Basic computations in a ring

Monday, August 7, 2017 3:29 PM

<u>Lemma</u>. Let R be a ring. For any $a, b \in R$, we have

① $0 \cdot a = a \cdot 0 = 0$

② $(-a) \cdot b = -ab = a \cdot (-b)$.

③ $(-a) \cdot (-b) = a \cdot b$.

<u>Pf.</u> ① $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$

In the abelian group $(R, +)$ we have cancellation. So $0 = 0 \cdot a$.

$a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$. So again using the cancellation property we have $a \cdot 0 = 0$.

② $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$

So $(-a) \cdot b = -a \cdot b$.

$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$

So $a \cdot (-b) = -a \cdot b$.

③ $(-a) \cdot (-b) = -(-a) \cdot b = -(-a \cdot b) = a \cdot b$.

(we have used part ② twice.) $\blacksquare$

In group theory, you have learned that in an additive group $(R, +)$ for any $a \in R$, the subgroup generated by a is $\{na \mid n \in \mathbb{Z}\}$

Characteristic of a unital ring.

Monday, August 7, 2017 3:47 PM

<u>Lemma.</u> Suppose R is a unital ring. Then $c: \mathbb{Z} \to R$,

$$c(n) = n 1_R \text{ is a ring homomorphism.}$$

<u>Proof.</u> In group theory, you have seen that c is an abelian group homomorphism $(\mathbb{Z},+) \to (R,+)$.

$\forall\ m,n \in \mathbb{Z}^+$, $c(m)\,c(n) = (\underbrace{1_R + \cdots + 1_R}_{m})(\underbrace{1_R + \cdots + 1_R}_{n})$

$$\overset{\boxed{\text{distribution}}}{=} \underbrace{1_R \times 1_R + \cdots + 1_R \times 1_R}_{mn} = \underbrace{1_R + \cdots + 1_R}_{mn}$$

$$= c(mn).$$

$$c(-m)\,c(n) = (\underbrace{(-1_R) + \cdots + (-1_R)}_{m})(\underbrace{1_R + \cdots + 1_R}_{n})$$

$$= \underbrace{(-1_R) \times 1_R + \cdots + (-1_R) \times 1_R}_{mn}$$

$$= \underbrace{(-1_R) + \cdots + (-1_R)}_{mn} = -mn 1_R$$

Similarly we can get $c(m)\,c(-n) = c(-mn)$ and $c(-m)\,c(-n) = c(mn)$.

$c(0)\,c(\pm n) = 0 \cdot c(\pm n) = 0 = c(0)$

$c(\pm m)\,c(0) = c(\pm m) \cdot 0 = 0 = c(0)$. ■

<u>Def.</u> The characteristic of a ring R is <u>zero</u> if there is no positive integer n such that $nx = 0$ for any $x \in R$.

Characteristic of a ring

Monday, August 28, 2017 7:41 PM

If for some positive integer n we have $nx=0$ for any $x\in R$, the characteristic of R is the smallest such number.

So $\text{char}(R)\, x = 0$ for any $x\in R$.

Proposition. Let $\ell = \text{l.c.m.}\{\text{ord}(x) \mid x\in R\}$ where $\text{ord}(x)$ is the order of x in $(R,+)$. If $\ell<\infty$, then $\text{char}(R)=\ell$. If $\ell=\infty$, then $\text{char}(R)=0$.

Pf. From group theory we know $nx=0$ if and only if $\text{ord}(x)\mid n$. So if $\exists n\in\mathbb{Z}^+$, $\forall x\in R$, $nx=0$, then $\text{ord}(x)$'s have a common multiple as x ranges in R. And so

$$\text{char}(R)\neq 0 \iff \ell = \text{l.c.m.}\{\text{ord}(x)\mid x\in R\}<\infty.$$

$\forall x\in R$, $\text{char}(R)x=0$ implies $\text{ord}(x)\mid \text{char}(R)$. Hence $\ell \mid \text{char}(R)$.

If $\text{char}(R)\neq 0$, $\ell\mid \text{char}(R)$ implies $\ell\leq \text{char}(R)$.

