

## Homework 4 Solutions

### Ch 12: 1, 2, 9, 22 - 26, 60, 63

1.  $2 \times 2$  matrices over  $\mathbb{Z}_2$  is finite and non-commutative. Since

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ while } \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$2 \times 2$  matrices with entries from  $2\mathbb{Z}$  would be an example of infinite, non-commutative with no unit.

2. Consider  $R = 2\mathbb{Z}_{10} = \{0, 2, 4, 6, 8\}$ . 6 is unity since  $(5+1)(2m) = 10m + 2m = 2m \pmod{10}$  (or by inspection if you prefer). To see that each element is a unit, check  $2 \cdot 8 = 6 \pmod{10}$ ,  $4 \cdot 4 = 6 \pmod{10}$ .

9. This is sort of a standard type of result you should expect. If  $R = \bigcap R_i$  then we need to show closure under operations, but this is trivial since each  $R_i$  is closed.

22. Let  $u, v \in U(R)$ , then  $(u \cdot v) \cdot (v^{-1} \cdot u^{-1}) = (u(vv^{-1})u^{-1}) = u1u^{-1} = uu^{-1} = 1$ , so  $v^{-1}u^{-1} = (uv)^{-1}$  and thus  $uv$  is a unit if  $u$  and  $v$  are such. The rest is even simpler.

23. Determine  $U(\mathbb{Z}[i])$  we need  $(a+bi)(c+di) = 1$  so  $(ac-bd) = 1$  while  $(ad+bc) = 0$ . The only units are  $\pm 1$  and  $\pm i$  are units. That these are the only units can be seen thus

$$(a+bi)^{-1} = \frac{a-bi}{a^2+b^2}$$

so  $a+bi \in \mathbb{Z}[i]$  iff  $\frac{a}{a^2+b^2}, \frac{b}{a^2+b^2} \in \mathbb{Z}$ , for this we must have  $a = \pm 1$  and  $b = 0$  or  $b = \pm 1$  and  $a = 0$ .

24. Show that  $U(R_1 \times R_2 \times \cdots \times R_n) = U(R_1) \times U(R_2) \times \cdots \times U(R_n)$ .

It would suffice to consider  $n = 2$  and use induction. Suppose  $(r, s) \in U(R_1 \times R_2)$  so there is  $(r', s')$  such that  $(r, s)(r', s') = (1, 1)$ , but then  $(r, s) \in U(R_1) \times U(R_2)$ . Essentially the same argument works in the other direction.

25. Determine  $U(\mathbb{Z}[x])$ . Let  $p = a + p_1(x)x$  and  $q = b + q_1(x)x$  then  $pq = (ab + (aq_1(x) + bp_1(x))x + p_1(x)q_1(x)x^2 = 1$  iff  $(a, b) = \pm(1, 1)$ . So  $U(\mathbb{Z}[x]) = U(\mathbb{Z})$ .

26. Determine  $U(\mathbb{R}[x])$ . This is like the above, the only  $f \in \mathbb{R}[x]$  with a multiplicative inverse is  $f = a \in \mathbb{R}^* = U(\mathbb{R})$ . So  $U(\mathbb{R}[x]) = U(\mathbb{R})$ .

60. Show that  $4x^2 + 6x + 3$  is a unit in  $\mathbb{Z}_8[x]$ .

$$(4x^2 + 6x + 3)(2x + 3) = 8x^3 + 12x^2 + 6x + 12x^2 + 18x + 9 = 8x^2 + 24x^2 + 24x + 9 \pmod{8} = 1$$

**63.**  $A \in M_2(\mathbb{Z})$  We know  $\det(AB) = \det(A)\det(B)$  and so if  $AB = I$ , then  $\det(A)\det(B) = 1$  and as  $\det(A), \det(B) \in \mathbb{Z}$  it must be that  $\det(A) = \pm 1$ .

## Ch 13: 7, 12, 17, 30, 43, 49, 51, 56, 57, 64

**7.** Let  $R$  be a finite commutative ring with unity. Show that every  $r \in R$  is either a unit or a 0-divisor.

Suppose  $r$  is not a zero-divisor. Consider the map  $s \mapsto rs$ . If  $rs = rs'$ , then  $rs - rs' = r(s - s') = 0$ . If  $s \neq s'$  for any  $s, s' \in R$ , then  $r$  is a 0-divisor. Else, the map is 1-1 and hence onto, so  $rs = 1$  for some  $s$ . (**A counting argument.**)

Any time you have an integral domain that is not a field you have non-zero-divisor non-unit elements, like 2 in  $\mathbb{Z}$ .

