

## MATH 113 HOMEWORK 7 SOLUTIONS

### 1. RINGS AND IDEALS

**Problem 1.1.** Let  $R$  be a ring and let  $I$  and  $J$  be ideals of  $R$ .

- (1) Show that  $I \cap J$  is an ideal of  $R$ .
- (2) Show that the set  $I + J = \{i + j \mid i \in I, j \in J\}$  is an ideal of  $R$ .
- (3) Let  $n, m \in \mathbb{N}$  be arbitrary, and consider the principal ideals  $(n) \subseteq \mathbb{Z}$  and  $(m) \subseteq \mathbb{Z}$ . Calculate  $(n) \cap (m)$  and  $(n) + (m)$ .
- (4) Consider the principal ideals  $I = (x)$  and  $J = (x + 1)$  in  $\mathbb{R}[x]$ . Calculate  $I \cap J$  and  $I + J$ .

**Solution 1.1.1.** (1) The set  $I \cap J$  is nonempty since  $0 \in I$  and  $0 \in J$ , so  $0 \in I \cap J$ . Let  $a, b \in I \cap J$  and  $r \in R$  be arbitrary. Then  $a, b \in I$  and  $a, b \in J$ . Since  $I$  and  $J$  are ideals, we have  $a - b \in I$  and  $a - b \in J$ , so  $a - b \in I \cap J$ . Likewise,  $ra, ar \in I$  and  $ra, ar \in J$ , hence  $ra, ar \in I \cap J$ . Thus  $I \cap J$  is an ideal of  $R$ .

(2) We have that  $I + J$  is nonempty since  $0 = 0 + 0 \in I + J$ . Let  $x, y \in I + J$  and  $r \in R$  be arbitrary. By definition,  $x = a + b$  and  $y = c + d$  for some  $a, c \in I$  and  $b, d \in J$ . Then  $x - y = (a + b) - (c + d) = (a - c) + (b - d) \in I + J$ . Since  $I$  and  $J$  are ideals, we have  $ra, ar \in I$  and  $rb, br \in J$ , hence  $rx = ra + rb \in I + J$  and  $xr = ar + br \in I + J$ . Thus  $I + J$  is an ideal of  $R$ .

(3) We have actually already done this calculation. If  $n = 0$ , then  $(n) \cap (m) = (0)$  and  $(n) + (m) = (m)$ . If  $n \neq 0$  and  $m \neq 0$ , we have  $(n) \cap (m) = (\text{lcm}(n, m))$  and  $(n) + (m) = (\text{gcd}(n, m))$ .

(4) I claim first that  $I \cap J = (x^2 + x)$ . Indeed, suppose  $p(x) \in I \cap J$ . Then  $p(x) \in I$ , so  $x|p(x)$ , hence  $0$  is a root of  $p(x)$  and  $p(x) = xq(x)$  for some  $q(x) \in R[x]$ . And  $p(x) \in J$  also, so  $x + 1|p(x)$ . Hence  $-1$  is a root of  $q(x)$ , so  $q(x) = (x + 1)r(x)$  for some  $r(x) \in R[x]$ , so  $p(x) = x(x + 1)r(x) = (x^2 + x)r(x)$ , hence  $p(x) \in (x^2 + x)$ . Thus  $I \cap J \subseteq (x^2 + x)$ .

On the other hand, if  $p(x) \in (x^2 + x)$ , then  $p(x) = x(x + 1)r(x)$  for some  $r(x) \in R[x]$ , and hence  $p(x) \in I \cap J$ . Thus  $I \cap J = (x^2 + x)$ .

Now I claim that  $I + J = (1) = R[x]$ . Indeed, we have  $1 = -x + x + 1 \in I + J$ . Hence for all  $p(x) \in R[x]$  we have  $p(x) = p(x) \cdot 1 \in I + J$ , so  $I + J = R[x] = (1)$ .

