Thm (Wedderburn) Every finite integral domain is a field.

(Proof.) Recall:

- I.D.s are commutative rings with unity which have no zero divisors.
- A field is a commutative division ring — i.e., has unity, and every nonzero elt is a unit.

So we NTS that if D is a finite I.D., then every nonzero elt. is a unit.

Given $a \neq 0 \in D$, define $\lambda_a : D^\times \to D^\times$, where
$$d \mapsto ad$$
$$D^\times = D - \{0\}.$$

No zero divisors $\Rightarrow ad \neq 0$. Notice that λ_a is injective:
$$\lambda_a(d_1) = \lambda_a(d_2) \Rightarrow ad_1 = ad_2 \Rightarrow d_1 = d_2,$$
by left cancellation in I.D.s. Because $D^\times$ is finite, this means that λ_a is surjective, so $\exists\, b \in D^\times$ s.t.
$$\lambda_a(b) = 1. \quad \text{i.e., } ab = 1.$$

So $b = a^{-1}$, and a is a unit. ∎

Def. The characteristic of a ring R, 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, then $\operatorname{char} R := 0$.

<u>Ex.</u> $\operatorname{char} \mathbb{Z}_5 = 5$. | $\operatorname{Char} \mathbb{Z} = 0$

$(x+y)^5 = x^5 + y^5$ in $\mathbb{Z}_5$

<u>Lemma</u> Let R be a ring with unity. If $1 \in R$ has order n, then $\operatorname{char} R = n$.

(Proof.) If $1 \in R$ has order n, then

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

$\forall\, r \in R$. So $\operatorname{char} R \leq n$.

OTOH, if $m = \operatorname{char} R$, then $m1 = 0$, since $1 \in R$.

So $m \geq n$.

$\therefore \operatorname{char} R = n$. ∎

<u>Prop.</u> The characteristic of an I.D. is either prime or 0.

(Proof.) If $1 \in R$ does not have finite order, then $\operatorname{Char} R = 0$.

If 1 has order n, & $n = ab$ for some $1 < a, b < n$.

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

B/c R is an I.D., either $a1 = 0$ OR $b1 = 0$.

$\times$

So n must be prime. ∎

Ring homomorphisms

Def. If R & S are rings, then a map

$$\phi : R \to S$$

is called a ring homomorphism if

$$\phi(a+b) = \phi(a) + \phi(b) \text{ \& } \phi(ab) = \phi(a)\phi(b),$$

$\forall\, a,b \in R$. A bijective ring homom. is a ring isomorphism, and the kernel of a ring homom. ϕ 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 commutative, then $\phi(R)$ is a comm. 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. ◪

Recall: We built quotient groups by "dividing by kernels."

i.e., normal subgroups.

We'll build quotient rings in the same way.

Def. An **ideal** of a ring R is a subring $I \subseteq R$ with the property that $rI \subseteq I$ and $Ir \subseteq I$, $\forall r \in R$.

Rmk. Technically this is a "two-sided ideal."

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

② $I = n\mathbb{Z} \subset \mathbb{Z} = R$.

$\langle n \rangle$

$r(nm) = rnm = n(rm) \in n\mathbb{Z}$

$(nm)r = n(rm) \in n\mathbb{Z}$ ✓

③ For any community ring with unity R and any $a \in R$, $\langle a \rangle := \{ ar \mid r \in R \}$ is the **ideal generated by a**. Ideals of this form are called **principal ideal**.

Check: $ar \in I$, $s \in R \Rightarrow (ar)s = a(rs) \in I$

So $Is \subseteq I$

Commutativity $\Rightarrow sI \subseteq I$.

Warning: Principal ideals are more commonly denoted (a).

<u>Prop</u>. Every ideal of $\mathbb{Z}$ is a principal ideal.

(Proof.) Exercise. $\blacksquare$

<u>Prop</u>. For any ring homom. $\phi: R \to S$, $\ker \phi$ is an ideal of R.

(Proof.) We already know that $\ker \phi$ is an additive subgroup of R. Notice that if $a \in \ker \phi$ and $r \in R$, then

$$\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0$$

& $$\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0.$$

So $ra, ar \in \ker \phi$. So $r(\ker\phi) \subseteq \ker \phi$ & $(\ker \phi) r \subseteq \ker \phi$. $\blacksquare$

<u>Thm</u>. Let I be an ideal of R and define a multiplication operation on the quotient group R/I by

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

for any $r, s \in R$. This operation makes R/I into a ring.

(Proof.) Already know R/I to be an abelian group under $+$. NTS multiplication is ① well-defined

② associative

③ distributive.

$\left.\right\}$ Exercise.

Well-defined: Suppose $r_0 + I = r_1 + I$ & $s_0 + I = s_1 + I$.

Then $r_1 \in r_0 + I$ & $s_1 \in s_0 + I$, so

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

for some $a_r, a_s \in I$.

Then
$$\begin{aligned}
(r_1+I)(s_1+I) &= r_1 s_1 + I \\
&= (r_0 + a_r)(s_0 + a_s) + I \\
&= r_0 s_0 + \underbrace{a_r s_0}_{\in\, I s_0 \subseteq I} + \underbrace{r_0 a_s}_{\in\, r_0 I \subseteq I} + \underbrace{a_r a_s}_{\in\, I} + I \\
&= r_0 s_0 + I \\
&= (r_0 + I)(s_0 + I).
\end{aligned}$$

$\blacksquare$

Def. If I is an ideal of a ring R, we call R/I a **quotient ring**. We define a **canonical homomorphism**

$$\begin{aligned}
\phi_I : R &\longrightarrow R/I \\
r &\longmapsto r + I
\end{aligned}$$

associated to I.

Check: ϕ_I is a homomorphism and $\ker \phi_I = I$.