**Note** This shows that every finite integral domain is a field!

**12.** In  $\mathbb{Z}_7$  give interpretations for  $1/2$ ,  $-2/3$ ,  $\sqrt{-3}$ , and  $-1/6$ .

$2 \cdot 4 = 1 \pmod{7}$  so  $4 = 1/2 \pmod{7}$ .

$1/3 = 5 \pmod{7}$  since  $3 \cdot 5 = 15 = 1 \pmod{7}$  and so  $2/3 = 10 = 3 \pmod{7}$  and this makes sense as  $3 \cdot 3 = 9 = 2 \pmod{7}$  and so  $-2/3 = -3 = 4 \pmod{7}$ .

$-3 = 4 \pmod{7}$  so  $2 = \sqrt{-3} \pmod{7}$ , that is,  $2^2 = 4 = -3 \pmod{7}$ . What about  $-2 = 5 \pmod{7}$ ?  $(-2)^2 = 5^2 = 25 = 4 \pmod{7}$ , do yes, 2 and  $-2$  both satisfy  $x^2 = -3$ .

$1/6 = 6$  since  $6 \cdot 6 = 1 \pmod{7}$  and so  $-1/6 = -6 = 1 \pmod{7}$ .

All pretty strange:)

**17.** In an integral domain if  $a_1 a_2 \cdots a_n = 0$ , then for some  $i$ ,  $a_i = 0$ . So if  $r^n = 0$ , then  $r = 0$ .

**30.**  $\mathbb{Q}[\sqrt{d}]$  is a field for  $d$  an integer. Closure under addition and multiplication are obvious and

$$a + b\sqrt{d} \cdot \frac{a - b\sqrt{d}}{a^2 - b^2 \cdot d} = 1$$

so

$$(a + b\sqrt{d})^{-1} = \frac{a}{a^2 - b^2 \cdot d} - \frac{b}{a^2 - b^2 \cdot d} \sqrt{d}$$

**43.** Show that  $\mathbb{Z}_7[\sqrt{3}]$  is a field. The additive group part is clear essentially being isomorphic to  $\mathbb{Z}_7 \times \mathbb{Z}_7$ .

The multiplication is  $(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}$ . This will satisfy all the rules except possibly having inverses, so consider

$$1 = (a + b\sqrt{3}) \left( \frac{a - b\sqrt{3}}{(a + b\sqrt{3})(a - b\sqrt{3})} \right)$$

This will be true if  $\mathbb{Z}_7[\sqrt{3}]$  is a field. So the proposed inverse of  $a + b\sqrt{3}$  is

$$\left( \frac{a}{a^2 - 3b^2} \right) - \left( \frac{b}{a^2 - 3b^2} \right) \sqrt{3}$$

For this to work we need that  $a^2 - 3b^2 \neq 0$  in  $\mathbb{Z}_7$  when  $a$  and  $b$  are not both 0.

Suppose  $a^2 = 3b^2 \pmod{7}$ . In this case we would have  $3 = (a/b)^2$ , so we can't have  $a^2 = 3b^2$  unless 3 is a square in  $\mathbb{Z}_7$ .

We can just check that  $m^2 \pmod{7} \neq 3$  for  $m = 0, 1, \dots, 6$ .

This indicates what is needed in general,  $\mathbb{Z}_p[\sqrt{k}]$  is a field provided that  $k$  is not a square in  $\mathbb{Z}_p$ .

**49.** Let  $x_1, \dots, x_n$  belong to a ring with prime characteristic  $p$ . First notice  $(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \dots + \binom{p}{p-1}xy^{p-1} + y^p$ . All of the middle terms have a factor of  $p$  and hence become 0. Thus  $(x+y)^p = x^p + y^p$ . Now then  $(x+y)^{p^2} = ((x+y)^p)^p = (x^p + y^p)^p = (x^p)^p + (y^p)^p = x^{p^2} + y^{p^2}$ , etc. By induction on  $m$ ,  $(x+y)^{p^m} = x^{p^m} + y^{p^m}$ .

Now  $((x_1 + x_2) + x_3)^{p^m} = (x_1 + x_2)^{p^m} + x_3^{p^m} = x_1^{p^m} + x_2^{p^m} + x_3^{p^m}$ . So by induction on  $k$ ,

$$(x_1 + \dots + x_k)^{p^m} = x_1^{p^m} + \dots + x_k^{p^m}$$

**Questions** Where did we use  $p$  is prime? Where did we use commutativity?

This shows we need the "prime" assumption: In  $\mathbb{Z}_4$  we have  $(1+1)^4 = 2^4 = 0 \neq (1^4 + 1^4) = 2$ .