**Problem 1.2.** Let  $n \in \mathbb{N}$  be arbitrary. Show that the ideal  $n\mathbb{Z} \subseteq \mathbb{Z}$  is prime if and only if  $n$  is prime.

**Solution 1.2.1.** Suppose that  $n$  is prime. Then we know that  $\mathbb{Z}/n\mathbb{Z}$  is a field, hence  $n\mathbb{Z}$  is maximal, thus prime.

Suppose that  $n$  is not prime. If  $n = 1$  then  $n\mathbb{Z} = \mathbb{Z}$  which is not a prime ideal by definition. If  $n \neq 1$ , then there exist  $a, b \in \mathbb{N}$ ,  $1 < a \leq b < n$ , such that  $ab = n$ . But then  $a, b \notin n\mathbb{Z}$ , but  $ab \in n\mathbb{Z}$ . Hence  $n\mathbb{Z}$  is not prime.

## 2. POLYNOMIALS

**Problem 2.1.** Let  $I$  be the subset of  $\mathbb{Z}[x]$  consisting of all polynomials with even constant term, i.e. if  $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$  then  $p(x) \in I$  iff  $a_0 \in 2\mathbb{Z}$ .

- (1) Show that  $I$  is an ideal of  $\mathbb{Z}[x]$ .
- (2) Show that  $I$  is not a principal ideal of  $\mathbb{Z}[x]$ .
- (3) Is  $I$  prime? Maximal?

**Solution 2.1.1.** (1) Note first that  $I$  is nonempty since  $0 \in I$ . Let  $p(x), q(x) \in I$  be arbitrary, and let  $a$  be the constant term of  $p(x)$  and  $b$  be the constant term of  $q(x)$ , so  $a, b \in 2\mathbb{Z}$ . Then  $a - b \in 2\mathbb{Z}$  is the constant term of  $p(x) - q(x)$ , so  $p(x) - q(x) \in \mathbb{Z}[x]$ . Let  $r(x) \in \mathbb{Z}[x]$  be arbitrary, say with constant term  $c \in \mathbb{Z}$ . Then the constant term of  $r(x)p(x)$  is  $ca \in 2\mathbb{Z}$ , hence  $r(x)p(x) \in I$ . Thus  $I$  is an ideal of  $\mathbb{Z}[x]$  (note we do not have to check  $p(x)r(x) \in I$  since  $\mathbb{Z}[x]$  is commutative).

(2) Note that we have  $2, x \in I$  but  $1 \notin I$ . Suppose that  $I$  were principal, say with generator  $p(x)$ . Then  $2 = p(x)q(x)$  for some  $q(x) \in \mathbb{Z}[x]$ . Hence  $p(x)$  must be constant, i.e.  $p(x) = a \in 2\mathbb{Z}$  since  $p(x) \in I$ . Since 2 is a multiple of  $a \in 2\mathbb{Z}$ , we must have  $a = \pm 2$ . Then in either case  $I = (p(x)) = (2)$  since 2 and  $-2$  generate the same ideal. But I claim  $x \notin (2)$ . Indeed, let  $\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}/2\mathbb{Z}[x]$  be the reduction homomorphism. Then  $(2) \subseteq \ker \phi$ , but  $x \notin \ker \phi$  since  $\phi(x) = x \neq 0$ . Hence we have a contradiction, so  $I$  is not principal.

(3) I claim that  $\mathbb{Z}[x]/I \cong \mathbb{Z}/2\mathbb{Z}$ , hence  $I$  is both prime and maximal. Let

$$\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}/2\mathbb{Z}$$

be the homomorphism which sends  $p(x)$  to  $p(0) \pmod{2}$ , i.e. sends  $p(x)$  to its constant term modulo 2. It is easy to see that this is a surjective homomorphism and that  $\ker \phi = I$ . The desired isomorphism follows by the first isomorphism theorem. Since  $\mathbb{Z}/2\mathbb{Z}$  is a field, we have that  $I$  is maximal (hence prime).

