

1. (a) Let  $0_R$  be the additive identity of  $R$ .

$$a \odot 0_R = a \Leftrightarrow a + 0_R - 1 = a \Leftrightarrow (-a) + a + 0_R - 1 = (-a) + a$$

$$\Leftrightarrow 0_R - 1 = 0 \Leftrightarrow 0_R = 1$$

$$\therefore 0_R = 1$$

(b) Yes.  $a \odot 1_R = a \mid_R - a - 1_R + 2 = a$ .

$$\rightarrow a \mid_R - 2a - 1_R + 2 = 0$$

$$\rightarrow 1_R(a-1) - 2(a-1) = 0$$

$$\rightarrow (1_R - 2)(a-1) = 0$$

$\rightarrow 1_R = 2$  or  $a=1$  (Since  $\mathbb{Z}$  is an integral domain.)  
 $\rightarrow 1_R = 2$  (Since  $a$  is a nonzero element.)

(c) By (a),  $0_R = 1$ .

$a \odot b = 1$  then  $ab - a - b + 2 = 1 \Rightarrow (a-1)(b-1) = 0$  In  $\mathbb{Z}$

forcing  $a=1$  or  $b=1$ . Since  $\mathbb{Z}$  is an integral domain. Thus  $R$  is an integral domain.

2. (a) None.

(b)  $3, 2, 4, 6$ .

(c)  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  s.t.  $ad - bc = 0$ .

$a, b, c, d \in \mathbb{R}$ , not all of them are zeros.

(d)  $(0,1), (0,2), (1,0), (2,0), (1,2), (2,1)$

(e) None

14

3. (a) Let  $a, b, c \in F$  s.t.  $c = a - b$ . and let  $f(a) = f(b)$ .

Since  $f$  is a nonzero homomorphism,

$$f(c) = f(a - b) = f(a) - f(b) = 0 \rightarrow \text{this means that } c = 0.$$

Therefore,  $a = b$ .

So what?

(b) There is none.

(c)



4. (a) Consider <sup>monic</sup> polynomials of degree 2 that are reducible in  $\mathbb{Z}_p[x]$ .

$(x+a)(x+b)$  would be the form.

(i)  $a=b$

There are  $p$  situations.

(ii)  $a \neq b$ .

There are  $p(p-1)/2$  situations.

By (i), (ii) there are  $p + \frac{p(p-1)}{2} = \frac{p(p+1)}{2}$  <sup>monic</sup> reducible polynomials of degree 2.

The number of monic polynomials of degree 2 is  $p^2$  since we can think that the form would be  $x^2 + cx + d$ .

Thus, there are  $p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}$  monic irreducible polynomials of degree 2.

(b) Let  $f(x) = x^2 - x$  then we can see that.

$$f(0) = 0$$

$$f(3) = 3^2 - 3 = 0$$

$$f(6) = 6^2 - 6 = 0.$$

$$f(1) = 1^2 - 1 = 0$$

$$f(4) = 4^2 - 4 = 0$$

$$f(2) = 2^2 - 2 = 0$$

$$f(5) = 5^2 - 5 = 0$$

By factor theorem  $x^2 - x = x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$ .



5. Lemma. Every irreducible polynomial  $p(x) \in \mathbb{R}[x]$  is of degree 1 or 2.

pf) Factorize  $p(x)$  over  $\mathbb{C}$ . Let  $\alpha \in \mathbb{C}$  be a root of  $p(x)$ . Then  $\bar{\alpha}$  is also a root of  $p(x)$  since it is the only way that the coefficients of  $p(x)$  could all be in  $\mathbb{R}$ .

If  $\alpha = \bar{\alpha}$ , then  $\alpha \in \mathbb{R}$  and  $(x - \alpha) \mid p(x)$ . Since  $x - \alpha \in \mathbb{R}[x]$ ,  $p(x)$  is an associate of  $x - \alpha$ .

If  $\alpha \neq \bar{\alpha}$ , then  $(x - \alpha)(x - \bar{\alpha}) \mid p(x)$ . Since  $x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} \in \mathbb{R}[x]$ ,  $p(x)$  is an associate of  $(x - \alpha)(x - \bar{\alpha})$ .

By Lemma, we can say as below.

①  $ax^2 + bx + c$  s.t.  $a, b, c \in \mathbb{R}$  and  $b^2 - 4ac < 0$  when  $a \neq 0$ .

②  $dx + e$  s.t.  $d, e \in \mathbb{R}$  when  $d \neq 0$ .

① and ② are irreducible polynomials.



6. (a)  $U_{27} = \{a \mid (n, a) = 1, 0 \leq a \leq n\}$

$= \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$

Thus  $|U_{27}| = 18$

(b) By (a), Yes. We can see that  $8^6 = 1$ .

Thus the order of 8 is 6.

7. (a)  $aba^{-1} = b^2 \rightarrow ab = b^2a$

(b) By (a),  $a^2b = b^{32}a^2$  and  $a^2 = e$  (e is the identity).

$\rightarrow b = b^{31} \rightarrow e = b^{31}$  thus  $|b| = 31$