What about the commutativity issue? Consider  $M_2(\mathbb{Z}_2)$ . Let  $x = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$  and  $y = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ , then

$$\begin{aligned} x^2 &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \\ y^2 &= \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ x^2 + y^2 &= I + I = O \\ x + y &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ (x + y)^2 &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \end{aligned}$$

So  $x^2 + y^2 \neq (x+y)^2$ .

**51.** Let  $F$  be a finite field of character  $p$  (we know  $p$  is a prime). What we need to see is the  $|F| = p^m$  for some  $m$ . Suppose  $q \mid |F|$  for some  $q \neq p$ , then there is a  $g \in F$  with  $|g| = q$ , that is  $qg = g + g + \dots + g = 0$ , but then  $g \cdot (q \cdot 1) = 0$  and so  $q \cdot 1 = 0$ , but then  $p \mid q$ . So  $|F| = p^m$  for some  $m$ .

**56.** Find all solutions to  $x^2 - x + 2$  over  $\mathbb{Z}_3[i]$ .

We do have  $x^2 - x + 2 = x^2 + 2x - 1 = (x+1)^2 - 2 = (x+1)^2 + 1$  so  $x = 1 \pm i$ . So  $x = -1 - i = 2 + 2i$  and  $x = -1 + i = 2 + i$  are the two roots.

**57.** Consider  $x^2 - 5x + 6 = (x-2)(x-3) = 0$  Find all solutions in  $\mathbb{Z}_7, \mathbb{Z}_8, \mathbb{Z}_{12}$ , and  $\mathbb{Z}_{14}$ .

$\mathbb{Z}_7$  is a field so  $x = 2$  and  $x = 3 \pmod{7}$  is the only solution.

In  $\mathbb{Z}_8$ , notice that  $(x-2)(x-3) = (x+6)(x+5)$  so we have

$x$	0	1	2	3	4	5	6	7
$x^2 - 5x + 6$	$6 \cdot 5 = 6$	$7 \cdot 6 = 2$	$0 \cdot 7 = 0$	$1 \cdot 0 = 0$	$2 \cdot 1 = 2$	$3 \cdot 2 = 6$	$4 \cdot 3 = 4$	$5 \cdot 4 = 4$

So in  $\mathbb{Z}_8$  we have 2, 3 as roots.

Note that  $x^2 - 1 = (x - 1)(x + 1)$  has roots 1 and  $-1 = 7 \pmod{8}$  as indicated in the factorization, but also 3 and 5. So in  $\mathbb{Z}_{p^k}$  an  $n^{\text{th}}$ -degree polynomial may have more than  $n$  roots.

$\mathbb{Z}_{12} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3$  so we can solve these separately. In  $\mathbb{Z}_3$  we have  $x^2 - 5x + 6 = x^2 + x = (x)(x + 1) = (x)(x - 2)$  in  $\mathbb{Z}_3$  so  $x = 0$  and  $x = 2$  in  $\mathbb{Z}_3$ . In  $\mathbb{Z}_4$  we have  $x^2 - 5x + 6 = x^2 + 3x + 2 = (x + 2)(x + 1)$  so  $x = -2, x = -1$ , that is  $x = 2$  and  $x = 3$ . Thus the solutions are  $(2, 0), (2, 2), (3, 0), (3, 2)$ , these correspond to 6, 2, 3, 11 in  $\mathbb{Z}_{12}$ .

$\mathbb{Z}_{14} \simeq \mathbb{Z}_2 \times \mathbb{Z}_7$  and in  $\mathbb{Z}_2$   $x^2 - 5x + 6 = x^2 + x = (x)(x + 1) = (x)(x - 1)$  so we have 0, 1 for roots and in  $\mathbb{Z}_7$  we have 2 and 3 so we have  $(0, 2), (0, 3), (1, 2)$ , and  $(1, 3)$  which corresponds to 2, 3, 9, 10.

**64.** In a finite field  $F$  with  $|F| = n$ ,  $|F^*| = n - 1$  and  $x^{|F^*|} = 1$  for all  $x \in F^*$ . (Since in any group  $G$ ,  $g^{|G|} = e$ .)

## Ch 14: 10, 22, 42, 48, 51, 55, 60, 62, 67, 73, 78, 80

**10.** In  $\mathbb{Z}[x]$  show that  $(2x, 3) = (x, 3)$ . Clearly,  $2x \in (x, 3)$  so  $(2x, 3) \subseteq (x, 3)$ . Conversely,  $3x \in (2x, 3)$  so  $x = 3x - 2x \in (2x, 3)$ .