**Problem 2.2.** Let  $R$  be a commutative ring with 1 and let  $I$  be an ideal of  $R$ . Let  $I[x] \subseteq R[x]$  be the set of all polynomials  $a_0 + a_1x + \cdots + a_nx^n \in R[x]$  such that  $a_i \in I$  for all  $i$ .

- (1) Show that  $I[x]$  is an ideal of  $R[x]$ .
- (2) Show that  $R[x]/I[x] \cong (R/I)[x]$ .
- (3) Use (2) to show that  $3\mathbb{Z}[x]$  is a prime ideal in  $\mathbb{Z}[x]$  which is not maximal.

**Solution 2.2.1.** (1 and 2) For  $a \in R$ , write  $\bar{a}$  for  $a + I \in R/I$ . Let  $\phi : R[x] \rightarrow R/I[x]$  be the homomorphism defined by

$$\phi(a_0 + a_1x + \cdots + a_nx^n) = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n,$$

i.e. this homomorphism “reduces coefficients mod  $I$ .” In class we showed that in the case  $R = \mathbb{Z}$  and  $I = n\mathbb{Z}$ , this is a homomorphism. This proof carries over word for word, symbol for symbol to show that  $\phi$  is a homomorphism in this case also. Clearly  $\phi$  is surjective.

Now, I claim that  $I[x] = \ker \phi$ . Indeed,

$$0 = \phi(a_0 + a_1x + \cdots + a_nx^n) = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n$$

if and only if  $\bar{a}_i = 0$  for all  $i$ , if and only if  $a_i \in I$  for all  $i$ . Thus  $\ker \phi = I[x]$  is an ideal of  $R[x]$  and by the first isomorphism theorem we have  $R[x]/I[x] \cong (R/I)[x]$ .

(3) By part (2), we have that

$$\mathbb{Z}[x]/3\mathbb{Z}[x] \cong \mathbb{Z}/3\mathbb{Z}[x].$$

Since  $\mathbb{Z}/3\mathbb{Z}[x]$  is an integral domain which is not a field, we have that  $3\mathbb{Z}[x]$  is a prime ideal but not maximal.

### 3. IRREDUCIBLE POLYNOMIALS AND FIELDS

**Problem 3.1.** Which of the following polynomials are irreducible over  $\mathbb{Q}[x]$ ?

- (1)  $x^3 + 3x^2 + x + 1$ ,
- (2)  $x^4 + x^2 + 2x + 1$ ,
- (3)  $5x^5 + 4x^4 + 6x^2 + 10x + 6$ .

**Solution 3.1.1.** (1) The polynomial  $p(x) = x^3 + 3x^2 + x + 1$  is irreducible over  $\mathbb{Q}[x]$ . By the Gauss Lemma, it is enough to show it does not factor over  $\mathbb{Z}$ , and since  $\deg p(x) = 3$ , it is enough to show  $p(x)$  has no root in  $\mathbb{Z}$ . We know that the only possible integer (or rational) roots of  $p(x)$  are  $\pm 1$ . We have  $p(1) = 6 \neq 0$  and  $p(-1) = 2 \neq 0$ . Hence  $p(x)$  is irreducible.

(2) The polynomial  $p(x) = x^4 + x^2 + 2x + 1$  is irreducible over  $\mathbb{Q}[x]$ . Again by the Gauss Lemma, it suffices to show that this polynomial is irreducible over  $\mathbb{Z}[x]$ . As in part (1), we immediately see that  $p(x)$  cannot have a degree-1 factor, since  $p(1) = 5 \neq 0$  and  $p(-1) = 1 \neq 0$ . Now, suppose that  $p(x)$  factors into degree-2 factors, say

$$p(x) = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd.$$

Then  $bd = 1$ , so  $b = d = \pm 1$ . Hence  $2 = ad + bc + \pm(a + c)$ , but also  $0 = (a + c)$  from the  $x^3$  coefficients. This is a contradiction, hence  $p(x)$  is irreducible.

