Homework 3

Aleck Zhao

February 21, 2017

1. Let A be a commutative ring containing a field F as a subring. For each $a \in A$, we define the multiplication by a map

$$\begin{aligned} m_a : A &\to A \\ x &\mapsto ax. \end{aligned}$$

(a) Regarding A as an F-vector space in the natural way, show that m_a is a linear transformation over F.

Proof. Let $b \in F$ and $u, v \in A$. Then we have

$$\begin{aligned} m_a(u+v) = a(u+v) = au + av = m_a(u) + m_a(v) \\ m_a(bu) = a(bu) = b(au) = bm_a(u) \end{aligned}$$

The second equality comes from the fact that A is a commutative ring. Thus, m_a is a linear transformation over F, as desired. □

(b) Suppose that A is an integral domain which is finite dimensional as an F-vector space. Show that A is a field.

Proof. If $a \neq 0$, then

$$\ker m_a = \{\, x \in A \mid ax = 0 \,\} = \{0\}$$

since we are in an integral domain. Thus, $\dim(\ker m_a) = 0$, so by the result of Exercise 31, we have $\dim A = \dim(\operatorname{im} m_a)$. By the result of Exercise 32, if both A and $\operatorname{im} m_a$ have dimension n, they are both isomorphic to F^n, so they are isomorphic to each other. Thus, m_a is a bijective map, and in particular surjective. Since $1 \in A$, there must exist $x \in A$ such that $ax = 1$, and since a was arbitrary, it follows that every possible choice for nonzero a was invertible, so F is a field, as desired. □

Section 5.2: Principal Ideal Domains

13. (a) Show that $\mathbb{Z}[\sqrt{-2}]$ is euclidean with $\delta(a) = |N(a|$.

Proof. Here, $\omega = \sqrt{-2} \implies \omega^2 = -2$. We claim that $\mathbb{Z}[\omega]$ satisfies the condition of Lemma 1. For any $r, s \in \mathbb{Q}$, let m and n be the nearest integers to r and s, respectively. Then,

$$\left|(r-m)^2 - \omega^2(s-n)^2\right| \leq \left|\left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2\right| = \left|\frac{3}{4}\right| < 1$$

Thus, $\mathbb{Z}[\omega]$ is euclidean by Lemma 1. □

(b) If $a = 4 + 3\sqrt{-2}$ and $b = 3 - \sqrt{-2}$, write $a = qb + r$, where $r = 0$ or $\delta(r) < \delta(b)$.

Solution. Consider a division in $\mathbb{C}$, where

$$\frac{a}{b} = \frac{4 + 3\sqrt{-2}}{3 - \sqrt{-2}} = \frac{(4 + 3\sqrt{-2})(3 + \sqrt{-2})}{11} = \frac{6}{11} + \frac{13}{11}\sqrt{-2}$$

So we may estimate $q = 1 + \sqrt{-2}$. Then

$$\begin{aligned} qb &= (1 + \sqrt{-2})(3 - \sqrt{-2}) = 5 + 2\sqrt{-2} \\ \implies r &= -1 + \sqrt{-2} \end{aligned}$$

This is a legitimate factorization because

$$\delta(r) = |N(r)| = \left|(-1)^2 + 2\right| = 3 < 11 = \delta(b)$$

□

Section 6.1: Vector Spaces

21. If $u = a_1v_1 + a_2v_2 + \cdots + a_nv_n$ in a vector space V, and if $a_1 \neq 0$, show that $\operatorname{span}\{v_1, v_2, \cdots, v_n\} = \operatorname{span}\{u, v_2, \cdots, v_n\}$.

Proof. Let $w = b_1v_1 + b_2v_2 + \cdots + b_nv_n$ be an element in $\operatorname{span}\{v_1, v_2, \cdots, v_n\}$. Since $a_1 \neq 0$, it has an inverse, so

$$\begin{aligned} & u = a_1v_1 + a_2v_2 + \cdots + a_nv_n \\ \implies & v_1 = a_1^{-1}u - a_1^{-1}a_2v_2 - a_1^{-1}a_3v_3 - \cdots - a_1^{-1}a_nv_n \end{aligned}$$

Substituting, we have

$$\begin{aligned} w &= b_1(a_1^{-1}u - a_1^{-1}a_2v_2 - \cdots - a_1^{-1}a_nv_n) + a_2v_2 + \cdots + a_nv_n \\ &= a_1^{-1}b_1u + (a_2 - a_1^{-1}a_2b_1)v_2 + \cdots + (a_n - a_1^{-1}a_nb_1)v_n \end{aligned}$$

so $w \in \operatorname{span}\{u, v_2, \cdots, v_n\}$.