**22.** Let  $R$  be a finite commutative ring and  $I$  be prime. Then  $R/I$  is a finite integral domain and hence a field. We have shown before that any finite integral domain is a field, the reason is simple, let  $a$  be a non-zero element of a finite integral domain, then  $ab = ac \iff a(b - c) = 0 \iff b - c = 0 \iff b = c$ , so the map  $c \mapsto ac$  is 1-1 and hence onto. So  $ac = 1$  for some  $c$ .

**42.** Show that  $\mathbb{R}[x]/(x^2 + 1)$  is a field. Consider  $\phi : \mathbb{R}[x] \rightarrow \mathbb{C}$  given by  $x \mapsto i$  (or  $x \mapsto -i$ ) and extended uniquely to  $\mathbb{R}[x]$ . Clearly,  $\phi$  is a homomorphism and  $p(x) \in \ker(\phi) \iff p(i) = 0 \iff (x - i) \mid p(x)$ . Since  $p(x) \in \mathbb{R}[x]$   $-i$  must also be a root, namely,  $z$  is a root of  $p(x)$  iff  $\bar{z}$  is a root of  $\bar{p}(z)$ , so  $(x - i)(x + i) = x^2 + 1 \mid p(x)$ . So  $(x^2 + 1) = \ker(\phi)$ .

**48.** Let  $I = \{a + bi \mid a, b \in 2\mathbb{Z}\} = 2\mathbb{Z}[i] = (2)$ . So  $I$  is clearly an ideal. There will be four classes,  $I, 1 + I, i + I, (1 + i) + I$  and  $\mathbb{Z}[i]/I$  will be isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_2$ . This is not an integral domain, since  $(1 + i)(1 + i) = (1 - 1) + 2i \in 2\mathbb{Z}[i]$ .

**51.** In  $\mathbb{Z}[x]$  show that  $I = \{f(x) \mid f(0) \text{ is even}\} = (x, 2)$ . It is clear that  $f(x) \in I \iff f(x) = p(x) \cdot x + a$  for  $a \in 2\mathbb{Z}$ . This has just two elements,  $I$  and  $1 + I$ , and  $\mathbb{Z}[x]/I$  is isomorphic to  $\mathbb{Z}_2$ . This is a field, so  $I$  is maximal, hence prime.

**55.** In  $\mathbb{Z}_5[x]$  let  $I = (x^2 + x + 2)$  find a multiplicative inverse to  $(2x + 3) + I$ . We are looking for  $p(x)$  so that  $(2x + 3)p(x) = r(x)(x^2 + x + 2) + 1$ . Solved by "guessing"  $(2x + 3)(3x + 1) = 6x^2 + 11x + 3 = (x^2 + x + 2) + 1$ .

**60.** In a principal ideal domain, show that every prime ideal is maximal. Let  $(p)$  be prime, if  $(p)$  were not maximal, then, there is  $J$  so that  $(p) \subset J \subset R$ . But  $J = (q)$  since we are in a principal ideal domain and hence  $q \mid p$ , and so  $p = q \cdot r$ . But then  $p \mid q$  or  $p \mid r$ . Suppose  $p \mid r$ , then  $r = p \cdot d$  and we have  $p = q \cdot r = q \cdot p \cdot d$  so  $p \cdot (1 - q \cdot d) = 0$  and thus  $q \cdot d = 1$  and so  $q$  is a unit. This is a contradiction since  $(q) \neq R$ . A similar argument works if  $p \mid q$ . In this case, we get  $r$  as a unit, so that  $(p) = (q)$ , again a contradiction.

**62.** Showing that  $N(A)$  is an ideal is straightforward. Suppose  $r, s \in N(A)$  so that  $r^n, s^m \in A$ ; let  $k = \max\{m, n\}$ , then  $(r + s)^k = \sum_{i=0}^k \binom{k}{i} r^i s^{k-i}$ . In every term either  $r^i$  or  $s^{k-i}$  will be in

$A$  since  $i \geq n$  or  $k - i \geq m$  for all  $i$ . So  $(r + s)^k \in A$ . That  $r \cdot s \in N(A)$  for all  $r \in R$  and  $s \in N(A)$  is simpler.

