Math 309 – Intermediate Linear Algebra Homework 2 Xida Ren

(Due Friday, February 9)

Each problem will be graded out of 10 points.

1. Is $\mathbb{Q}[\sqrt{5}] := \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$ a field?

Proof. Because $\mathbb{Q}[\sqrt{5}]$ is a subset of the $\mathbb{R}$, we have assocativity and commutativity of addition and multiplication, and distributivity of multiplication over addition. The identity elements for addition and multiplication are in $\mathbb{R}$, so setting $a = 0, b = 0$ and $a = 1, b = 0$ would give us these.

Now, two properties remain: addition and multiplication have to be closed, and they have to have inverses in $\mathbb{Q}[\sqrt{5}]$.

Closedness

Let x, y be any two members of $\mathbb{Q}[\sqrt{5}]$. Find a_x, b_x, a_y, b_y such that $x = a_x + b_x\sqrt{5}, y = a_y + b_y\sqrt{5}$.

$\mathbb{Q}[\sqrt{5}]$ is closed under addition because the rationals are closed under addition and

$$x + y = (a_x + a_y) + (b_x + b_y)\sqrt{5}$$

.

$\mathbb{Q}[\sqrt{5}]$ closed under multiplication because the rationals are closed under addition and

$$x \cdot y = (a_x + b_x\sqrt{5})(a_y + b_y\sqrt{5}) = (a_x a_y + 5b_x b_y) + (a_x b_y + a_y b_x)\sqrt{5}$$

.

Inverses

The additive inverse of $a + b\sqrt{5}$ is just $-a - b\sqrt{5}$. $a + b\sqrt{5} + (a - b\sqrt{5}) = 0 + 0\sqrt{5}$.

The multiplicative inverse is a bit interesting. Multiplying $a + b\sqrt{5}$ by $a - b\sqrt{5}$ gives us $a^2 - 5b^2$, an integer with a multiplicative inverse $e \in \mathbb{Q}$.

So the multiplicative inverse of $a + b\sqrt{5}$ is just $e(a - b\sqrt{5})$.

e always exists because no pair of rationals a, b can satisfy $a^2 = 5b^2$: let $\frac{m}{n}$ be the most reduced integer-fraction representation of $\frac{a}{b}$. We have

$$5 = \frac{m^2}{n^2}$$

.

Now, we show that no integers m and n exist to satisfy this equation.

First, observe that since the result of this division is an integer, all prime factors of n are also prime factors of m. Second, because the fraction is in its most reduced form, m and n can share no common factors. So $n = 1$ because 1 is the only number without prime factors.

But this means that $5 = m^2$ where m is an integer, which is impossible: the square function is monotonously increasing for positive numbers, and we have $2^2 = 4 < 5 < 9 = 3^2$.

So there does not exist rationals a, b such that $a^2 = 5b^2$ and $a^2 - 5b^2$ would never be 0 for rationals a, b.

□

2. (a) Is $\mathbb{Z}_7[\sqrt{5}] := \{a + b\sqrt{5} : a, b \in \mathbb{Z}_7\}$ a field?
(b) Is $\mathbb{Z}_{11}[\sqrt{5}] := \{a + b\sqrt{5} : a, b \in \mathbb{Z}_{11}\}$ a field?

(a) Yes.

Proof. We first prove that addition and multiplication have commutativity, assocativity, and distributivity by proving that we could take things to $\mathbb{Q}[\sqrt{5}]$ and back for our addition and multiplication operations. We then prove that we have closedness, identities, and inverses.

Our operations are defined in the same way as operations in $\mathbb{Q}[\sqrt{5}]$, except after each operation we close the set by bringing the rational and root-5 parts of a number back between 0 and 6 by dividing by 7 and taking the remainder. Call this double-remainder-taking operation R, and note two things:
$R(a + b\sqrt{5}) = R(a) + R(b)\sqrt{5}$ for any a, b, and $R(a + 7k) = R(a)$ for an integer k.

Addition and multiplication are closed because integers add and multiply to integers, and $\sqrt{5} \times \sqrt{5}$ is an integer. Thus when we apply R to the sum or products of two numbers of form $a + b\sqrt{5}$, we get a number of the same form with $a, b \in \mathbb{Z}_7$.

Addition has all the requisite properties, including the identity element and the inverse elements, because $\mathbb{Z}_[\sqrt{5}]$ can actually be seen as two copies of $\mathbb{Z}_7$ bound together.

So our real problem is multiplication. Commutativity comes easy: we apply the remainder operation R to the result of the multiplication, so switching the operands should not matter.