(3) The polynomial  $p(x) = 5x^5 + 4x^4 + 6x^2 + 10x + 6$  is irreducible over  $\mathbb{Q}[x]$  by Eisenstein's Criterion applied to the prime 2.

**Problem 3.2.** Let  $p(x) = x^2 + ax + b \in \mathbb{R}[x]$  be an irreducible polynomial. Show that  $\mathbb{R}[x]/(p(x)) \cong \mathbb{C}$ . (Hint: quadratic formula!)

**Solution 3.2.1.** By the quadratic formula, we know that

$$\alpha = \frac{-a + \sqrt{a^2 - 4b}}{2} \in \mathbb{C}$$

is a root of  $p(x)$ . Since  $p(x)$  is irreducible over  $\mathbb{R}$ , we know that  $\alpha \notin \mathbb{R}$ , hence  $\alpha = c + id$  for some  $c, d \in \mathbb{R}$  with  $d \neq 0$  (namely  $c = -a$  and  $d = \sqrt{4b - a^2}/2$ ). Now, define a homomorphism

$$\phi : \mathbb{R}[x] \rightarrow \mathbb{C}$$

by  $\phi(p(x)) = p(\alpha)$ . I claim first that  $\phi$  is surjective. Indeed, let  $e + if \in \mathbb{C}$  be arbitrary. Then

$$\phi\left(\frac{f}{d}x + \left(e - \frac{fc}{d}\right)\right) = \frac{f}{d}(c + id) + e - \frac{fc}{d} = e + if.$$

Notice that we needed  $d \neq 0$  here in order to be able to divide by  $d$ ! Now I claim that  $\ker \phi = (p(x))$ . Certainly  $p(x) \in \ker \phi$  since  $p(\alpha) = 0$ , thus  $(p(x)) \subseteq \ker \phi$ . Now,  $p(x)$  is irreducible, thus  $(p(x))$  is maximal, so either  $\ker \phi = (p(x))$  or  $\ker \phi = \mathbb{R}[x]$ . But the latter is impossible since  $\phi(1) = 1 \neq 0$ . Thus  $\ker \phi = (p(x))$ , so by the first isomorphism theorem we have

$$\mathbb{R}[x]/(p(x)) \cong \mathbb{C}.$$

**Problem 3.3** (An example of a finite field). Do the following:

- (1) Show that the polynomial  $x^2 + 1$  is irreducible in  $\mathbb{Z}/3\mathbb{Z}[x]$ . Conclude that the ring  $K = (\mathbb{Z}/3\mathbb{Z}[x])/(x^2 + 1)$  is a field.
- (2) Show that every element of this field can be uniquely written in the form  $\overline{ax + b}$  for some  $a, b \in \mathbb{Z}/3\mathbb{Z}$ , and use this to calculate the number of elements in  $K$ .
- (3) Compute a full multiplication table for  $K$ .
- (4) Let  $M$  be the  $2 \times 2$ -matrix

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

with entries in  $\mathbb{Z}/3\mathbb{Z}$ . Show that  $M^2 = -I$ , where  $I$  is the identity matrix.

- (5) Consider the set of all matrices of the form  $aM + bI$  where  $a, b \in \mathbb{Z}/3\mathbb{Z}$ . Show that this set forms a ring  $R$ .

(6) Show that  $K \cong R$ . (Hint: use the first isomorphism theorem).

**Solution 3.3.1.** (1) Since  $x^2 + 1$  has degree 2, it is irreducible if and only if it has no roots; it is easy to check that this is the case.

(2) This is now a theorem we have proven in class: if  $p(x) \in F[x]$  is an irreducible polynomial of degree  $n$ , then  $\{1, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n-1}\}$  is a basis for  $F[x]/(p(x))$  over  $F$ . In our case this just says that  $\{1, \bar{x}\}$  is a basis, i.e. every element of  $K$  can be written uniquely as  $a\bar{x} + b = \overline{ax + b}$  for some  $a, b \in \mathbb{Z}/3\mathbb{Z}$ . (To prove this directly, let  $p(x) \in \mathbb{Z}/3\mathbb{Z}[x]$  be arbitrary. Then  $p(x) = q(x)(x^2 + 1) + r(x)$  for a unique polynomial  $r(x) = ax + b$  of degree  $< 2$ . Then  $\overline{q(x)(x^2 + 1)} = \overline{ax + b}$ .)