Here is even more!

$$N(A) = \bigcap \{J \supset A \mid J \text{ is prime}\}$$

First notice that for any  $r \in R$  with  $r^n \in A$ , if  $A \subset J$  and  $J$  is prime, then  $r^n \in J$  and hence  $r \in J$  (as  $J$  is prime). So we have containment  $N(A) \subseteq \bigcap \{J \supset A \mid J \text{ is prime}\}$ .

Now suppose  $r \notin N(A)$ , then we want to find a prime ideal  $J$  with  $A \subset J$  and  $r \notin J$ . Look at  $\mathcal{I}$  being the set of all ideals of  $R$  such that  $r^n \notin I$  for any  $n$ . We can find a maximal such ideal  $J$ , we just need to show that  $J$  is prime. Suppose  $a \cdot b \in J$  and  $a, b \notin J$ . By maximality, this means that  $r^n \in (a) + J$  and  $r^m \in (b) + J$  so  $r^n = at + s$  and  $r^m = bt' + s'$  for  $t, t' \in R$  and  $s, s' \in J$ . This means  $r^{n+m} = abtt' + ats' + bt's + ss' \in J$  which is a contradiction, so  $a \in J$  or  $b \in J$ .

**67.** First notice that by the polynomial division algorithm  $p(x) = ax + b \bmod x^2 + x + 1$  for all  $p(x) \in \mathbb{Z}_2[x]$ . So the elements of the field are  $0, 1, x$ , and  $1 + x$  here  $x(1 + x) + (x^2 + x + 1) = 1 + (x^2 + x + 1)$  so  $x^{-1} = 1 + x$  and we see that  $\mathbb{Z}_2[x]$  is a field.

**73.** Show that if  $R$  is a PID, then  $R/I$  is a PID for all ideals  $I \subset R$ . Let  $J \subset R/I$  be an ideal, then  $J = J'/I$  for  $J' = \{r \in R \mid r + I \in J\}$ . We know  $J' = (p)$  in  $R$  and so  $J = (p)/I = (p/I)$ . So  $R/I$  is a PID.

**78.** Show that the characteristic of  $R = \mathbb{Z}[i]/(a + bi)\mathbb{Z}[i]$  divides  $a^2 + b^2$ .

In [this note](#) there is a lot of information, for this problem the relevant thing is this:

$\phi : \mathbb{Z}[i] \rightarrow \mathbb{Z}_{a^2+b^2}$  defined by  $\phi(z) = \text{Re}(z\overline{(a+bi)}) \bmod (a^2 + b^2) = (ca + db) \bmod (a^2 + b^2)$ , where  $z = c + di$ , is a homomorphism of the additive group structure with  $\ker(\phi) = (a + bi)\mathbb{Z}[i]$ . Then the first homomorphism theorem gives

$$\mathbb{Z}[i]/(a + bi)\mathbb{Z}[i] \simeq \text{Im}(\phi) < \mathbb{Z}_{a^2+b^2}$$

Thus  $\mathbb{Z}[i]/(a + bi)\mathbb{Z}[i]$  is cyclic with order dividing  $a^2 + b^2$  and so  $|1| = \text{char}(\mathbb{Z}[i]/(a + bi)\mathbb{Z}[i]) \mid a^2 + b^2$ .

So the thing to show is that  $\phi$  is a homomorphism and  $\ker(\phi)$  is as advertised. Let  $\xi = a + bi$  to minimize space and writing, then

$$\begin{aligned} \phi(z + w) &= \text{Re}((z + w)\bar{\xi}) \bmod |\xi|^2 = \text{Re}(z\bar{\xi} + w\bar{\xi}) \bmod |\xi|^2 = (\text{Re}(z\bar{\xi}) + \text{Re}(w\bar{\xi})) \bmod |\xi|^2 \\ &= \text{Re}(z\bar{\xi}) \bmod |\xi|^2 + \text{Re}(w\bar{\xi}) \bmod |\xi|^2 = \phi(z) + \phi(w) \end{aligned}$$

Well, that was easy. Now notice  $(a + bi)\mathbb{Z}[i] \subseteq \ker(\phi)$  since

$$\phi(\xi) = \text{Re}(\xi\bar{\xi}) \bmod |\xi|^2 = |\xi|^2 \bmod |\xi|^2 = 0 \bmod |\xi|^2$$

Finally, if  $z = c + di$  we need  $\phi(z) = 0 \implies z \in (a + bi)\mathbb{Z}[i]$ , said another way we need to show

$$a^2 + b^2 \mid ca + bd \implies a + bi \mid c + di$$

Now

$$\frac{c+di}{a+bi} = \frac{(c+di)(a-bi)}{(a+bi)(a-bi)} = \frac{ac+bd}{a^2+b^2} + i\frac{ad-bc}{a^2+b^2}$$

So it would suffice to have

$$a^2 + b^2 \mid ac + bd \implies a^2 + b^2 \mid ad - bc$$

This turns out to follow from a nice fact to know:

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

This is clear as it immediately follows from  $|z||w| = |zw|$  in  $\mathbb{C}$ , by squaring both sides!

