisfies the cancellation property, then B also satisfies the cancellation property.

---

Exer: E. Examples of Homomorphisms

E.5. $(A = \mathbb{R}\times\mathbb{R}, +, \odot)$ $\quad (a,b)\odot(c,d) = (ac, bc)$

$f: A \to M_2(\mathbb{R})$ $\quad f(x,y) = \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}$.

- $f((x_1,y_1)+(x_2,y_2)) = f((x_1+x_2, y_1+y_2)) = \begin{pmatrix} x_1+x_2 & 0 \\ y_1+y_2 & 0 \end{pmatrix} = \begin{pmatrix} x_1 & 0 \\ y_1 & 0 \end{pmatrix} + \begin{pmatrix} x_2 & 0 \\ y_2 & 0 \end{pmatrix} = f((x_1,y_1)) + f((x_2,y_2))$
- $f((x_1,y_1)\odot(x_2,y_2)) = f((x_1x_2, y_1x_2)) = \begin{pmatrix} x_1x_2 & 0 \\ y_1x_2 & 0 \end{pmatrix} = \begin{pmatrix} x_1 & 0 \\ y_1 & 0 \end{pmatrix}\cdot\begin{pmatrix} x_2 & 0 \\ y_2 & 0 \end{pmatrix} = f((x_1,y_1))\cdot f((x_2,y_2))$

$\mathrm{rang}(f) = \left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \in M_2(\mathbb{R}) \right\}$. $\quad \ker(f) = \{(0,0)\}$.

Exer F.5. $f: A \to B$ is a homomorphism. B is an integral domain.

$f(x) = f(x\cdot 1) = f(x)\cdot f(1)$ $\quad$ B is an integral domain $\Leftrightarrow$ B satisfies the cancellation property.

$\Rightarrow$ 2 cases: $\cdot\ \exists x \in A$, s.t. $f(x) \neq 0 \Rightarrow f(1) = 1$

OR $\cdot\ \forall x \in A,\ f(x) = 0 \Leftrightarrow f(1) = 0$

If $f(1) = 1$, and $x$ is invertible, then $f(x)\cdot f(x^{-1}) = f(x x^{-1}) = f(1) = 1 \Rightarrow f(x)$ is invertible

$f(x^{-1})\cdot f(x) = f(x^{-1} x) = f(1) = 1$

If $A$ and $B$ are rings, an isomorphism from $A$ to $B$ is a homomorphism which is a one-to-one correspondence from $A$ to $B$. In other words, it is an injective and surjective homomorphism.

Chap 17

<u>Ex</u>: A.1 $A=\mathbb{Z}$ with addition: $a\oplus b = a+b-1$

$$a\odot b = ab-(a+b)+2$$

$(A,\oplus)$ is an abelian group with identity $1$ and $\ominus a = 2-a \ \forall a\in A$

$(A,\odot)$ is associative: $(a\odot b)\odot c = (ab-(a+b)+2)\odot c$

$$= (ab-(a+b)+2)c-(ab-(a+b)+2+c)+2$$

$$= abc-ac-bc-ab+a+b+c$$

$$\Vert$$

$$a\odot(b\odot c) = a\odot(bc-(b+c)+2)$$

$$= a(bc-(b+c)+2)-(a+bc-(b+c)+2)+2 = abc-ab-ac-bc+a+b+c$$

---

$(\mathbb{Z},\oplus,\odot)$ is isomorphic to $(\mathbb{Z},+,\times)$:

$$f:\ \mathbb{Z}\longrightarrow\mathbb{Z} \qquad f \text{ is bijective: } f^{-1}(y)=y+1.$$

$$x \longmapsto x-1$$

$$f(x\oplus y) = x\oplus y-1 = (x+y-1)-1 = x-1+y-1 = f(x)+f(y)$$

$$f(x\odot y) = x\odot y-1 = xy-(x+y)+2-1 = (x-1)\cdot(y-1) = f(x)\cdot f(y).$$

---

<u>Exer</u> G.3. $\{(x,x): x\in\mathbb{Z}\}$ is a subring of $\mathbb{Z}\times\mathbb{Z}$.

$$\{(x,x): x\in\mathbb{Z}\}\cong\mathbb{Z}$$

$$f:\ \mathbb{Z}\longrightarrow\{(x,x): x\in\mathbb{Z}\} \qquad f \text{ is bijective homomorphism}$$

$$x\longmapsto(x,x).$$