$\forall x\in R$, $\text{ord}(x)\mid \ell \Rightarrow \ell x = 0$; this implies $\text{char}(R)\leq \ell$.

Therefore, if $\text{char}(R)\neq 0$, then $\text{char}(R)=\ell$. ∎

Next we will find the characteristic of a unital ring.

Characteristic of a unital ring

Monday, August 7, 2017 4:46 PM

Lemma. For a unital ring R, $\operatorname{l.c.m.}\{\operatorname{ord}(x) \mid x \in R\} = \operatorname{ord}(1_R)$.

And so $\operatorname{char}(R) = \begin{cases} \operatorname{ord}(1_R) & \text{if } \operatorname{ord}(1_R) < \infty \\ 0 & \text{if } \operatorname{ord}(1_R) = \infty. \end{cases}$

Pf. If $\operatorname{ord}(1_R) = \infty$, then by the definition of the character. of a ring, we have $\operatorname{char}(R) = 0$. And the claim follows.

If $\operatorname{ord}(1_R) = n < \infty$, then $n\, 1_R = 0$. So for any $a \in R$, we have $(n\, 1_R) \cdot a = 0 \cdot a = 0$, which implies

$$0 = (\underbrace{1_R + \cdots + 1_R}_{n}) \cdot a = \underbrace{a + \cdots + a}_{n} = n a.$$

And so $\operatorname{ord}(a) \mid n$; and the claim follows. ∎

Lemma. Let $c : \mathbb{Z} \to \mathbb{Z}_n$, $c(a) = a\, 1_{\mathbb{Z}_n}$. Then

$c(a)$ is the remainder of a divided by n.

Pf. Suppose q is the quotient and r is the remainder of a divided by n. Then $a = nq + r$. So

$$c(a) = (nq+r)\, 1_{\mathbb{Z}_n} \underset{\substack{\text{Since} \\ n 1_{\mathbb{Z}_n} = 0}}{=} r\, 1_{\mathbb{Z}_n} = \underbrace{1_{\mathbb{Z}_n} + \cdots + 1_{\mathbb{Z}_n}}_{r} = r.$$

∎

Homomorphisms between Zn's

Monday, August 7, 2017 5:00 PM

<u>Propositions</u>. Let $m,n\in\mathbb{Z}^+$. Then

$c_{m,n}:\mathbb{Z}_m\to\mathbb{Z}_n$, $c_{m,n}(a)=a1_{\mathbb{Z}_n}$ is a homomorphism

if and only if $n\mid m$.

<u>Pf</u>: $(\Rightarrow)$ If $c_{m,n}$ is a group homomorphism from

$(\mathbb{Z}_m,+)$ to $(\mathbb{Z}_n,+)$, then

$$m\,1_{\mathbb{Z}_n}=m\,c_{m,n}(1_{\mathbb{Z}_m})=c_{m,n}(m\,1_{\mathbb{Z}_m})$$

$$=c_{m,n}(0_{\mathbb{Z}_m})=0_{\mathbb{Z}_n}.$$

So the additive order of $1_{\mathbb{Z}_n}$ should divide m,

which means $n\mid m$.

$(\Leftarrow)$. $c_{m,n}(a\oplus_m b)=(a\oplus_m b)\,1_{\mathbb{Z}_n}\overset{n}{\equiv}a\oplus_m b$

$a\oplus_m b\overset{m}{\equiv}a+b$, which means $m\mid a+b-a\oplus_m b$.

Since $n\mid m$, we get that $n\mid a+b-a\oplus_m b$. So

$a\oplus_m b\overset{n}{\equiv}a+b$. Hence

$c_{m,n}(a\oplus_m b)\overset{n}{\equiv}a+b\overset{n}{\equiv}a\oplus_n b$. Thus $c_{m,n}(a\oplus_m b)=a\oplus_n b$.