**80.** Let  $R = \mathbb{Z}[\sqrt{-5}]$  and  $I = \{a + b\sqrt{-5} \mid a - b \text{ is even}\}$ . Show that  $I$  is maximal.

Consider the map

$$\phi(a + b\sqrt{-5}) = \begin{cases} 1 & a - b \text{ is odd} \\ 0 & a - b \text{ is even} \end{cases}$$

Check that  $\phi : \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{Z}_2$  is a surjective homomorphism. The main thing is multiplication where we have

$$\phi((a + b\sqrt{-5})(c + d\sqrt{-5})) = \begin{cases} 1 & (ac - 5bd) - (ad + bc) \text{ is odd} \\ 0 & (ac - 5bd) - (ad + bc) \text{ is even} \end{cases}$$

We have

$$(ac - 5bd) - (ad + bc) = (ac + bd) - (ad + bc) - 6bd = a(c - d) + b(d - c) - 6bd = (a - b)(c - d) - 6bd$$

So  $(ac - 5bd) - (ad + bc)$  is odd only when  $(a - b)$  and  $(c - d)$  are odd. This is what we need here.

Since  $\mathbb{Z}_2$  is a field,  $I$  is maximal.

## Ch 15: 12, 14, 26, 31, 34, 38, 40, 44, 46, 50, 65, 67

**12.** The point here is that if  $\phi : m\mathbb{Z} \rightarrow n\mathbb{Z}$ , then

$$\phi(mk) = \underbrace{\phi(m) + \cdots + \phi(m)}_{k \text{ times}} = k\phi(m)$$

so clearly everything is determined by  $\phi(m)$  and if we hope to be onto, then  $\phi(m) = \pm n$  must hold. But then we have

$$\phi(m \cdot (mn)) = mn\phi(m) = mn^2 \neq n(n^2) = n\phi(m^2) = \phi(m^2n)$$

So the map cannot work on products.

**Note:** The following argument does not work. Since  $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m \not\cong \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ ,  $m\mathbb{Z} \not\cong n\mathbb{Z}$ . For this, we would require that

$$I \simeq J \implies R/I \simeq R/J$$

which is not true, for example, in  $R = \mathbb{Z}[x_1, x_2, \dots]$  we have  $I = \langle x_1, x_2, \dots \rangle$  and  $J = \langle x_2, x_3, \dots \rangle$  so that  $I \simeq J$  by the map  $x_i \mapsto x_{i+1}$ . But  $R/I \simeq \mathbb{Z}$  while  $R/J \simeq \mathbb{Z}[x]$ .

It is true in this example that neither of  $R/I$  or  $R/J$  is finite, so perhaps this short argument might be saved, but I do not see it.

**14.** Show that  $\mathbb{Z}_3[i] \simeq \mathbb{Z}_3[x]/(x^2 + 1)$ . Nothing is special about 3 here except that it is prime, so  $\mathbb{Z}_3$  is a field.

Define  $\phi : \mathbb{Z}_3[x] \rightarrow \mathbb{Z}_3[i]$  by  $\phi(f(x)) = f(i)$ , this is clearly a ring homomorphism. (This sort of evaluation map is always a homomorphism.) The map is clearly onto as  $\phi(a + bx) = a + bi$ .  $f(x) \in \ker(\phi)$  iff  $f(i) = 0$ . Since the coefficients are in  $\mathbb{Z}_3$  we have  $\overline{f(i)} = \overline{f(-i)} = f(-i) = 0$ . this by the division algorithm we have that  $(x - i)(x + i) = x^2 + 1 \mid f(x)$  since if not  $f(x) = (x^2 + 1)q(x) + (ax + b)$  so  $f(i) = b + ia = 0$  and so  $a = b = 0$ .

**26.** Determine all ring homomorphisms  $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ .

If we insist that  $\phi(1) = 1$ , i.e., that  $\phi$  is a homomorphism of unitary rings, then there is just one, namely  $\phi(1) = 1$  and so  $\phi(m) = \phi(m \cdot 1) = m\phi(1) = m$ , so just the identity.

