

11/2/06

R 231 # 14, 26, 27

R 239 # 12, 13

R 239 # 22, 26

Recall Rings have two operations,  $\cdot$  &  $+$   
 $(R, +)$  abelian group,  $\cdot$  associative, distributive rules

subring is subset closed under  $\cdot$ , subgroup under  $+$

division ring = ring w/  $1$ , all  $\neq 0$  elts are invertible

group of units U(R) under  $\cdot$ .

### Polynomial rings

start w/  $R$  a comm ring w/  $1$  = ring of coefficients

Def  $R[x] = \{ a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in R, n \geq 0 \}$

• usual operations

•  $R[x]$  also comm ring w/  $1$

•  $R$  is a subring, constant polynomials

Usual defs degree, coeffs, leading coeff, monic, constant term, etc...

Warning: coefficients are from  $R$ , exponents still in  $\mathbb{Z}$

$$\text{Ex } \mathbb{Z}/3\mathbb{Z}[x] \quad (x^5 - 2x^2 + x - 1) + (x^4 - x^2 + x + 2)$$

$$= x^5 + x^4 + 2x + 1$$

$$(x+1)^3 = x^3 + 1 \quad !!$$

(2)

- Prop 1.  $R[x]$  is an integral domain iff only if  $R$  is an integral domain
2. If  $R$  is an integral domain then  $\mathcal{U}(R[x]) = \mathcal{U}(R)$

## Matrix Rings

Def:  $R$  any ring,  $n > 0$ .  $M_n(R) = \{n \times n \text{ matrices w/ entries in } R\}$

operations:  $(A+B)_{ij} = A_{ij} + B_{ij}$

$$(AB)_{ij} = \sum_{k=1}^n A_{ik} B_{kj}$$

Remarks 1.  $n > 1 \Rightarrow M_n(R)$  not commutative

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ ba & 0 \end{pmatrix}$$

2.  $M_n(R)$  always has zero divisors  $n > 1$
3.  $M_n(R)$  has identity iff  $R$  does
4.  $\mathcal{U}(M_n(R)) \cong \mathcal{U}(R)$
5.  $S$  subring  $R \Rightarrow M_n(S) \subset M_n(R)$

## Group Rings

$R$  a commutative ring w/ 1

$G = \{g_1, g_2, \dots, g_n\}$  a finite group,  $g_1 = e$

Def. The group ring  $RG$  is:

elements =  $\{c_1 g_1 + c_2 g_2 + \dots + c_n g_n \mid c_i \in R\}$   
= formal "linear" combos of group elements.

operations:  $\sum_{i=1}^n a_i g_i + \sum_{i=1}^n b_i g_i = \sum_{i=1}^n (a_i + b_i) g_i$

multiplication:

- $(a_i g_i)(b_j g_j) = a_i b_j g_i g_j$
- Now use distributive laws.

$$\left( \sum_{g \in G} a_g g \right) \left( \sum_{g \in G} b_g g \right) = \sum_{g \in G} \left( \sum_{x \in G} a_x b_{x^{-1}g} \right) g \quad \text{convolution}$$

Prop.  $R = R \cdot e$  is a subring of  $RG$

2.  $G \leq U(RG)$

3.  $RG$  always has zero divisors

$$g^n = e \Rightarrow (1 - g^n) = 0$$

$$(1 + g + g^2 + \dots + g^{n-1})(1 - g) = 0$$

4.  $S$  subring  $R \Rightarrow SG$  subring  $RG$

5. In  $RG$ , polynomials w/ zero constant term are a subring  
not so here

## Homomorphisms & Quotient Rings

Def  $\varphi: R \rightarrow S$  is a ring homomorphism if

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \forall a, b \in R$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

Def Kernel =  $\{r \in R \mid \varphi(r) = 0\}$

Def If  $\varphi$  is also a bijection say it is an isomorphism and that  $R \cong S$ .

Thm 1. Image of subring under  $\varphi$  is a subring  
2.  $\text{Ker } \varphi$  is a subring.

### Quotient Rings

Let  $I$  be a subring, thus  $R/I$  is a group under  $+$ .

Def  $(a+I)(b+I) = ab+I$  multiplication on  $R/I$ .

Question When is this well-defined?

•  $(0+F)(0+F) = I$  so  $I$  must be closed under  $\cdot$ .  
 $I$  must be a subring

• Let  $i \in I$  so  $a+i = a+i+F$

$(a+i+I)(b+I) = ab+ib+I$  so must have  $ib \in F$   
similarly  $bi \in I$

5

Def. An left ideal is a subring  $I \subseteq R$  such that  
$$r \cdot i \in I \quad \forall r \in R, i \in I.$$

A right ideal is a subring  $I \subseteq R$  such that  
$$i \cdot r \in I \quad \forall r \in R, i \in I.$$

An (two-sided) ideal is both a left & right ideal.

Theorem Let  $R$  be a ring,  $I$  an ideal. Then  
the group  $R/I$  is a ring under the operations

$$(a+I) \cdot (b+I) = ab+I$$
$$(a+I) + (b+I) = a+b+I.$$

$R/I$  is a quotient ring