Day 20 July 2, 2024

Def. The characteristic of a ring, denoted char R, is defined to be the least positive integer n s.t. $nr = 0$, $\forall r \in R$, if such an integer exists. If no such integer exists, char $R := 0$.

$$nr := \underbrace{r + r + \cdots + r}_{n \text{ times}}$$

Prop. Let R be a ring with unity $1 \in R$. If 1 has order n, then char $R = n$.

(Proof.)

Suppose 1 has order n and pick $r \in R$. Then

$$nr = n(1r) = (n1)r = 0r = 0.$$

So char $R \leq n$.

OTOH, if $m = \text{char } R$, then $m1 = 0$.

So $m \geq n$, since n is the order of 1.

So char $R \geq n \Rightarrow$ char $R = n$. ∎

Prop. The characteristic of an I.D. is either prime or zero.

(Proof.) If $1 \in R$ is not of finite order, then char $R = 0$.

So suppose order of 1 is $n < \infty$. If n is composite, write $n = ab$, for some $1 < a, b < n$. Then

$$0 = n1 = (ab)1 = (a1)(b1).$$

Since R is an I.D., either $a1 = 0$ or $b1 = 0$.

But $1 < a, b < n$, a contradiction. ∎

Def. If R & S are rings, then a map
$$\phi: R \to S$$
is called a ring homomorphism if
$$\phi(a+b) = \phi(a) + \phi(b) \ \& \ \phi(ab) = \phi(a)\phi(b),$$
for all $a, b \in R$. A bijective ring homomorphism is a ring isomorphism. The Kernel of a ring homomorphism $\phi: R \to S$, denoted $\operatorname{Ker} \phi$, is
$$\operatorname{Ker} \phi := \{r \in R \mid \phi(r) = 0\}.$$

Prop. Let $\phi: R \to S$ be a ring homomorphism.

1. If R is a commutative ring, then $\phi(R)$ is a commutative ring.
2. $\phi(0) = 0$.
3. If R & S are rings with unity and ϕ is surjective, then $\phi(1) = 1$.
4. If R is a field and $\phi(R) \neq \{0\}$, then $\phi(R)$ is a field.

(Proof.) Exercise. ∎

Ideals & quotients

Def. An ideal of a ring R is a subring $I \subseteq R$ s.t. $rI \subseteq I$ and $Ir \subseteq I$, $\forall r \in R$.

Rmk. These are also called two-sided ideals. We won't study left ideals or right ideals.

Ex. ① Trivial ideals: $I = \{0\}$ & $I = R$

② $I = n\mathbb{Z} \subseteq \mathbb{Z}$

$\forall\, r \in \mathbb{Z}$ and $s \in I$, $s = nk$, for some $k \in \mathbb{Z}$.

Then $rs = r(nk) = n(rk) \in n\mathbb{Z}$

& $sr = (nk)r = n(kr) \in n\mathbb{Z}$,

so $rI \subseteq I$ and $Ir \subseteq I$.

③ For any commutative ring with unity R,

$$\langle a \rangle := \{ar \mid r \in R\} = (a)$$

is the ideal generated by a. We call ideals of this form principal.

Prop. Every ideal of $\mathbb{Z}$ is a principal ideal.

(Proof.) Exercise. ∎

Prop. For any homomorphism of rings $\phi : R \to S$, $\operatorname{Ker}\phi$ is an ideal of R.

(Proof.) Since ϕ is a homom. of groups, $\operatorname{Ker}\phi$ is an additive subgroup of R. It remains to check that $r(\operatorname{Ker}\phi) \subseteq \operatorname{Ker}\phi$ & $(\operatorname{Ker}\phi)r \subseteq \operatorname{Ker}\phi$, $\forall\, r \in R$. Pick $a \in \operatorname{Ker}\phi$. Then

$$\phi(ra) = \phi(r)\,\phi(a) = \phi(r)\cdot 0 = 0 \Rightarrow ra \in \operatorname{Ker}\phi$$

$$\&\quad \phi(ar) = \phi(a)\,\phi(r) = 0\cdot\phi(r) = 0 \Rightarrow ar \in \operatorname{Ker}\phi.$$

So $r(\operatorname{Ker}\phi) \subseteq \operatorname{Ker}\phi$ & $(\operatorname{Ker}\phi)r \subseteq \operatorname{Ker}\phi$. ∎

Thm. Let I be an ideal of R. Then the operation defined by

$$(r+I)(s+I) := rs+I,$$

for every $r, s \in R$, gives a valid ring structure to the quotient group R/I.

(Proof.) We know already that R/I forms an abelian group under coset addition.
We need to check that our proposed multiplication is well-defined, associative, & distributive.
We'll check well-defined.

Suppose $r_0 + I = r_1 + I$ & $s_0 + I = s_1 + I$.
Then $r_1 \in r_0 + I$ and $s_1 \in s_0 + I$,
so $\exists\, a_r, a_s \in I$ s.t.

$$r_1 = r_0 + a_r \quad \& \quad s_1 = s_0 + a_s.$$

So
$$\begin{aligned}(r_1+I)(s_1+I) &= r_1 s_1 + I \\ &= (r_0 + a_r)(s_0 + a_s) + I \\ &= (r_0 s_0 + a_r s_0 + r_0 a_s + a_r a_s) + I \\ &= r_0 s_0 + I\end{aligned}$$

$I s_0 \subseteq I$ $\quad$ $r_0 I \subseteq I$

So multiplication is well-defined. ☒

Def. If I is an ideal of R, we call R/I the quotient ring of R by I.