For the reverse inclusion, let $x = c_1u + c_2v_2 + \cdots + c_nv_n$ be an element in $\operatorname{span}\{u, v_2, \cdots, v_n\}$. Substituting the expression for u, we have

$$\begin{aligned} x &= c_1(a_1v_1 + a_2v_2 + \cdots + a_nv_n) + c_2v_2 + \cdots + c_nv_n \\ &= a_1c_1v_1 + (a_2c_1 + c_2)v_2 + \cdots + (a_nc_1 + c_n)v_n \end{aligned}$$

so $x \in \operatorname{span}\{v_1, \cdots, v_n\}$. Thus, the two spanning sets are equal, as desired. □

23. (a) Show that an independent set $\{v_1, \cdots, v_n\}$ in ${}_FV$ with n maximal is a basis.

Proof. If n is maximal, then for any $v \in V$, the set $\{v, v_1, \cdots, v_n\}$ is linearly dependent, so we may write

$$0 = av + a_1v_1 + \cdots + a_nv_n$$

for where not all of a, a_i are nonzero. WLOG, $a \neq 0$, so it has an inverse, and

$$v = -a^{-1}a_1v_1 - \cdots - a^{-1}a_nv_n$$

so v is a linear combination of the v_i. Since v was arbitrary, it follows that the set $\{v_1, \cdots, v_n\}$ spans V, and if they are linearly independent, this set is a basis, as desired. □

(b) Show that a spanning set $\{v_1, \cdots, v_n\}$ of ${}_FV$ with n minimal is a basis.

Proof. Suppose $\{v_1, \cdots, v_n\}$ is not a basis. Then there exists a nontrivial linear combination

$$a_1 v_1 + \cdots + a_n v_n = 0$$

WLOG $a_n \neq 0$, so we have

$$v_n = -a_n^{-1} a_1 v_1 - \cdots - a_n^{-1} a_{n-1} v_{n-1}$$

Thus, the set $\{v_1, \cdots, v_{n-1}\}$ spans V, which contradicts the minimality of n. Thus, $\{v_1, \cdots, v_n\}$ is a basis, as desired. □

30. If U is a subspace of a vector space ${}_FV$, define a scalar multiplication on the (additive) factor group V/U by $a(v+U) = av + U$. Show that V/U is a vector space and that if V is finite dimensional, then V/U is finite dimensional and $\dim V/U = \dim V - \dim U$.

Proof. Let $a, b \in F$ and $v + U, w + U \in V/U$.

V1
$$a\left[(v+U) + (w+U)\right] = a(v + w + U) = (av + aw) + U$$

V2
$$(a+b)(v+U) = a(v+U) + b(v+U) = (av+U) + (bv+U) = (av+bv) + U$$

V3
$$a(b(v+U)) = a(bv+U) = abv + U = (ab)(v+U)$$

V4
$$1(v+U) = v + U$$

Thus the four vector space axioms are satisfied, so V/U is a vector space.

Suppose $\dim V = n$, and let $\{v_1, \cdots, v_n\}$ be a basis. Then I claim that the set $\{v_1 + U, \cdots, v_n + U\}$ spans V/U. For any coset $v + U \in V/U$, since $v \in V$, we may write

$$\begin{aligned} v &= a_1 v_1 + \cdots + a_n v_n \\ v + U &= (a_1 v_1 + \cdots + a_n v_n) + U \\ &= a_1(v_1 + U) + \cdots + a_n(v_n + U) \\ &\in \operatorname{span}\{v_1 + U, \cdots, v_n + U\} \end{aligned}$$

Thus, $\{v_1 + U, \cdots, v_n + U\}$ spans V/U, and any spanning set contains a basis, so $\dim V/U \leq n$, so it is finite, as desired. □

31. A linear transformation $\varphi : {}_FV \to {}_FW$ is a map such that $\varphi(v+w) = \varphi(v) + \varphi(w)$ and $\varphi(av) = a\varphi(v)$ for all $a \in F$ and all $v, w \in V$.