If we allow  $\phi(1) \neq 1$ , then we still have that  $\phi$  is determined by  $\phi(1)$  since  $\phi(m) = \phi(m \cdot 1) = m\phi(1)$ . since  $\phi(1 \cdot 1) = \phi(1)\phi(1) = \phi(1)$  we have  $\phi(1) = k$  for some  $k \in \mathbb{Z}_n$  satisfying  $k^2 = k$  or  $k(k - 1) = 0$ . (That is  $\phi(1)$  must be an idempotent element of  $\mathbb{Z}_n$ .)

We can count the number of idempotents. If  $n = p_1^{m_1} \cdots p_k^{m_k}$ , then

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_k^{m_k}}$$

so any idempotent  $k$  can be associated to  $(k_1, \dots, k_l)$  where each  $k_i$  is idempotent in  $\mathbb{Z}_{p_i^{m_i}}$ , but this means that  $p_i^{m_i} \mid k_i(k_i - 1)$  and as  $p_i$  can only divide one of  $k_i$  or  $k_i - 1$  we know that either  $k_i = p_i^{m_i}$  or  $k_i = 1$ . Thus there are  $2^l$  many idempotents and so  $2^l$  many homomorphisms of  $\mathbb{Z}_n$  where there are  $l$  many distinct prime divisors of  $n$ .

**31.** Prove that  $R[x]/(x^2)$  is ring isomorphic to  $\left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in R \right\}$ .

Let  $\phi(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = \begin{bmatrix} a_0 & a_1 \\ 0 & a_0 \end{bmatrix}$ . Preservation of addition is trivial. For multiplication notice

$$f(x)g(x) = (a_0 + a_1x + q(x)x^2)(b_0 + b_1x + r(x)x^2) = a_0b_0 + (a_0b_1 + a_1b_0)x + s(x)x^2$$

and so

$$\phi(f(x))\phi(g(x)) = \begin{bmatrix} a_0 & a_1 \\ 0 & a_0 \end{bmatrix} \begin{bmatrix} b_0 & b_1 \\ 0 & b_0 \end{bmatrix} = \begin{bmatrix} a_0b_0 & a_0b_1 + a_1b_0 \\ 0 & a_0b_0 \end{bmatrix} = \phi(f(x)g(x))$$

We have  $f(x) \in \ker(\phi)$  iff  $f(x) = 0 + 0x + q(x)x^2 \in (x^2)$ , so

$$R[x]/\ker(\phi) = R[x]/(x^2) \simeq \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in R \right\}$$

**34.** Let  $\phi : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$  be given by  $\phi(m, n) = (m \bmod a, n \bmod b)$ . It is easy to see that  $\phi$  is a surjective homomorphism.

$$(m, n) \in \ker(\phi) \iff m \bmod a = 0 \text{ and } n \bmod b = 0 \iff (m, n) \in (a) \times (b)$$

So  $\mathbb{Z} \times \mathbb{Z} / \ker(\phi) = (\mathbb{Z} \times \mathbb{Z}) / ((a) \times (b)) \simeq \mathbb{Z}_a \times \mathbb{Z}_b$ .

**38.** Let  $n$  be given in base 10 as,  $n = d_k d_{k-1} \cdots d_1 d_0 = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10 + d_0$  where  $d_i \in \mathbb{Z}_{10}$ . Then, since  $10 = -1 \pmod{11}$ ,

$$\begin{aligned} n \pmod{11} &= d_k (10 \pmod{11})^k + d_{k-1} (10 \pmod{11})^{k-1} + \cdots + d_1 (10 \pmod{11}) + d_0 \\ &= (d_k (-1)^k + d_{k-1} (-1)^{k-1} + \cdots + d_1 (-1) + d_0) \pmod{11} \end{aligned}$$

So

$$11 \mid n \iff 11 \mid d_k (-1)^k + d_{k-1} (-1)^{k-1} + \cdots + d_1 (-1) + d_0$$

**40.** Suppose  $\phi : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$  is a ring homomorphism. Then as discussed above, it must be the case that  $\phi(1)$  completely determines  $\phi$ , and it must be that  $\phi(1)^2 = \phi(1)$  and  $n \mid m\phi(1)$ , since  $\phi(0) = 0$  is required. If  $\phi(1) = 1$ , then we must have  $n \mid m$ .

**44.** Clearly,  $R[x]/(x) \simeq R$  so  $(x)$  is maximal iff  $R$  is a field. So  $(x)$  is maximal in  $\mathbb{Z}_n[x]$  iff  $\mathbb{Z}_n$  is a field iff  $n$  is prime.

