

§26 Homomorphisms and factor rings

For groups

- homomorphisms $G \xrightarrow{\phi} G'$ give comparison of groups $\leadsto$ simplify structure, extract info: set equation, ...
- $\text{Ker } \phi = \{g \in G \mid \phi(g) = e_{G'}\}$ is a normal subgroup.
- $G / \text{Ker } \phi$ can be identified with $\phi[G]$
quotient image

What are the analogues for rings?

Def. R, R' : rings

- a homomorphism of rings from R to R' is given by a map (function) $\phi: R \rightarrow R'$ s.t.
- compatibility with addition $\phi(a+b) = \phi(a) + \phi(b)$
 - compatibility with multiplication $\phi(ab) = \phi(a)\phi(b)$

We've looked at this for $R[X] \rightarrow S$ (§22)In particular a hom. of rings is a hom. of additive groups $(R, +) \rightarrow (R', +)$ $\leadsto R / \text{Ker } \phi \cong \phi[R]$ as (commutative) groupsConsistency with multiplication: if $a \in \text{Ker } \phi$, $b \in R$

$$\phi(ab) = \phi(a)\phi(b) = 0_{R'}\phi(b) = 0_{R'} \Rightarrow ab \in \text{Ker } \phi$$

similarly $ba \in \text{Ker } \phi$

Def. R : ringan ideal of R is a subset $N \subset R$ such that

- $a, b \in N \Rightarrow a+b \in N$, $0 \in N$, $-a \in N$ (additive subgroup)
- $a \in N$, $b \in R \Rightarrow ab, ba \in N$

Ex. any subgroup of $\mathbb{Z}$ is also an ideal
 subgroup of $\mathbb{Z}$: $H = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$
 for some $n \in \mathbb{Z}$

$$nk \in n\mathbb{Z}, \quad l \in \mathbb{Z} \Rightarrow (nk) \cdot l = n(kl) \in n\mathbb{Z}$$

Ex. ideals of $M_2 = \{2 \times 2 \text{ matrixes}\} : \{0\} \text{ \& } M_2$

$$x = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in N \stackrel{\text{ideal}}{\subset} M_2 \rightsquigarrow \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} x \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \text{ etc.}$$

are in N

$$\text{if } \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in N \text{ then } \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

is also in N etc.

$$\rightsquigarrow N = M_2$$

Non-ex.

Prop. Def. (Cor. 26.14) ^{Def 26.15} R : ring, $N \subset R$: ideal

Then the quotient group R/N has a multiplication
 binary operation that makes it a ring

$$\text{defined by } [a][b] = [ab]$$

we say R/N is the quotient ring (factor ring) of R
 Proof. We need to check by N

- $[a][b] = [ab]$ is well-defined

i.e. if $[a] = [a']$ then $[ab] = [a'b]$, etc.

- associativity of this bin. op.

- distributive law : $([a] + [b])[c] = [a][c] + [b][c]$,
 etc.

Step 1 well-definedness

$[a] = [a']$ means $c = a - a'$ is in N

we want $[ab] = [a'b]$ i.e. $ab - a'b \in N$

$$\begin{cases} ab - a'b = (a - a')b = cb & \text{distr. law} \\ cb \in N & \text{(ideal property) from } c \in N \end{cases}$$

Step 2 associativity

$$([a][b])[c] = [ab][c] = [(ab)c]$$

$$[a]([b][c]) = [a(bc)] \quad \swarrow \text{equal}$$

Step 3 distributive law

$$\begin{aligned} ([a] + [b])[c] &= [a+b][c] = [(a+b)c] \\ [a][c] + [b][c] &= [ac] + [bc] = [ac+bc] \end{aligned} \quad \text{eg.}$$

Non-example of ideal (which are subrings)

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid a \in \mathbb{R} \right\} \subset M_2$$

$R \subset R[X]$ inclusion as constant polynomials

~~Def.~~ Ex. of quot. rings

$$R[X] \supset N = \{ a_2 X^2 + a_3 X^3 + \dots + a_k X^k \mid k \geq 2, a_i \in R \}$$

$\rightarrow$ elements of quot. ring $R[X]/N$ can be represented by $a_0 + a_1 X$

$$\begin{aligned} \text{multiplication rule: } (a_0 + a_1 X)(b_0 + b_1 X) \\ = a_0 b_0 + a_0 b_1 X + a_1 b_0 X \\ + \underbrace{a_1 b_1 X^2}_{\text{treated as } 0} \end{aligned}$$

this is called the dual number ring
(particularly when $R = \mathbb{R}$)