- $\left.\begin{array}{l} c_{m,n}(a\odot_m b)=(a\odot_m b)\,1_{\mathbb{Z}_n}\overset{n}{\equiv}a\odot_m b \\ \left.\begin{array}{l} a\odot_m b\overset{m}{\equiv}ab \\ n\mid m\end{array}\right\}\Rightarrow a\odot_m b\overset{n}{\equiv}ab\end{array}\right\}\Rightarrow$ (next page)

Modern Chinese remainder theorem

Monday, August 7, 2017 5:15 PM

$c_{m,n}(a \odot_m b) \overset{n}{\equiv} ab \overset{n}{\equiv} a \odot_n b$, which implies

$$c_{m,n}(a \odot_m b) = a \odot_n b .$$

And so $c_{m,n}$ is a homomorphism. ∎

<u>Remark</u>. If $m, n \in \mathbb{Z}^+$ and $n \mid m$, then the following is a "commutative diagram"

$$\begin{tikzcd} & \mathbb{Z} \arrow[dl, "c_m"'] \arrow[dr, "c_n"] \arrow[d, phantom, "\circlearrowright"] & \\ \mathbb{Z}_m \arrow[rr, "c_{m,n}"'] & & \mathbb{Z}_n \end{tikzcd}$$

where $c_m(a) = a 1_{\mathbb{Z}_m}$ and $c_n(a) = a 1_{\mathbb{Z}_n}$;

this means $c_n = c_{m,n} \circ c_m$.

<u>Theorem</u>. Let $r, s \in \mathbb{Z}^+$ and $\gcd(r,s) = 1$. Then

$$\mathbb{Z}_{rs} \simeq \mathbb{Z}_r \times \mathbb{Z}_s .$$

<u>Proof</u>. Let $\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ be

$$\phi(a) = (c_{rs,r}(a), c_{rs,s}(a)).$$ Then

$$\begin{aligned}\phi(ab) &= (c_{rs,r}(ab), c_{rs,s}(ab)) \\ &= (c_{rs,r}(a)\, c_{rs,r}(b), c_{rs,s}(a)\, c_{rs,s}(b)) \\ &= (c_{rs,r}(a), c_{rs,s}(a))(c_{rs,r}(b), c_{rs,s}(b)) = \phi(a)\phi(b).\end{aligned}$$

And similarly one can show $\phi(a+b) = \phi(a) + \phi(b)$

Notice that, since $r \mid rs$ and $s \mid rs$, by Proposition $c_{rs,r}$ and

Modern Chinese remainder theorem

Monday, August 7, 2017 10:17 PM

$c_{rs,s}$ are homomorphisms.

Since ϕ is a group homomorphism, it is injective if and only if its kernel is $\{0\}$.

$$\begin{aligned}
\phi(a)=0 &\iff c_{rs,r}(a)=0 \text{ and } c_{rs,s}(a)=0\\
&\iff a1_{\mathbb{Z}_r}=0 \text{ and } a1_{\mathbb{Z}_s}=0\\
&\iff r\mid a \text{ and } s\mid a\\
&\iff rs\mid a \iff a=0 \text{ in } \mathbb{Z}_{rs}.
\end{aligned}$$

Since the additive order of $1_{\mathbb{Z}_r}$ is r

since $\gcd(r,s)=1$

[Recall. If $\gcd(r,s)=1$, then $\exists\, x,y\in\mathbb{Z}$ s.t. $rx+sy=1$. So $a=arx+asy$

$r\mid a \Rightarrow a=rk$

$s\mid a \Rightarrow a=sl$

$$\begin{aligned}
&= sl\,rx+rk\,sy\\
&= rs\,(\underbrace{lx+ky}_{\text{an integer}})
\end{aligned}$$

So $rs\mid a$.]

Hence ϕ is injective. Since $|\mathbb{Z}_{rs}|=rs=|\mathbb{Z}_r\times\mathbb{Z}_s|$, we get that ϕ is also surjective. ■

Euler's phi function

Monday, August 7, 2017 10:33 PM

<u>Def.</u> Let R be a unital ring. An element $x \in R$ is called a <u>unit</u> if $\exists\, x' \in R$ such that $xx' = x'x = 1$.

The set of all the units of R is denoted by $U(R)$.