Since there are 3 choices for  $a$  and 3 choices for  $b$ ,  $K$  is a field with 9 elements.

(3) Let  $\alpha = \bar{x}$ . Then  $\alpha^2 = -1 = 2$ . We use this to compute:

	0	1	2	$\alpha$	$\alpha + 1$	$\alpha + 2$	$2\alpha$	$2\alpha + 1$	$2\alpha + 2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$\alpha$	$\alpha + 1$	$\alpha + 2$	$2\alpha$	$2\alpha + 1$	$2\alpha + 2$
2	0	2	1	$2\alpha$	$2\alpha + 2$	$2\alpha + 1$	$\alpha$	$\alpha + 2$	$\alpha + 1$
$\alpha$	0	$\alpha$	$2\alpha$	2	$\alpha + 2$	$2\alpha + 2$	1	$\alpha + 1$	$2\alpha + 1$
$\alpha + 1$	0	$\alpha + 1$	$2\alpha + 2$	$\alpha + 2$	$2\alpha$	1	$2\alpha + 1$	2	$\alpha$
$\alpha + 2$	0	$\alpha + 2$	$2\alpha + 1$	$2\alpha + 2$	1	$\alpha$	$\alpha + 1$	$2\alpha$	2
$2\alpha$	0	$2\alpha$	$\alpha$	1	$2\alpha + 1$	$\alpha + 1$	2	$2\alpha + 2$	$\alpha + 2$
$2\alpha + 1$	0	$2\alpha + 1$	$\alpha + 2$	$\alpha + 1$	2	$2\alpha$	$2\alpha + 2$	$\alpha$	1
$2\alpha + 2$	0	$2\alpha + 2$	$\alpha + 1$	$2\alpha + 1$	$\alpha$	2	$\alpha + 2$	1	$2\alpha$

(4) We have

$$M^2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = -I,$$

since  $2 = -1$  in  $\mathbb{Z}/3\mathbb{Z}$ .

(5) Since  $M_2(\mathbb{Z}/3\mathbb{Z})$  is a ring, it suffices to show that the set  $R$  of matrices of the form  $aM + bI$  is closed under addition, additive inverses, and multiplication (we also have to check that it is nonempty, but this is trivial). Addition and additive inverses are clear. For multiplication, we have

$$(aM + bI)(cM + dI) = (acM^2 + bcM + adM + bdI) = (ad + bc)M + (bd - ac)I.$$

Hence  $R$  is indeed a subring of  $M_2(\mathbb{Z}/3\mathbb{Z})$ .

(6) Define a homomorphism  $\phi : \mathbb{Z}/3\mathbb{Z}[x] \rightarrow R$  by

$$\phi(a_0 + a_1x + \dots + a_nx^n) = a_0I + a_1M + \dots + a_nM^n.$$

It is easy to see that this is a homomorphism. The function  $\phi$  is surjective since  $aM + bI = \phi(ax + b)$ . I claim that  $\ker \phi = (x^2 + 1)$ . We have  $\phi(x^2 + 1) = M^2 + I = -I + I = 0$ , so certainly  $(x^2 + 1) \subseteq \ker \phi$ .

Since  $(x^2 + 1)$  is maximal, to show that  $\ker \phi = (x^2 + 1)$  it suffices to show that  $\ker \phi \neq \mathbb{Z}/3\mathbb{Z}[x]$ . But  $\phi$  is not the zero homomorphism since  $\phi(1) = I \neq 0$ . Hence  $\ker \phi = (x^2 + 1)$ , so by the first isomorphism theorem,  $K = \mathbb{Z}/3\mathbb{Z}[x]/(x^2 + 1) \cong R$ .

