

p. 174

1. 0      2. 16      3. 1      4. 22      5. (1, 6)      6. (2, 2)

7. comm. ring, no unity, not a field

8. Not a ring (not a group under +)

9. comm. ring w/ unity, not a field

10. comm. ring, no unity, not a field

11. comm. ring w/ unity not a field

12. Field. (Notice that  $(a+b\sqrt{2})^{-1} = \frac{1}{a^2+2b^2} (a-b\sqrt{2})$ )

13. Not closed under mult.

14.  $\{\pm 1\}$       15.  $\{1, 1, -1, 1, 1, -1, 1, -1\}$

16.  $\{1, 2, 3, 4\}$       17. all  $q \neq 0$

20. 16 possible matrices. Units are those w/ determinant a unit, in this case that means  $\det = 1$ .

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The other 10 matrices have  $\det = 0$ .

55. Let  $x, y \in R$ .

$$(x+y)^2 = (x+y)^2 \text{ since Boolean}$$

$$x+y = (x^2 + xy + yx + y^2) \quad \text{but } x^2 = xy^2 = y$$

$$\text{Thus } xy + yx = 0.$$

Notice that setting  $x=y$  gives  $x^2 + x^2 = 0$  so  
 $x+x=0$

so actually  $x = -x \quad \forall x \in R$

In particular  $xy = -xy$  so actually

$$xy = yx$$

22. No,  $\det(A+B) \neq \det A + \det B$

27. Reasoning is bogus, just because  $AB$  is the zero matrix doesn't mean  $A$  or  $B$  must be.

Ex 
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

37.  $U = \{u \in R \mid u \text{ is invertible}\}$

a.  $1 \cdot 1 = 1$  so 1 is a unit so  $U$  has identity

b. If  $u \in U$  then  $u u^{-1} = u^{-1} u = 1$  so clearly  $u^{-1}$  is also a unit, thus  $U$  is closed under inverse.

c. Let  $u_1, u_2 \in U$ , so  $u_1, u_2$  are invertible.

$$(u_1 u_2) \cdot (u_2^{-1} u_1^{-1}) = u_1 u_2^{-1} u_1^{-1} = 1$$

$$(u_2^{-1} u_1^{-1}) (u_1 u_2) = u_2^{-1} u_2 = 1$$

Thus  $u_1 u_2$  is also a unit w/ inverse  $u_2^{-1} u_1^{-1}$ .

46. Suppose  $a^n = 0$ ,  $b^m = 0$  and  $R$  is commutative. Then

$$(a+b)^{nm} = a^{nm} + \binom{nm}{1} a^{nm-1} b + \dots + \binom{nm}{m-1} a^m b^{m-1} + \dots + b^{nm}$$

All terms have a degree  $\geq m$

or  
 $b^m \mid \dots \geq m$  so

$(a+b)^{nm} = 0$  so  $a+b$  is nilpotent.

p. 174

$$50. I_a = \{x \in R \mid ax = 0\}$$

$$0x = 0 \text{ so } 0 \in I_a.$$

$$\text{Let } x, y \in I_a \text{ so } ax = 0, ay = 0$$

$$\text{Then } a(x-y) = ax - ay = 0 - 0 = 0 \text{ so } x-y \in I_a.$$

$$a(xy) = (ax)y = 0y = 0 \text{ so } xy \in I_a.$$

Thus  $I_a$  is a subring.

5d. Ex. 18.15 shows that the map

$$\phi: \mathbb{Z}_n \rightarrow \mathbb{Z}_r \times \mathbb{Z}_s \text{ given by}$$

$\phi(n \cdot 1) = (n \cdot 1, n \cdot 1) = (n \bmod r, n \bmod s)$  is a ring isomorphism when  $\gcd(r, s) = 1$ .

$$\text{Suppose we must solve } \begin{aligned} x &\equiv m \pmod{r} \\ x &\equiv n \pmod{s}. \end{aligned}$$

$\phi$  is onto so choose  $x$  such that  $\phi(x) = (m, n)$ .

Then  $x \equiv m \pmod{r}$  and  $x \equiv n \pmod{s}$  by def. of  $\phi$ .

p. 182

$$1. \quad 0, 3, 5, 8, 9, 11$$

$$2. \quad 3x = 2 \text{ in } \mathbb{Z}_7 \quad x = 3$$

$$3x = 2 \text{ in } \mathbb{Z}_{23} \quad x = 16$$

3.  $x^2 + 2x + 2 = 0$  in  $\mathbb{Z}_6$

no solutions, poly is irreducible in  $\mathbb{Z}_6[x]$ .