<u>Ex.</u> $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$

<u>Ex.</u> $U(\mathbb{Z}) = \{1, -1\}$

<u>Pf.</u> $a \in U(\mathbb{Z}) \Rightarrow \exists\, a' \in \mathbb{Z},\ aa' = 1$

$\Rightarrow |a|\,|a'| = 1 \Rightarrow 0 < |a| \leq 1$

$\Rightarrow |a| = 1 \Rightarrow a = 1$ or -1.

$1 \times 1 = 1$ and $(-1) \times (-1) = 1$.

So $1, -1 \in U(\mathbb{Z})$. ■

<u>Lemma.</u> $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \gcd(x,n) = 1\}$.

<u>Pf.</u> $x \in U(\mathbb{Z}_n) \Rightarrow \exists\, x' \in \mathbb{Z}_n,\ x \odot_n x' = 1$

$\Rightarrow \exists\, x' \in \mathbb{Z},\ xx' \equiv 1 \pmod{n}$

$\Rightarrow \exists\, x', k \in \mathbb{Z},\ xx' - 1 = nk$

$\Rightarrow \exists\, x', k \in \mathbb{Z},\ xx' - nk = 1 \Rightarrow \gcd(x,n) = 1$.

$\gcd(x,n) = 1 \Rightarrow \exists\, r, s \in \mathbb{Z},\ xr + ns = 1$

$\Rightarrow xr \equiv 1 \pmod{n}$

$\Rightarrow x \odot c_n(r) = 1 \Rightarrow x \in U(\mathbb{Z}_n)$. ■

<u>Def.</u> (The Euler ϕ-function) For $n \in \mathbb{Z}^+$, let $\phi(n) = |U(\mathbb{Z}_n)|$.

<u>Proposition.</u> Let $r, s \in \mathbb{Z}^+$ and suppose $\gcd(r,s) = 1$.

Then $\phi(rs) = \phi(r)\phi(s)$, where ϕ is the Euler func.

<u>Pf.</u> By the Chinese Remainder Theorem $\exists\, f: \mathbb{Z}_{rs} \xrightarrow{\sim} \mathbb{Z}_r \times \mathbb{Z}_s$.

Division ring and field

Monday, August 7, 2017 10:52 PM

$x \in U(\mathbb{Z}_{rs}) \iff f(x) \in U(\mathbb{Z}_r \times \mathbb{Z}_s)$ (why ?)

$\iff f(x) \in U(\mathbb{Z}_r) \times U(\mathbb{Z}_s)$ (why ?)

So $|U(\mathbb{Z}_{rs})| = |U(\mathbb{Z}_r)||U(\mathbb{Z}_s)|$. Hence $\phi(rs) = \phi(r)\phi(s)$. ■

Def. A unital ring D is called a division ring if

$U(D) = D \setminus \{0\}$; that means any non-zero element is a unit (has an inverse.) .

- A commutative division ring is called a field.

Exercise. Show that $H = \left\{ \begin{bmatrix} z & \omega \\ -\bar{\omega} & \bar{z} \end{bmatrix} \middle| \ \omega, z \in \mathbb{C} \right\}$ is a non-commutative division ring.

[Hint. Assuming H is a ring, let's show $U(H) = H \setminus \{0\}$.

Recall that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. So

$$\begin{bmatrix} z & \omega \\ -\bar{\omega} & \bar{z} \end{bmatrix}^{-1} = \frac{1}{z \cdot \bar{z} + \omega \cdot \bar{\omega}} \begin{bmatrix} \bar{z} & -\omega \\ \bar{\omega} & z \end{bmatrix} = \frac{1}{|z|^2 + |\omega|^2} \begin{bmatrix} \bar{z} & -\omega \\ \bar{\omega} & z \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \text{ where } a = \frac{\bar{z}}{|z|^2 + |\omega|^2} \text{ and}$$

$b = -\omega / |z|^2 + |\omega|^2$.

Notice that if $\begin{bmatrix} z & \omega \\ -\bar{\omega} & \bar{z} \end{bmatrix} \neq 0$, then $|z|^2 + |\omega|^2 \neq 0$.]