Matrix Analysis Homework 2

龙肖灵
Xiaoling Long
Student ID.:81943968
Email:longxl@shanghaitech.edu.cn

September 26, 2017

Problem 1 (4/10, *If G is an abelian group, then $End(G)$ is a ring*):

Let G be an abelian group with group operation $*$. For $\phi, \psi \in End(G)$, consider the definition of $\phi + \psi$ and $\phi\psi$ that we gave in the class. Verify that $End(G)$ is a ring under these two operations, i.e., check that all the axioms of the ring structure are true. For example, verify that for $\phi, \psi, \chi \in End(G)$, we have that $\phi(\psi + \chi) = \phi\psi + \phi\chi$.

Proof.

$$\forall \phi, \psi, \chi \in End(G)$$

1. We have that,

$$\begin{aligned}[(\phi + \psi) + \chi](g) &= [\phi + \psi](g) * \chi(g) \\ &= [\phi(g) * \psi(g)] * \chi(g)\end{aligned}$$

G is an abelian group.

$$\begin{aligned}[\phi(g) * \psi(g)] * \chi(g) &= \phi(g) * [\psi(g) * \chi(g)] \\ &= [\phi + (\psi + \chi)](g)\end{aligned}$$

So(+ is associative),

$$(\phi + \psi) + \chi = \phi + (\psi + \chi)$$

2. And then,

$$\begin{aligned}[\phi + \psi](g) &= \phi(g) * \psi(g) \\ &= \psi(g) * \phi(g) \\ &= [\psi + \phi](g) \quad (+ \text{ is commutative})\end{aligned}$$

3. Identity under $+$,
Let $\forall g \in End(V) \quad 0_{End(V)} : g \mapsto e_G$($e_G$ is identity of group G) be identity of group $End(V)$ under $+$.

$$\begin{aligned}[\phi + 0_{End(V)}](g) &= \phi(g) * 0_{End(V)}(g) \\ &= \phi(g) * e_G(g) \\ &= \phi(g)\end{aligned}$$

We can say that,

$$\phi + 0_{End(g)} = \phi$$

So $0_{End(V)}$ is identity of $End(V)$ under operation $+$

4. Inverse of $+$,let $-\phi : g \mapsto (\phi(g))^{-1}$.
   We can know,

$$\begin{aligned}[\phi + (-\phi)](g) &= \phi(g) * ([-\phi])(g) \\ &= \phi(g) * (\phi(g))^{-1} \\ &= e_G \\ &= 0_{End(V)}(g)\end{aligned}$$

   So, we can say that
$$[\phi + (-\phi)] = 0_{End(V)}$$

5. About $\cdot$, we have that,

$$\begin{aligned}[(\phi \cdot \psi) \cdot \chi](g) &= [\phi \cdot \psi](\chi(g)) \\ &= \phi[\psi(\chi(g))]\end{aligned}$$

   Also, we have this,

$$\begin{aligned}[\phi \cdot (\psi \cdot \chi)](g) &= \phi[(\psi \cdot \chi)(g)] \\ &= \phi[\psi(\chi(g))]\end{aligned}$$

   Finally, $\cdot$ is associative.

$$[(\phi \cdot \psi) \cdot \chi](g) = [\phi \cdot (\psi \cdot \chi)](g)$$

6. Let $forall g \in G \quad 1_{End(V)} : g \mapsto g$, then,

$$\begin{aligned}[\phi \cdot 1_{End(V)}](g) &= \phi(1_{End(V)}(g)) \\ &= \phi(g)\end{aligned}$$

   Finally, we get

$$(\phi \cdot 1_{End(V)}) = \phi$$

7. Left distributivity.

$$\begin{aligned}[\phi(\psi + \chi)](g) &= \phi[\psi(g) * \chi(g)] \\ &= [\phi(\psi(g))] * [\phi(\chi(g))]\end{aligned}$$

   And

$$\begin{aligned}[\phi\psi + \phi\chi](g) &= [\phi\psi(g)] * [\phi\psi(g)] \\ &= [\phi(\psi(g))] * [\phi(\chi(g))] \\ &= [\phi(\psi + \chi)](g) \quad \text{(Done.)}\end{aligned}$$

8. Right distributivity.

$$\begin{aligned}[(\phi + \psi)\chi](g) &= [\phi + \psi](\chi(g)) \\ &= [\phi(\chi(g))] * [\psi(\chi(g))] \\ &= [\phi\chi](g) * [\psi\chi](g) \\ &= [\phi\chi + \psi\chi](g) \quad \text{(Done.)}\end{aligned}$$

So, $End(V)$ satisfies the all properties of ring.$End(V)$ is a ring under $+$ and $\cdot$.