(a) Show that $\ker\varphi$ and $\operatorname{im}\varphi$ are subspaces of V and W, respectively.

Proof. $\ker\varphi$: We have

$$\varphi(0) + \varphi(0) = \varphi(0+0) = \varphi(0) \implies \varphi(0) = 0$$

so $0 \in \ker\varphi$. Let $v, w \in \ker\varphi$ and $a \in F$. Then

$$\varphi(v) + \varphi(w) = 0 + 0 = 0 = \varphi(v+w) \implies v + w \in \ker\varphi$$

and

$$\varphi(av) = a\varphi(v) = a \cdot 0 = 0 \implies av \in \ker \varphi$$

Thus, $\ker \varphi$ is a subgroup of V that is closed under addition and scalar multiplication, so it is a subspace, as desired.

$\operatorname{im} \varphi$: From above, we know that $0 \in \operatorname{im} \varphi$ since $\varphi(0) = 0$. Let $\varphi(x), \varphi(y) \in \operatorname{im} \varphi$ and $b \in F$. Then

$$\varphi(x) + \varphi(y) = \varphi(x + y) \in \operatorname{im} \varphi$$

since $x + y \in V$ because V is a vector space. We also have

$$b\varphi(x) = \varphi(bx) \in \operatorname{im} \varphi$$

since $bx \in V$. Thus, $\operatorname{im} \varphi$ is a subgroup of W that is closed under addition and scalar multiplication, so it is a subspace, as desired. □

(b) If V is finite dimensional, show that $\operatorname{im} \varphi$ is also finite dimensional.

Proof. Suppose $\dim V = n$, and let $\{v_1, \cdots, v_n\}$ be a basis for V. Then I claim that $\{\varphi(v_1), \cdots, \varphi(v_n)\}$ spans $\operatorname{im} \varphi$. Consider $\varphi(v) \in \operatorname{im} \varphi$, where $v \in V$. Then we may write

$$\begin{aligned} v &= a_1 v_1 + \cdots + a_n v_n \\ \varphi(v) &= \varphi(a_1 v_1 + \cdots + a_n v_n) \\ &= a_1 \varphi(v_1) + \cdots + a_n \varphi(v_n) \\ &\in \operatorname{span} \{\varphi(v_1), \cdots, \varphi(v_n)\} \end{aligned}$$

Since every spanning set contains a basis, it follows that $\dim(\operatorname{im} \varphi) \leq n$, so it is finite, as desired. □

(c) If V is finite dimensional, show that $\dim V = \dim(\ker \varphi) + \dim(\operatorname{im} \varphi)$.

Proof. If $\dim V = \dim(\ker \varphi)$, then $\ker \varphi = V$, so then $\dim(\operatorname{im} \varphi) = \dim \{0\} = 0$, and the relation is satisfied.

Otherwise, since $\ker \varphi \subsetneq V$, we have $\dim(\ker \varphi) < n$. Let $\dim(\ker \varphi) = m$, so that $\{u_1, \cdots, u_m\}$ is a basis for $\ker \varphi$. Then there exists some $v_1 \in V$ such that $v_1 \notin \ker \varphi$. Thus, $\{u_1, \cdots, u_m, v_1\}$ is a linearly independent set in V. We may continue extending this set, but this process must eventually stop since V is finite dimensional, and the resulting set will be a basis.

