Prop: If R is a ring then:

1) $\forall a \in R$, $0a = a0 = 0$

(additive inverse)

2) $\forall a, b \in R$, $(-a)b = -(ab) = a(-b)$

3) $\forall a, b \in R$, $(-a)(-b) = ab$

4) If R has an identity then it is unique

and $-a = (-1)a$

5) $\forall a, b, c \in R$ and a is not a zero-divisor then:

if $ab = ac$ then $a = 0$ or $b = c$.

Prop: If R is a finite integral domain then it is a field.

Pf: Let $a \in R \setminus \{0\}$, consider $f: R \to R$ defined by

$f(b) = ab$. This map is injective:

If $ab = ac$ then by prop from before $b = c$.

Since R is finite, f is bijective, so $\exists b \in R$ s.t.

$ab = 1$. $\blacksquare$

Prop: If R is an ID then $\forall f, g \in R[x] \setminus \{0\}$,

$\deg(fg) = \deg f + \deg g$.

Also $(R[x])^\times = R^\times$, and $R[x]$ is an ID.

Ring homomorphisms

Def: Suppose R, S are rings. A ring homomorphism is a map $\phi : R \to S$ satisfying:

i) $\forall a, b \in R$, $\phi(a+b) = \phi(a) + \phi(b)$, and

ii) $\forall a, b \in R$, $\phi(ab) = \phi(a)\phi(b)$.

- $\ker(\phi) = \{ a \in R : \phi(a) = 0_S \}$
- If ϕ is bijective it is a ring isomorphism.

Exs: i) $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

$a \mapsto \bar{a}$

This is a ring hom. b/c add. and mult. of residue classes modulo $n\mathbb{Z}$ well-defined.

2a) $\phi : R[x] \to R$

$f(x) \mapsto f(0)$

$f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$

- $(f+g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots$

$\phi(f+g) = a_0 + b_0 = \phi(f) + \phi(g)$

- $(fg)(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots$

$\phi(fg) = a_0 b_0 = \phi(f)\phi(g)$

So this is a ring homom.

b) $\phi : \mathbb{R}[x] \to \mathbb{R}$

$\phi(a_n x^n + \cdots + a_0) = a_1$

$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{j=0}^{m} b_j x^j$

- $(f+g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots$

  $\phi(f+g) = a_1 + b_1 = \phi(f) + \phi(g)$

- $(fg)(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots$

  $\phi(fg) = a_0 b_1 + a_1 b_0 \neq a_1 b_1$

  (in general)

So ϕ is not a ring homom.

3) $\phi : \mathbb{Z} \to \mathbb{Z}$

$n \mapsto 2n$

- $\phi(m+n) = 2(m+n) = 2m + 2n = \phi(m) + \phi(n)$
- $\phi(1 \cdot 1) = 2 \neq \phi(1) \cdot \phi(1)$

This is not a ring hom.

Prop: If $\phi: R \to S$ is a ring hom. then

i) $\text{im}(\phi)$ is a subring of S,

ii) $\ker(\phi)$ is a subring of R.

Motivational: Suppose $\phi: R \to S$ is a ring hom., let $K = \ker\phi$, and let R/K be the collection of additive cosets.

- $(R/K, +)$ is a group, because $(R,+)$ is Abelian, so $(K,+) \trianglelefteq (R,+)$.
- Multiplication of cosets by the rule $(aK)(bK) = abK$ is also well defined, and $(R/K, +, \cdot)$ is a ring.

Why is mult. of cosets well defined?

Suppose $(a+x)K = aK$, $(b+y)K = bK$, for some $x, y \in R$. Then $x, y \in K$, and $(a+x)(b+y) = ab + ay + xb + xy$, and $ay + xb + xy \in K \Rightarrow abK = (a+x)(b+y)K$.

Def:
- A subring $I \subseteq R$ is a <u>left-ideal</u> if $\forall a \in R$, $aI \subseteq I$.
- A subring $I \subseteq R$ is a <u>right-ideal</u> if $\forall a \in R$, $Ia \subseteq I$.
- A subring $I \subseteq R$ is an <u>ideal</u> if $\forall a \in R$,

  $aI \subseteq I$ and $Ia \subseteq I$.

Prop: If $I \subseteq R$ is an ideal then the additive group R/I forms a ring with $(aI)(bI) = abI$.
Conversely if I is an additive subgroup and multipl. as above is well defined, then I is an ideal).