□

Problem 2 (3/10, *Injectivity of ring homomorphisms on a field*): Let $V \neq 0$ be a vector space over a field F and let $\sigma : F \to End(V)$ be its associated ring homomorphism. Show that if $0 \neq c \in F$, then $\sigma(c)$ can not be the zero element of $End(V)$. More generally, show that if $R \neq 0$ is any ring and $\tau : F \to R$ is any ring homomorphism, then $\tau(c) = 0 \Rightarrow c = 0$.

Proof. If $\exists c \in F$ and $c \neq 0$, $\sigma(c) = 0_{End(V)}$, we have that,

$$\begin{aligned} \forall a \in F \quad \sigma(c \cdot a) &= \sigma(c) \cdot \sigma(a) \\ &= 0_{End(V)} \cdot \sigma(a) \\ &= 0_{End(V)} \end{aligned}$$

Actually, we have

$$\begin{aligned} \forall f \in F \quad \exists c \in F \quad f = ac \\ \rightarrow \forall f \in F \quad \sigma(f) = 0_{End(V)} \end{aligned}$$

So, $End(V)$ is a zero ring. And if $End(V)$ is not a zero ring, we have $\forall f \in F$: $\sigma(f) \neq 0_{End(V)}$, except $c = 0$.Now I will show that.
Let 0 be identity element of F. And we can say that,

$$\forall c \in F \quad c + 0 = 0 + c = c$$

Let $c \neq 0$,so,

$$\begin{aligned} \sigma(c + 0) &= \sigma(c) + \sigma(0) \\ \sigma(c) &= \sigma(c) + \sigma(0) \end{aligned}$$

Because

$$\begin{aligned} \forall c \in F : \sigma(c) + 0_{End(V)} &= 0_{End(V)} + \sigma(c) = \sigma(c) \\ \sigma(0) &= 0_{End(V)} \end{aligned}$$

So, we can give a conclusion that if $End(V)$ is not a zero ring, $\forall 0 \neq c \in F \rightarrow \sigma(c)$ can not be the zero element of $End(V)$.
More generally, by contrary, supposed $\exists c \in R$ and $c \neq 0$ let $\tau(c) = 0$

$$\begin{aligned} \forall a \in R \quad \exists b \in R &: a = b \cdot c \\ \tau(b \cdot c) &= \tau(b) \cdot \tau(c) \\ &= \tau(b) \cdot 0 \\ &= 0 \\ \rightarrow \tau(a) &= 0 \end{aligned}$$

So F is a zero ring. Contraty to condition. And if $a = 0$ we have $\tau(0)$ always equals to 0. We can conclude that

$$\tau(c) = 0 \rightarrow c = 0$$

Done. $\square$

Problem 3 (3/10, *An adventure in ring theory*): Let R be a commutative ring with additive identity 0 and multiplicative identity 1. Let r be a nilpotent element of R, i.e., there exists a positive integer n such that $r^n = 0$. Show that the element $u := r + 1$ is an unit of R, i.e., show that there exists some element $p \in R$, such that $up = 1$. Terminology: the set of invertible elements of a ring is a group, known as the group of units of the ring. Thus the group of units of a field is the entire field except the zero element.

Proof. It means that there always is a inverse if $u = r+1$. Because the properties of the ring. We can say that.

$$\begin{aligned} u \cdot 1 &= u \\ &= r + 1 \qquad (1) \\ r + 0 &= r \end{aligned}$$

Let $n = 2$, then we have

$$r^2 = 0 \tag{2}$$

$$\begin{aligned} u \cdot r &= (r+1) \cdot r \\ &= r^2 + r \end{aligned} \tag{3}$$

Bring (2) into (3), we can get

$$u \cdot r = r \tag{4}$$

Then (1) minus (4),

$$u \cdot 1 - u \cdot r = 1$$

And R is a commutative ring with multiplicative.

$$u \cdot (1 - r) = 1$$
$$(1 - r) \cdot u = 1$$

And we can easily get $1 - r \in R$. Finally, we can say $u := r + 1$ is an unit of R.
And the inverse of u is $1 - r$.
Done. $\square$