4.  $x^2 + 2x + 4 = 0$  in  $\mathbb{Z}_6$

$x=2$  (factors as  $(x-2)^2$ )

5.  $\text{char } 2\mathbb{Z} = 0$ .

8.  $\text{char } \mathbb{Z}_3 \times \mathbb{Z}_3 = 3$

9.  $\text{char } \mathbb{Z}_3 \times \mathbb{Z}_4 = 12$

17 a. F b. T c. F d. F e. T f. T g. F

h. T i. F j. F

18. 1.  $\mathbb{Q}$  2.  $\mathbb{Z}$  3.  $\mathbb{Z}_6$  4.  $2\mathbb{Z}$  5.  $M_3(\mathbb{R})$

6. Matrices of form  $\begin{pmatrix} 0 & x \\ 0 & x \\ 0 & 0 \end{pmatrix}$  & entries from a field.

27. A subdomain must contain 1 and the char. By Thm 18.15  
the char is determined by which multiples

$n \cdot 1$  are zero, and this

is the same regardless of whether we consider 1 as  
an element of  $D$  or of the subdomain.

30. a.

$S$  is already an abelian group since it is a direct product of two abelian groups w/ usual operation.

Distributive law

$$\begin{aligned}
 (r_1, n_1) \cdot ((r_2, n_2) + (r_3, n_3)) &= (r_1, n_1) \cdot (r_2 + r_3, n_2 + n_3) \\
 &= (r_1(r_2 + r_3) + n_1 \cdot (r_2 + r_3) + (r_2 + r_3) \cdot r_1, n_1(n_2 + n_3)) \\
 &= (r_1 r_2 + r_1 r_3 + n_1 r_2 + n_1 r_3 + r_2 r_1 + r_3 r_1, n_1 n_2 + n_1 n_3) \\
 &= (r_1 r_2 + n_1 r_2 + r_2 r_1 + r_1 r_3 + n_1 r_3 + r_3 r_1, n_1 n_2 + n_1 n_3) \\
 &= (r_1 r_2 + n_1 r_2 + r_2 r_1, n_1 n_2) + (r_1 r_3 + n_1 r_3 + r_3 r_1, n_1 n_3) \\
 &= (r_1, n_1) \cdot (r_2, n_2) + (r_1, n_1) \cdot (r_3, n_3)
 \end{aligned}$$

So left dist. law holds. The other one is essentially the same.

Associative Law

- Notice that the  $n_i$ 's are integers, they commute w/ the  $r$ 's since  $n \cdot r$  is notation for  $r + r + \dots + r$ .

$$\begin{aligned}
 ((r_1, n_1) \cdot (r_2, n_2)) \cdot (r_3, n_3) &= (r_1 r_2 + n_1 r_1 + n_2 r_2, n_1 n_2) \cdot (r_3, n_3) \\
 &= (r_1 r_2 r_3 + n_3 r_1 r_2 + n_3 n_1 r_1 + n_3 n_2 r_2 + n_1 n_2 r_3, n_1 n_2 n_3) \\
 &\quad + n_3 r_1 r_3 + n_1 r_2 r_3
 \end{aligned}$$

$$\begin{aligned}
 (r_1, n_1) \cdot [(r_2, n_2) \cdot (r_3, n_3)] &= (r_1, n_1) \cdot (r_2 r_3 + n_3 r_2 + n_2 r_3, n_2 n_3) \\
 &= (r_1 r_2 r_3 + n_1 r_2 r_3 + n_1 n_3 r_2 + n_1 n_2 r_3 + n_2 n_3 r_1, n_1 n_2 n_3) \\
 &\quad + n_3 r_1 r_2 + n_2 r_1 r_3 \\
 &\text{same! (remember } n\text{'s commute w/ } r\text{'s)}
 \end{aligned}$$

b.  ~~$(r_1, n_1) \cdot (0, 1) = (r_1, n_1)$~~

$$(r_1, n_1) \cdot (0, 1) = (r_1, n_1) = (0, 1) \cdot (r_1, n_1)$$

so  $(0, 1)$  is identity

c.  $n \cdot (r_1, n_1) = (nr_1, n \cdot n_1) = 0$  iff  $nr_1 = 0$   
and  $n \cdot n_1 = 0$ .

But  $r_1 \in R$ ,  $n \in \mathbb{Z} \subset \mathbb{Z}_n$  and  $\text{char } R = 0$  or  $n$

so characteristics agree.

d.  $\phi$  is 1-1 is obvious.

$$\phi((r_1, r_2)) = (r_1, 0) + (r_2, 0) = (r_1 + r_2, 0) = \phi((r_1 + r_2))$$

$$\phi((r_1, r_2)) = (r_1, r_2, 0) = (r_1, 0) + (r_2, 0) = \phi(r_1) + \phi(r_2)$$