(Remark): The only thing that prevents us from doing the above to construct any finite field is to figure out how to find a matrix  $M$  which satisfies the desired polynomial equation. It turns out that this can always be done.

**Problem 3.4.** Show that there exists a field with 8 elements. Compute a full multiplication table for your example.

**Solution 3.4.1.** Let  $p(x) = x^3 + x + 1 \in \mathbb{Z}/2\mathbb{Z}[x]$ . Then  $p(x)$  is irreducible since it has no roots and has degree 3. Let  $K = (\mathbb{Z}/2\mathbb{Z}[x])/(p(x))$ . Then  $K$  is a field. We know moreover that this is a degree-3 field extension of  $\mathbb{Z}/2\mathbb{Z}$  and that if we let  $\alpha = \bar{x}$ , then a basis for the extension is given by  $1, \alpha, \alpha^2$ . Hence every element of  $K$  can be written uniquely in the form  $a\alpha^2 + b\alpha + c$  with  $a, b, c \in \mathbb{Z}/2\mathbb{Z}$ . There are two choices for  $a$ , two for  $b$ , and two for  $c$ , hence  $2^3 = 8$  total elements of  $K$ .

We have  $\alpha^3 + \alpha + 1 = 0$ , so  $\alpha^3 = \alpha + 1$  (since  $1 = -1$  in  $\mathbb{Z}/2\mathbb{Z}$ ). Using this (removing rows of zeros for compactness), we compute:

	1	$\alpha$	$\alpha + 1$	$\alpha^2$	$\alpha^2 + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$
1	1	$\alpha$	$\alpha + 1$	$\alpha^2$	$\alpha^2 + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$
$\alpha$	$\alpha$	$\alpha^2$	$\alpha^2 + \alpha$	$\alpha + 1$	1	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$
$\alpha + 1$	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + 1$	$\alpha^2 + \alpha + 1$	$\alpha^2$	1	$\alpha$
$\alpha^2$	$\alpha^2$	$\alpha + 1$	$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha$	$\alpha$	$\alpha^2 + 1$	1
$\alpha^2 + 1$	$\alpha^2 + 1$	1	$\alpha^2$	$\alpha$	$\alpha^2 + \alpha + 1$	$\alpha + 1$	$\alpha^2 + \alpha$
$\alpha^2 + \alpha$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	1	$\alpha^2 + 1$	$\alpha + 1$	$\alpha$	$\alpha^2$
$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$	$\alpha$	1	$\alpha^2 + \alpha$	$\alpha^2$	$\alpha + 1$

(Remark):  $p(x) = x^3 + x^2 + 1$  was also a viable choice. The resulting field is isomorphic to the one constructed above.

#### 4. LINEAR ALGEBRA

**Problem 4.1.** Do Judson, Ch. 18, Problem 15.

**Solution 4.1.1.** (a) Let  $T : V \rightarrow W$  be a linear transformation of vector spaces over  $F$ . We have to check that  $\ker(T)$  is nonempty and closed under addition and scalar multiplication. We have

$$T(0) = T(0 + 0) = T(0) + T(0),$$

hence subtracting  $T(0)$  from both sides yields  $T(0) = 0$ , so  $0 \in \ker(T)$ , thus  $\ker(T)$  is nonempty. Now, let  $u, v \in \ker(T)$  and  $a \in F$  be arbitrary. Then we have  $T(u + v) = T(u) + T(v) = 0 + 0 = 0$ , so  $u + v \in \ker(T)$ . And we have  $T(au) = aT(u) = a0 = 0$ , so  $au \in \ker(T)$ . Thus  $\ker(T)$  is a subspace

of  $V$ .