Assocativity can be proven using assocativity in $\mathbb{Z}[\sqrt{5}]$: we take our map R from $\mathbb{Z}[\sqrt{5}]$ to $\mathbb{Z}_7[\sqrt{5}]$ and prove that it preserves assocativity. First, we have $R(x \cdot R(y)) = R(x \cdot y)$: Let $C_{1,2,3,4}$ are be integer quotients whose value could be arbitrary. Then,

$$\begin{aligned}
R(x \cdot R(y)) &= R(x \cdot (r(a_y) + r(b_y)\sqrt{5})) \\
&= R(a_x r(a_y) + b_x r(b_y) + (a_x r(b_y) + b_x r(a_y))\sqrt{5}) \\
&= r(a_x r(a_y) + b_x r(b_y)) + r\left(a_x r(b_y) + b_x r(a_y)\right)\sqrt{5} \\
&= r(a_x(a_y + 7C_1) + b_x(b_y + 7C_2)) + r\left(a_x(b_y + 7C_3) + b_x(a_y + 7C_4)\right)\sqrt{5} \\
&= r(a_x a_y + b_x b_y + 7(a_x C_1 + b_x C_2)) + r\left(a_x b_y + b_x a_y + 7(a_x C_3 + b_x C_4)\right)\sqrt{5} \\
&= r(a_x a_y + b_x b_y) + r(a_x b_y + b_x a_y)\sqrt{5} \\
&= R(x \cdot y)
\end{aligned}$$

Now, if we perform the $\mathbb{Z}[sqrt5]$ multiplication over three members of $\mathbb{Z}[\sqrt{5}]$ but apply R after each multiplication, we can show that we'll get the same result no matter how we order the multiplications:

$$\begin{aligned} R(x \cdot R(y \cdot z)) &= R(x \cdot (y \cdot z)) \\ &= R((x \cdot y) \cdot z) \\ &= R(z \cdot (x \cdot y)) \\ &= R(z \cdot R(x \cdot y)) \\ &= R(R(x \cdot y) \cdot z) \end{aligned}$$

so we have commutativity.

Now, the only thing that remains is the multiplicative inverse. This is the real jucy part of the problem. Consider $a + b\sqrt{5} \in \mathbb{Z}_7[\sqrt{5}]$. We show that as long as $a + b\sqrt{5} \neq 0$, we always have a multiplicative inverse.

If $a + b\sqrt{5}$ is not 0, then $a - b\sqrt{5}$ is not 0 either. Multiplying them together gives $a^2 - 5b^2 \in \mathbb{Z}_7$. If this number has an inverse e in $\mathbb{Z}_7$, we can say $(a - b\sqrt{5})(a + b\sqrt{5})e = 1$. Because $\mathbb{Z}_7$ is a field, its only member without a multiplicative inverse is 0, so we now show that for any $a, b \in \mathbb{Z}_7$, $a^2 - 5b^2 = 0$ is impossible when neither of a, b is 0.

Assume $a, b \neq 0$. In the field $\mathbb{Z}_7$, $a^2 - 5b^2 = 0$ means $a^2 = 5b^2$. Because a, b both have multiplicative inverses, we can say $\frac{a^2}{b^2} = 5$, which means that $(\frac{a}{b})^2 = 5$. But this is impossible, since no number squares to 5 in $\mathbb{Z}_7$.

Hence we have the multiplicative inverse.

I wonder if I could have used something to make this proof easier? Also, what are these called, these cyclic something plus something squareroot something sets?

□

(b) No.

In fields, there are no zero divisors, but in $\mathbb{Z}_{11}[\sqrt{5}]$, we can do this:

$$\begin{aligned} (1 + 3\sqrt{5}) \cdot (1 + 8\sqrt{5}) &= 1 + 120 + 11\sqrt{5} \\ &= 121 + 11\sqrt{5} \\ &= 0 + 0\sqrt{5} \in \mathbb{Z}_{11}[\sqrt{5}] \end{aligned}$$

This has something to do with how $7^2 = 49 = 5 \mod 11$, which means that 5 has a square root in $\mathbb{Z}_{11}$, making it impossible for us to execute the same proof as for $\mathbb{Z}_7[\sqrt{5}]$.

A *zero divisor* x of a field $\mathbb{F}$ is a nonzero element such that there exists another nonzero element $y \in \mathbb{F}$ and $xy = 0$.

3. Prove that a field has no *zero divisors*, that is, if $x, y \in \mathbb{F}$ and $xy = 0$, then either $x = 0$ or $y = 0$.

Proof. Assume $y \neq 0$ and $xy = 0$. We prove that $x = 0$. The other case is automatically proven by symmetry due to commutativity.

Because $y \neq 0$, by F3 it has a multiplicative inverse z such that $yz = 1$. Right-multiply z to both sides of $xy = 0$ to get $(xy)z = (0)z$.

