New rings from old

Polynomial rings $R[x]$ or $R[x_1, x_2, \ldots, x_n]$

Matrix rings $Mat_{n\times n}(R)$

Ring of fractions $\{(a,b) : a \in R, b \in D\}$

Group rings $RG = \{r_1 g_1 + \cdots + r_n g_n : r_i \in R, g_i \in G\}$

Quotient rings R/I I ideal of R

r is a <u>unit</u> if $\exists s \in R$ s.t. $rs = 1$ or $sr = 1$

a is a <u>zero divisor</u> if $\exists s \in R$ s.t. $as = 0$ or $sa = 0$

x is <u>nilpotent</u> if $\exists m \in \mathbb{Z}^+$ s.t. $x^m = 0$

e is <u>idempotent</u> if $e^2 = e$

<u>Examples</u> $\mathbb{Z}$ - has only 1 as a unit

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ if $n = r \cdot s$ then r & s are zero divisors

if $\gcd(a,n) = 1$ then a is a unit of $\mathbb{Z}_n$

$\mathbb{Z}_2[x]/(x^2+x+1)$ - Field with 4 elements.

R - ring with 1

<u>Prop</u>: (a) $I = R$ iff I contains a unit

(b) if R is commutative. R is a field iff only ideals are 0 & R

$\forall u \in R \Rightarrow (u) = R \Rightarrow uv = 1$

Ideal is similar to notion of a normal subgroup of a group. in that quotient structure comes from cosets of ideals.

$J \subseteq R$ is an ideal if

(1) J is a subgroup of $(R,+)$

(2) $\{ra : r \in R, a \in J\} \subseteq J$ (left ideal)

$\{ar : r \in R, a \in J\} \subseteq J$ (right ideal)

("two-sided" if both left & right OR just "ideal").

$$a+J = \{a+r : r \in J\}$$

- J is an ideal of $R \Rightarrow R/J = \{a+J : a \in R\}$ is a ring

$(R/J, +_{R/J})$ is an abelian group $(a+J)+_{R/J}(b+J) = (a+b)+J$

$(R/J, \cdot_{R/J})$ is well defined

$(a+_R J)\cdot_{R/J}(b+J) = ab +_R Jb +_R aJ +_R J \cdot J = ab+J$

need to check that

There is a canonical projection

$\pi : R \to R/J$

where J is an ideal $\Leftrightarrow J = \ker\phi$ for some ϕ

There are analogues of the isomorphism theorems.

$$R \xrightarrow{\pi} R/J$$

$$\{J \subseteq K \subseteq R\} \longleftrightarrow \{\bar{K} \subseteq R/J\}$$

(K: ideal)

$$\{J \subseteq S \subseteq R\} \longleftrightarrow \{\bar{S} \subseteq R/J\}$$

(S: subring)

$$\pi^*(S) = \bigcup_{a+J \in S} (a+J) \qquad S \subseteq R/J$$

4th / (lattice iso thm)

/ ϕ is a homomorphism
$\text{im}(\phi)$ is a subring of R and
$\text{im}(\phi) \cong R/\ker(\phi)$

d/ If $A \subseteq R$ subring and B ideal of R
then $(A+B)/B \cong A/(A \cap B)$

$A+B$ is a subring of R and
$A \cap B$ is an ideal of A and

d/ If I & J are ideals of R
with $I \subseteq J$ then J/I is an ideal of R/I
and $(R/I)/(J/I) \cong R/J$

Say more about isomorphism theorems. →

but had not done previous page.

covered 11/4

Lemma: A division ring has no non-trivial ideals.
if $a \neq 0 \in J$ then $a^{-1} \in R$ ~~so~~ $a^{-1} \in J \Rightarrow r \in J \ \forall r \in R$

Wedderburn's Little theorem: finite division rings are fields.

Proofs generally req facts about cyclotomic polynomials

idea: show that if D is a finite division ring with center Z then Z is a field & D is a v.s. over Z. Use the class equation to show dim D over $Z = 1$ so $D = Z$.

Quaternions $a + bi + cj + dk \cong \left\{ \begin{bmatrix} y & z \\ -\bar{z} & \bar{y} \end{bmatrix} : y, z \in \mathbb{C} \right\}$ are not $\cong \mathbb{R}Q_8$

Ideal generated by a set $A = \{a_1, a_2, \ldots\}$

$$(A) = \bigcap_{\substack{I \text{ ideal} \\ A \subseteq I}} I$$

$RA = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n : r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}^+\}$

similarly AR and

$RAR = \{r_1 a_1 r_1' + \cdots + r_n a_n r_n' : r_i, r_i' \in R,\ a_i \in A,\ n \in \mathbb{Z}^+\}$

are the left ideal, right ideal & ideal generated by R. If R comm. $RA = AR = RAR = (A)$

I ideal of R with an identity $1 \neq 0$

I is principal if it is generated by a single element

I is finitely generated if it is generated by a finite set of elements.

I $\neq R$ is maximal if the only ideals containing I are I and R

If R is commutative, I is called prime if $I \neq R$ and if $a, b \in R$ and $ab \in I$ implies that either $a \in I$ or $b \in I$

details in book →

Prop: If R has an identity, every ideal is contained in a maximal ideal. (at least one)

Pf: Show if S is the set of ideals containing an ideal I and $\mathcal{C}$ a chain (ordered by inclusion.

$$J = \bigcup_{A \in \mathcal{C}} A$$

is a maximal ideal.

Prop: If R is commutative, M is a maximal ideal of R iff R/M is a field.

Pf: 4th (lattice) isomorphism theorem. and fact that only ideals of a field are 0 & R

Prop
Assume R is commutative. P is a prime ideal iff R/P is an integral domain.

Pf: "translate definition of prime ideal into language of quotients"

R- commutative
Prop: Every maximal ideal is a prime ideal

Pf: M maximal ⇒ R/M is a field & integral domain

R - commutative

Integral domain is a ring with no zero divisors (except 0).

Euclidean domain is an I.D. with a division algorithm that is
$\forall a, b \in R$ s.t. $b \neq 0$ there is a norm on R
$N: R \to \mathbb{Z}^+$ with $a = qb + r$ and $r = 0$ OR $N(r) < N(b)$
q is called quotient r is called remainder.

Examples: Fields are E.D. $N(a) = 0$

$\mathbb{Z}$ is a E.D. with $N(a) = |a|$

$F[x]$ where F is a Field is E.D.
$N(p(x)) =$ degree of $p(x)$