(b) I would never ever call this the range. This is the image. And everyone writes this as  $T(V)$ , so forget his notation. Now,  $0 = T(0) \in T(V)$ , so  $T(V)$  is nonempty. Let  $w_1, w_2 \in T(V)$  and  $a \in F$  be arbitrary. Then there exist  $v_1, v_2 \in V$  such that  $T(v_1) = w_1$  and  $T(v_2) = w_2$ . Thus  $w_1 + w_2 = T(v_1) + T(v_2) = T(v_1 + v_2) \in T(V)$  and  $aw_1 = aT(v_1) = T(av_1) \in T(V)$ , so  $T(V)$  is closed under addition and scalar multiplication, hence is a subspace of  $W$ .

(c) Suppose that  $T$  is injective. Since  $T(0) = 0$  (as we showed in (1)),  $0 \in V$  is the only element which is sent to 0 (as  $T$  is injective), so  $\ker(T) = \{0\}$ .

On the other hand, suppose that  $\ker(T) = 0$  and suppose that  $T(u) = T(v)$  for some  $u, v \in V$ . Then

$$0 = T(u) - T(v) = T(u) + (-1)T(v) = T(u) + T(-1 \cdot v) = T(u) + T(-v) = T(u - v),$$

so  $u - v \in \ker(T)$  and hence  $u - v = 0$ . Thus  $u = v$ .

(d) As stated in an unproven theorem in class, any linearly independent subset of  $V$  can be extended to a basis for  $V$ . So if  $v_1, \dots, v_k$  is a basis for  $\ker(T)$ , then in particular this is a linearly independent subset of  $V$  and so can be extended to a basis for  $V$ .

Now, every element of  $T(V)$  is of the form  $T(v)$  for some  $v \in V$ , hence every element of  $T(V)$  can be written in the form

$$T(a_1v_1 + \dots + a_mv_m) = a_1T(v_1) + \dots + a_mT(v_m) = 0 + \dots + 0 + a_{k+1}T(v_{k+1}) + \dots + a_mT(v_m),$$

since  $T(v_i) = 0$  for  $1 \leq i \leq k$ . Thus the elements  $T(v_{k+1}), \dots, T(v_m)$  span  $T(V)$ . It remains to show that they are linearly independent.

Suppose that

$$a_{k+1}T(v_{k+1}) + \dots = a_mT(v_m) = 0.$$

Then since  $T$  is a linear transformation, we have

$$T(a_{k+1}v_{k+1} + \dots + a_mv_m) = 0,$$

so  $a_{k+1}v_{k+1} + \dots + a_mv_m \in \ker(T)$ . Since  $v_1, \dots, v_k$  is a basis for  $\ker(T)$ , there exist  $a_1, \dots, a_k \in F$  such that

$$a_{k+1}v_{k+1} + \dots + a_mv_m = a_1v_1 + \dots + a_kv_k,$$

and so

$$(-a_1)v_1 + \dots + (-a_k)v_k + a_{k+1}v_{k+1} + \dots + a_mv_m = 0.$$

Since  $v_1, \dots, v_m$  are linearly independent, it follows that in particular  $a_{k+1} = \dots = a_m = 0$ . Hence  $T(v_{k+1}), \dots, T(v_m)$  are linearly independent, as desired.

(e) As in the problem, suppose that  $T : V \rightarrow W$  is a linear transformation with  $\dim V = \dim W = n$ . Suppose that  $T$  is injective. Then  $\ker(T) = 0$ , so  $\dim T(V) = \dim V - \dim 0 = \dim V = \dim W$ . Thus  $T(V)$  is a subspace of  $W$  of the same dimension  $n$ , so  $T(V) = W$  (this follows from our theorem (unproven) that a linearly independent  $n$ -element subset of an  $n$ -dimensional vector space is a basis).

Suppose on the other hand that  $T$  is surjective. Then  $T(V) = W$ , so  $\dim V = \dim W = \dim T(V) = \dim V - \dim \ker(T)$ , hence  $\dim \ker(T) = 0$ , so  $\ker(T) = 0$ , hence  $T$  is injective.