By assocativity, $(xy)z = x(yz)$. Because z is the multiplicative inverse of y, $(yz) = 1$. So we can then apply the definition of the identity to get $x(yz) = x(1) = x$.

Now since $(xy)z = 0z = 0$ and $(xy)z = x$, we have proven that $x = 0$.

□

A real-valued function f defined on the real numbers is called an *even function* if $f(-t) = f(t)$ for each $t \in \mathbb{R}$.

4. Prove that the set $\mathcal{E}$ of even functions defined on the real line with operations

$$(f + g)(t) := f(t) + g(t),$$

$$(cf)(s) := c \cdot (f(s)),$$

where $c \in \mathbb{R}$, is a vector space over $\mathbb{R}$.

Proof. Functions are defined by the real numbers they yield for each input. Because real numbers have commutative and assocative addition, we have

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x)$$

and

$$(f + (g + h))(x) = f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x) = ((f + g) + h)(x)$$

.

Similarly, because real number multiplication is assocative and distributive, we have

$$(a(bf))(x) = a(bf(x)) = (ab)f(x) = ((ab)f)(x)$$

and

$$(a(f + g))(x) = a(f(x) + g(x)) = af(x) + ag(x) = (af + ag)(x)$$

. We have the multiplicative identitiy 1 because $1 \cdot f(x) = f(x)$.

So we only need to check closure under the two operations, the existance of the zero element, and the existance of the additive inverse for each element.

Adding two even functions gives an even function: because $f(-x) = f(x)$ and $g(-x) = g(x)$, we have:

$$(f + g)(-x) = f(-x) + g(-x) = f(x) + g(x) = (f + g)(x)$$

.

Multiplying an even function by a scalar also gives an even function: $f(-x) = f(x)$ implies $cf(-x) = cf(x)$.

The zero element is just the zero function $z(x) = 0$ for all x. It's easy to see how $(z + f)(x) = 0 + f(x) = f(x)$ for all functions f in our vector space. Also note that the zero function is even.

Finaly, the additive inverse can be found by multiplying any function by -1.
$(f + (-1)f)(x) = f(x) + (-1)f(x) = (1 - 1)f(x) = 0f(x) = 0$ for all x, giving the zero function. The additive inverse is also even by our result that scalar multiples of even functions are even.

□

Let $\mathbb{F}$ be a field. A *sequence* in $\mathbb{F}$ is a function σ from the positive integers into $\mathbb{F}$, and, if $\sigma(n) = a_n \in \mathbb{F}$ for $n \in \mathbb{N}$, then the sequence is denoted by $\{a_n\}$.

5. Let V consist of all sequences $\{a_n\}$ of elements of $\mathbb{F}$. For any $\{a_n\}, \{b_n\} \in V$ and any $c \in \mathbb{F}$, define

$$\{a_n\} + \{b_n\} := \{a_n + b_n\},$$
$$c \cdot \{a_n\} := \{ca_n\}.$$

Is V a vector space over $\mathbb{F}$?

Yes.

Proof. Commutativity and assocativity of addition is guaranteed by commutativity in the field: for each n,

$$a_n + b_n = b_n + a_n$$
$$a_n + (b_n + c_n) = (a_n + b_n) + c_n$$

.

Scalar multiplication is also assocative because $x(y(a_n)) = (xy)a_n$ for each n.

Distributivity comes similarly: for each n,

$$c(a_n + b_n) = ca_n + cb_n$$

.

The multiplicative identity is 1 in the field: $1a_n = a_n$ for all n.

The additive identity is a sequence $\{z_n\}$ where $z_n = 0$ for all n. Then, for any sequence $\{a_n\}$ and for any n, $a_n + z_n = a_n + 0 = 0$.

Additive inverses are implied by the above properties: for all n,
$a_n + (-1)a_n = (1 + -1)a_n = 0 = z_n$. □

6. Let V be a vector space over a field $\mathbb{F}$.

(a) Prove that the 0 vector in V is unique, that is, if 0 and e are both additive identities of V, then $e = 0$.

Proof. Because e is an additive identity,

$$e + 0 = 0$$

And because 0 is also an additive identity,

$$0 + e = e$$

And by commutativity of addition, we have $0 + e = e + 0$, so $e = 0$. □

(b) If $x \in V$, prove that the additive inverse of x is unique, that is, if y and z in V satisfy $x + y = 0$ and $x + z = 0$, then $y = z$.

Proof. Adding z to both sides of the first equation, we have

$$(x + y) + z = 0 + z = z$$

and adding y to both sides of the second, we get

$$(x + z) + y = 0 + y = y$$

Now by commutativity and assocativity the leftmost expression in both equation chains are equal, so

$$y = z$$

. □