Quotient Rings and Ideal Types

Recall: (normal subgroups) If G is a group and $H \leq G$, then $H \trianglelefteq G$ if and only if $\exists$ group K and group homomorphism $\varphi : G \to K$ with $\ker(\varphi) = H$.

We would like to recover the analagous statement for rings, with Ideals in place of normal subgroups and φ a ring homomorphism.

Theorem: (Quotient ring construction)

Let R be a ring and let I be an ideal of R. Then the set of cosets of I in R forms a ring, denoted by R/I, under the operations

$$\boxed{\begin{aligned}(x+I)+(y+I)&=(x+y)+I\\ (x+I)\cdot(y+I)&=(x\cdot y)+I\end{aligned}}$$

$\forall\ x, y \in R$

proof: We know $(R,+)$ is an abelian group, hence $(I,+) \trianglelefteq (R,+)$.

Therefore, we know that R/I is a group.

R/I is abelian since R is abelian:

$$(x+I)+(y+I) = (x+y)+I$$
$$= (y+x)+I$$
$$= (y+I)+(x+I)$$

We need to show that multiplication in R/I is well-defined; that is,

if $x_1 + I = x_2 + I$ and $y_1 + I = y_2 + I$, then

$$\underbrace{(x_1+I)(y_1+I)} = \underbrace{(x_2+I)(y_2+I)}$$

$$\boxed{(x_1y_1)+I = (x_2y_2)+I}$$

Check

Since $x_1 + I = x_2 + I$, $\exists\ z \in I$,

$x_1 = x_2 + z$.

Similarly, since $y_1 + I = y_2 + I$, $\exists\ w \in I$,

$y_1 = y_2 + w$.

Then

$$x_1 y_1 - x_2 y_2$$

$$= (x_2 + z)(y_2 + w) - x_2 y_2$$

$$= x_2 y_2 + x_2 w + z y_2 + z w - x_2 y_2$$

$$= \cancel{x_2 y_2} - \cancel{x_2 y_2} + x_2 w + z y_2 + z w$$

(addition is commutative)

$$= x_2 w + z y_2 + z w.$$

Since I is an ideal and $z, w \in I$, $x_2 w, z y_2, z w \in I$.

We can conclude that

$x_1y_1 - x_2y_2 \in I$

$\Rightarrow \quad x_1y_1 + I = x_2y_2 + I$

and so multiplication in R/I

is well-defined.

We need to show associativity

of multiplication and distributivity.

These both follow from the

properties on R itself.

For example, if $x, y, z \in R$,

$$(x+I)\cdot\big((y+I)+(z+I)\big)$$

$$=(x+I)\cdot\big((y+z)+I\big)$$

$$=(x\cdot(y+z))+I$$

$$=(x\cdot y+x\cdot z)+I$$

(distributivity in R)

$$=(x\cdot y+I)+(x\cdot z)+I$$

$$=(x+I)\cdot(y+I)+(x+I)(z+I)$$

$\square$

Example 1: Let $R = K[x]$ and let

$$I = \left\{ \sum_{\boxed{i=1}}^{n} a_i x^i \;\middle|\; n \in \mathbb{N} \right\}$$

Then R/I is a ring.

Note: if $p(x), q(x) \in R$,

and $p(x) - q(x) \in I$,

then $p(x) - q(x)$ has no

constant coefficient.

$$(x^2 + x + 1) - (x^3 + x + 1) \in I$$

This implies $p(x)$ and $q(x)$ have the same constant coefficient.

Then if $\alpha \in K$ and $r(x) \in I$, then

$$(r(x)+\alpha)+I = \alpha + I$$

Therefore, the cosets of I are just

$$\{ \alpha + I \mid \alpha \in K \}.$$

So R/I should be isomorphic (as a ring) to K.

Maximal Ideals

Let R be a ring. An ideal I of R is said to be **maximal** if $I \neq R$ and if $I \subseteq J$ where J is an ideal of R, then either

$$\boxed{I = J \text{ or } J = R}$$

Theorem: (R/I for I maximal)

Let R be a commutative unital ring. Then if $I \subseteq R$ is a maximal ideal, then R/I is a field.

proof: We know R/I is a ring. Observe that if $x, y \in R$ and 1_R is the multiplicative identity of R,

$$(x+I)(1_R+I) = (x \cdot 1_R) + I$$
$$= x + I$$

and

$$(x+I)(y+I) = (x \cdot y)+I$$

R is commutative $\rightarrow$ $= (y \cdot x)+I$

$$= (y+I)(x+I)$$

Therefore, R/I is a commutative ring with multiplicative identity $1_R + I$.

We need to show that if $x \notin I$, then $x+I$ should be a unit in R/I.

Define

$$J = \{ x \cdot y + z \mid y \in R, z \in I \}.$$

Note choosing $y = 0_R$ yields

that

$$I \subseteq J.$$

Now for all $y_1, y_2 \in R$, $z_1, z_2 \in I$

$$(x \cdot y_1 + z_1) - (x \cdot y_2 + z_2)$$

$$= x \cdot \underbrace{(y_1 - y_2)}_{\in R} + \underbrace{(z_1 - z_2)}_{\in I} \in J$$

Therefore $(J,+)$ is a subgroup of $(R,+)$. Moreover, if

$s \in R$,

$$s\cdot(xy+z)$$

$$= s\cdot(xy) + s\cdot z$$

$$= x\cdot(\underbrace{sy}_{\in R}) + \underbrace{s\cdot z}_{\in I} \qquad (R \text{ commutative})$$

$$\in J$$

Since R is commutative,

$$(xy+z)\cdot s = s\cdot(xy+z) \in J.$$

So J is an ideal!

But $I \subseteq J$

and $x \in J$ since

we can choose

$y = 1_R$, $z = 0_R$.

Therefore, $J \neq I$, so

$J = R$ by maximality of I.

Then $1_R \in J$, so

$\exists\ y \in R$, $z \in I$,

$1_R = x \cdot y + z$

$\Rightarrow 1_R - x \cdot y = z \in I$

$$\Rightarrow 1_R + I = x \cdot y + I$$

$$= (x+I) \cdot (y+I)$$

$$\Rightarrow (y+I) = (x+I)^{-1}$$

So every nonzero element of R/I is invertible

$\Rightarrow R/I$ is a field.

$\square$

Principal Ideals

Let R be a ring.

$I \subseteq R$ an ideal is **principal** if $\exists$

$x \in R$, $I = \langle x \rangle$

where $\langle x \rangle$ = the smallest

ideal of R containing x.