Last updated: Nov 23, 2024

Abstract Algebra Notes Week 12 — Wed, Nov 20 2024

Sec 16.3 | Part III: Quotient rings

Notation: Let A be a subring of a ring R, $r \in R$

$$r + A \stackrel{\text{def}}{=} \{ r + a : a \in A \}$$ called <u>cosets of A</u>

$$R/A \stackrel{\text{def}}{=} \{ \text{cosets of } A \text{ in } R \}$$
$$= \{ r + A : r \in R \}$$

<u>Note</u> Since $(R, +)$ is an abelian group and every subring A is a normal subgroup of $(R,+)$, R/A is a quotient group under the operation

$$(s+A) + (t+A) = (s+t) + A$$

(Review Sec 10.1)

Q: When is R/A also a ring with multiplication defined as

$$(s+A)(t+A) = st + A \text{ ?}$$

Recall
<u>Lemma 6.3</u> (about cosets)

$s + A = t + A$ iff $t \in s + A$ iff $t - s \in A$

Thm Let I be an ideal of a ring R.

(Thm 16.29) The additive quotient group R/I is also a ring with multiplication defined by

$$(s+I)(t+I) = st + I.$$

Def This ring is called a <u>quotient ring</u>.

Idea of proof We need to show that the product $(s+I)(t+I) = st + I$ is <u>independent of the choice of coset representatives</u>.

(meaning the multiplication operation is well-defined)

Suppose $s' \in s+I$ and $t' \in t+I$.

(Goal: show $s't' + I = st + I$)

Since $s' \in s+I$, we have $s' = s+a$ for some $a \in I$.

Similarly, we have $t' = t+b$ for some $b \in I$.

Then

$$s't' = (s+a)(t+b) = st + sb + at + ab.$$

We have $sb, at, ab \in I$ because $a, b \in I$ and I satisfies the absorbing property.

So $s't' \in st + I$.

Thus $s't' + I = st + I$, as needed $\square$

See Group Quiz

Ex $\mathbb{Z}/4\mathbb{Z} = \{0+4\mathbb{Z},\ 1+4\mathbb{Z},\ 2+4\mathbb{Z},\ 3+4\mathbb{Z}\}$

is a quotient ring.

$(2+4\mathbb{Z}) + (3+4\mathbb{Z}) = 5+4\mathbb{Z} = 1+4+4\mathbb{Z} = 1+4\mathbb{Z}$

$(2+4\mathbb{Z})\ (3+4\mathbb{Z}) = 6+4\mathbb{Z} = 2+4+4\mathbb{Z} = 2+4\mathbb{Z}$

Ex Let $R = \mathrm{Mat}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z} \right\}$ and let I be the ideal of R consisting of matrices with even entries.

See Group Quiz

$$\begin{bmatrix} 7 & 8 \\ 5 & -3 \end{bmatrix} + I = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 6 & 8 \\ 4 & -4 \end{bmatrix} + I = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + I.$$

Exercise: Show $R/I = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} + I : a,b,c,d \in \{0,1\} \right\}$

so R/I has $16 = 2^4$ elts.

$\rightarrow$ Group quiz part I

Ex Let $\mathbb{R}[x]$ denote the ring of polynomials w/

(Extra) real coefficients, and consider the principal ideal $\langle x^2+1 \rangle$ generated by x^2+1

$$\mathbb{R}[x]/\langle x^2+1 \rangle = \{ g(x) + \langle x^2+1 \rangle : g(x) \in \mathbb{R}[x] \}$$

We will show later that this quotient ring is isomorphic to $\mathbb{C}$ (Cauchy 1847)

Part IV: First Isomorphism Theorem

Note (Recall from Sec 11.2)

the natural or canonical homomorphism of groups

$$\pi : R \longrightarrow R/I$$
$$r \longmapsto r + I$$

The kernel of π is I and π is surjective.

Thm (Thm 16.30) Let I be an ideal of R.

The map $\pi : R \longrightarrow R/I$
$r \longmapsto r+I$

is a ring homomorphism from R onto R/I with kernel I.

Pf The note above tells us

π is surjective, is a group homomorphism, and has kernel I.

It remains to show that π preserves multiplication.

Let $s, t \in R$. Then

$$\pi(s)\pi(t) = (s+I)(t+I) = st + I = \pi(st) \quad \square$$

First Isomorphism Thm (Thm 16.31)

Let $f: R \to S$ be a ring homomorphism.
Let K denote $\ker f$.
Let $i: R/K \to S$ be defined by

$$r+K \longmapsto f(r) \quad \text{for all } r+K \in R/K$$

Then i is an injection $R/K \hookrightarrow S$.
In particular, we have an isomorphism given by i

$$\boxed{R/K \xrightarrow{\cong} \operatorname{Im} f}$$ — the upshot

Furthermore, $f = i \circ \underbrace{\pi}_{\substack{\text{the natural onto homomorphism} \\ R \longrightarrow R/\ker f}}$

The diagram

$$\begin{tikzcd} R \arrow[r, "\pi"] \arrow[dr, "f"'] & R/\ker f \arrow[d, dashed, "i"] \\ & f(R) \end{tikzcd}$$

, called a "commutative diagram"

illustrates the 1st isomorphism Thm.

We say "the diagram commutes" to mean $f = i \circ \pi$.

<u>Note</u> This tells us that every ring homomorphism can be written as a composition

$$(\text{1-1 homomorphism}) \circ (\text{onto homomorphism}).$$

<u>Ex</u> $\varphi: \mathbb{Z}[x] \to \mathbb{Z}$ defined by $\varphi(p(x)) = \underbrace{p(0)}_{\text{the constant term of } p(x)}$

$\ker \varphi = \langle x \rangle = \{ f(x)\, x : f(x) \in \mathbb{Z}[x] \}$

By 1st Isomorphism Thm, $\mathbb{Z}[x] / \langle x \rangle \cong \mathbb{Z}$

→ Group quiz part II