Suppose the final basis for V is $\{u_1, \cdots, u_m, v_1, \cdots, v_n\}$. I claim that $\{\varphi(v_1), \cdots, \varphi(v_n)\}$ forms a basis for $\operatorname{im} \varphi$. From part (b), we know that it spans $\operatorname{im} \varphi$, so it suffices to prove that it is linearly independent. Suppose we have a linear combination

$$\begin{aligned} 0 &= a_1 \varphi(v_1) + \cdots + a_n \varphi(v_n) \\ &= \varphi(a_1 v_1 + \cdots + a_n v_n) \end{aligned}$$

If $a_1 v_1 + \cdots + a_n v_n = 0$, then we must have $a_1 = \cdots = a_n = 0$ since the v_i are linearly independent. Otherwise,

$$\begin{aligned} & a_1 v_1 + \cdots + a_n v_n \in \ker \varphi \\ \implies & a_1 v_1 + \cdots + a_n v_n \in \operatorname{span} \{u_1, \cdots, u_m\} \end{aligned}$$

which contradicts the linear independence of $\{u_1, \cdots, u_m, v_1, \cdots, v_n\}$. Thus, $a_1 = \cdots = a_n = 0$, so $\{\varphi(v_1), \cdots, \varphi(v_n)\}$ is a linearly independent set, and spans $\operatorname{im} \varphi$, so it is a basis for $\operatorname{im} \varphi$. Now, we have $\dim(\ker \varphi) = m$ and $\dim(\operatorname{im} \varphi) = n$, and $\dim V = m + n$, so the relation is proven. □

32. Vector spaces ${}_FV$ and ${}_FW$ are called isomorphic if a one-to-one, onto linear transformation $V \to W$ exists. If ${}_FV$ has dimension n, show that $V \cong F^n$.

Proof. Since $\dim V = n$, its basis has n elements, say $\{v_1, \cdots, v_n\}$. Let $\{e_1, \cdots, e_n\}$ represent the standard basis for F^n. For any $u \in V$, we can represent it as

$$u = a_1 v_1 + \cdots + a_n v_n, \qquad a_i \in F, \forall i$$

Define the map

$$T : V \to F^n$$
$$a_1 v_1 + \cdots + a_n v_n \mapsto a_1 e_1 + \cdots + a_n e_n$$

I claim that this is a one-to-one, onto linear transformation.

To prove it is linear, let $a \in F$ and $u, v \in V$ such that

$$u = a_1 v_1 + \cdots + a_n v_n$$
$$v = b_1 v_1 + \cdots + b_n v_n$$

where $a_i, b_i \in F, \forall i$. Then we have

$$\begin{aligned} T(u+v) &= T\left[(a_1 v_1 + \cdots + a_n v_n) + (b_1 v_1 + \cdots + b_n v_n)\right] \\ &= T\left[(a_1 + b_1)v_1 + \cdots + (a_n + b_n)v_n\right] \\ &= (a_1 + b_1)e_1 + \cdots + (a_n + b_n)e_n \\ &= (a_1 e_1 + \cdots + a_n e_n) + (b_1 e_1 + \cdots + b_n e_n) \\ &= T(u) + T(v) \\ T(au) &= T\left[a(a_1 v_1 + \cdots + a_n v_n)\right] \\ &= T(a a_1 v_1 + \cdots + a a_n v_n) \\ &= a a_1 e_1 + \cdots + a a_n v_n \\ &= a(a_1 e_1 + \cdots + a_n v_n) \\ &= aT(u) \end{aligned}$$

Thus T is a linear transformation.

To prove it is injective, suppose

$$\begin{aligned} & T(u) = T(v) \\ \implies & T(a_1 v_1 + \cdots + a_n v_n) = T(b_1 v_1 + \cdots + b_n v_n) \\ \implies & a_1 e_1 + \cdots + a_n e_n = b_1 e_1 + \cdots + b_n e_n \end{aligned}$$

Since the e_i form a basis for F^n, necessarily we must have $a_i = b_i, \forall i$, so then

$$a_1 v_n + \cdots + a_n v_n = b_1 v_1 + \cdots + b_n v_n \implies u = v$$

so T is injective.

To prove it is surjective, take any $w \in F^n$, which can be written as a unique linear combination

$$w = c_1 e_1 + \cdots + c_n e_n$$

From here, we can recover $x \in V$ such that $T(x) = w$ by taking the coefficients of the e_i, so that

$$x = c_1 v_1 + \cdots + c_n v_n$$

Thus, T is surjective, so we have $V \cong F^n$, as desired. □