**46.** Show that if  $\phi : F \rightarrow F$  is a field homomorphism, then the prime subfield is fixed by  $F$ .

There are two ways to define the prime subfield,  $F_0$ . The official definition is

$$F_0 = \bigcap \{F' \subseteq F \mid F' \text{ is a subfield}\}$$

Since the intersection of subfields is a subfield, this definitely defines  $F_0$  as the minimal subfield. On the other hand,  $F_0$  is the subfield generated by  $1_F$ , for a field of prime characteristic  $p$ , this is just the copy of  $\mathbb{Z}_p$  generated from  $1_F$ . For a field of characteristic 0,  $F_0$  is the copy of  $\mathbb{Q}$  of the form  $n_F m_F^{-1}$  where  $m \neq 0$  and  $n_F = 1_F + \cdots + 1_F$ ,  $n$ -times.

So, according to each definition, there is a proof. The proof using the second definition is trivial, just using the fact that  $\phi(1_F) = 1_F$ .

The proof using the first definition is, perhaps, more interesting. The point is that  $\ker(\phi) = \{0_F\}$ , assuming that  $\ker(\phi) \neq F$ . This is because  $F/(0_F) \simeq F$  is a field, and so  $(0_F) = \{0_F\}$  is a maximal ideal, so there are no non-trivial ideals, and hence every epimorphism is an automorphism. So  $\phi(F_0) = \bigcap \{\phi(F') \mid F' \text{ a subfield of } F\} = \bigcap \{F' \mid F' \text{ a subfield of } F\} = F_0$ . This argument would not work except that  $\phi$  is a bijection and

$$F' \text{ is a subfield of } F \iff \phi(F') \text{ is a subfield of } \phi(F) = F$$

and

$$F' \text{ is a subfield of } \phi(F) = F \iff \phi^{-1}(F') \text{ is a subfield of } F$$

**50.** Prove that  $x \mapsto x^p$  is a ring homomorphism in a ring of prime characteristic  $p$ . We have already done the hard work

$$\begin{aligned} (x+y)^p &= \sum_{k=0}^p \binom{p-k}{k} x^k y^{p-k} = x^p + y^p && \text{since } p \mid \binom{p-k}{k} \text{ for } 0 < k < p \\ (x \cdot y)^p &= x^p \cdot y^p && \text{trivial} \end{aligned}$$

If  $R$  is a field, then  $\ker(\phi)$  can only be  $R$  or  $\{0\}$ . In this case  $\phi(1) \neq 0$  so  $\ker(\phi) = \{0\}$  and  $\phi : R \rightarrow R$  is injective. Now this gets us that  $\phi$  is an isomorphism between  $R$  and  $\phi(R)$  not that  $\phi \in \text{Aut}(R)$ , for this we would need to assume further that every member of  $R$  has



the form  $x^p$ , such a ring, or field, is called *perfect*. Any finite field is perfect, but there are imperfect infinite fields of characteristic  $p$ .

**65.** Let  $Q$  be the field of quotients of  $\mathbb{Z}[i]$  and define  $\phi : Q \rightarrow \mathbb{Q}[i]$  by  $(a, b) \mapsto a \cdot b^{-1}$ . We can check that this is well-defined and a field homomorphism.

To see that the map is well-defined, suppose  $(a, b) = (a', b')$ , that is  $ab' - a'b = 0$ . Then in  $\mathbb{Q}[i]$  it is also true that  $ab' = a'b$  and so  $ab^{-1} = a'b'^{-1}$  so  $\phi((a, b)) = \phi((a', b'))$ .

Next we check addition,  $\phi((a, b) + (a', b')) = \phi((ab' + a'b, bb')) = (ab' + a'b)(bb')^{-1} = ab^{-1} + a'b'^{-1} = \phi((a, b)) + \phi((a', b'))$ . Multiplication is similar.

The map is necessarily 1-1, being a map between fields, so all that is left is seeing that it is onto. Let  $r + si \in \mathbb{Q}[i]$ , then  $r = a/b$  and  $s = a'/b'$  where  $a, a', b, b' \in \mathbb{Z}$  so  $r + si = (ab' + a'bi)(bb')^{-1} \in \text{Img}(\phi)$ .

**67.** Let  $D$  be an integral domain and  $F$  the field of quotients. Let  $E$  be a field that contains  $D$ , then  $E$  contains naturally a copy of  $F$ .

This is exactly as above, define  $\phi : F \rightarrow E$  by  $(a, b) \mapsto ab^{-1}$ . Then  $\text{Img}(\phi)$  is the desired copy.