MA294 Lecture

Timothy Kohl

Boston University

March 21, 2024

Fields from Matrices

Definition

Let $S_2(\mathbb{R}) = \{\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \in \mathbb{R}\} \subseteq M_2(\mathbb{R})$.

Observe that

$$\begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} + \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 & y_1 + y_2 \\ -(y_1 + y_2) & x_1 + x_2 \end{pmatrix}$$

$$\begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} = \begin{pmatrix} x_1 x_2 - y_1 y_2 & x_1 y_2 + x_2 y_1 \\ -(x_1 y_1 + x_2 y_1) & x_1 x_2 - y_1 y_2 \end{pmatrix}$$

Also note that $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ are in $S_2(\mathbb{R})$ so $S_2(\mathbb{R})$ is a ring.

Note also, that the elements in $S_2(\mathbb{R})$ commute.

Moreover, note that $det \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = x^2 + y^2$ which means that every every non-zero element (matrix) in $S_2(\mathbb{R})$ is invertible.

So it seems that $S_2(\mathbb{R})$ is a field, and indeed it is, in fact $S_2(\mathbb{R}) \cong \mathbb{C}$ where the bijection is

$$\psi : \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mapsto x + iy$$

which respects the addition *and* multiplication.

i.e. $\psi(M+N) = \psi(M) + \psi(N)$ and $\psi(MN) = \psi(M)\psi(N)$.

What's also intriguing is that this construction can be done for finite fields, namely $S_2(\mathbb{Z}_p)$ where the matrix elements come from $\mathbb{Z}_p$ instead of $\mathbb{R}$, that is:

$$S_2(\mathbb{Z}_p) = \{\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \in \mathbb{Z}_p\} \subseteq M_2(\mathbb{Z}_p)$$

where all the comments about the case for $\mathbb{R}$ work here too.. except for one issue.

Recall that $det \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = x^2 + y^2$, which was zero (for the case of $\mathbb{R}$) when $x = y = 0$, however, in $\mathbb{Z}_5$ for example, $1^2 + 2^2 = 5 \equiv 0 \ (mod\ 5)$ so that $\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$ is a non-zero element which is non-invertible since $det = 0$, so $S_2(\mathbb{Z}_5)$ is not a field.

However, $S_2(\mathbb{Z}_3)$ *is* a field (with 9 elements) as is $S_2(\mathbb{Z}_7)$ (which has 49 elements).

As it turns out $S_2(\mathbb{Z}_p)$ is a field if and only if $p \equiv 3 \ (mod\ 4)$.

We saw earlier the definition of the complex numbers:

$$
\begin{aligned}
\mathbb{C} &= \{a + b\ i \mid a, b \in \mathbb{R},\ i^2 = -1\} \\
(a + bi) + (c + di) &= (a + c) + (b + d)i \\
(a + bi)(c + di) &= (ac - bd) + (ad + bc)i \\
(0 + 0i) + (a + bi) &= a + bi \\
(1 + 0i)(a + bi) &= a + bi
\end{aligned}
$$

where, in particular, the multiplication is keyed to the fact that $i^2 = -1$.

Moreover, $\mathbb{C}$ can also be viewed as a vector space in that every $z \in \mathbb{C}$ is of the form $z = a + bi = a \cdot 1 + b \cdot i$.

i.e. every element of $\mathbb{C}$ is a linear combination of $\{1, i\}$

This begs the question as to whether one could generalize this idea, and indeed there is, but there are some startling contrasts in comparison to $\mathbb{C}$.

The Quaternions (Hamiltonians) as a set is

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

namely linear combinations of $\{1, i, j, k\}$ (so that $\mathbb{H}$ is additively just like the vector space $\mathbb{R}^4$) but where the i, j, k have the following properties:

$$\begin{aligned} 1 \cdot i = i,\ 1 \cdot j = j,\ 1 \cdot k = k \\ i^2 = j^2 = k^2 = -1 \\ ij = k,\ jk = i,\ ki = j \\ ji = -k,\ kj = -i,\ ik = -j \end{aligned}$$

where a product $(a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k)$ is expanded out and simplified according to the rules governing 1, i, j, and k as above.

One may (with some effort!) verify that $\mathbb{H}$ is a ring, with additive identity $0 + 0i + 0j + 0k$ and multiplicative identity $1 + 0i + 0j + 0k$.

The other properties (such as associativity) are messy to check, but do hold.

One of the principal observations is that $\mathbb{H}$ is a non-commutative ring, which stems of course from the rules governing how the 'basis' elements are multiplied.

The similarity to $\mathbb{C}$ is obvious in that j and k are two other 'square roots of -1' but what is a lso interesting is the following similarity with $\mathbb{C}$ which we'll discuss in more generality later.

If $z = a + bi \in \mathbb{C}$ where $(a, b) \neq (0, 0)$ we saw that

$$z^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i \in \mathbb{C}$$

which means that $\mathbb{C}$ is a *field*.

In a similar way although requiring a bit more work :-),one may show that every non-zero $h = a + bi + cj + dk \in \mathbb{H}$ has a multiplicative inverse as well.

However, as $\mathbb{H}$ is non-commutative, we use the term division ring to characterize $\mathbb{H}$.

We'll talk more about fields later on.

Polynomials

Definition

If R is a commutative ring and x a variable, the polynomial ring $R[x]$ is the set of all expressions of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where $n \geq 0$ is an integer, and each $a_i \in R$, where if $a_n \neq 0$ we say $deg(f) = n$. Addition is defined degree by degree, namely

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\ g(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \\ &\downarrow \text{ assuming } n \geq m \\ f(x) + g(x) &= (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0) \end{aligned}$$

where for $t > m$ we view $b_t = 0$.

Definition

Multiplication is as follows:

$$f(x)\cdot g(x) = (a_n b_m)x^{n+m} + \cdots + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + (a_0 b_1 + a_1 b_0)x + a_0 b_0$$

.Also 0 (i.e. the constant polynomial) is the additive identity and $1 \in R$ is the multiplicative identity.

If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ (i.e. $a_n = 1$) then we say $f(x)$ is a monic polynomial.

We also note that if R is $\mathbb{Z}$ or a field like $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or even $\mathbb{Z}_p$ then

$$deg(f(x) + g(x)) \leq max\{deg(f(x)), deg(g(x))\}$$
$$deg(f(x) \cdot g(x)) = deg(f(x)) + deg(g(x))$$

If $R = \mathbb{Z}_m$ for m not a prime then it is possible to have $deg(f(x) \cdot g(x)) \leq deg(f(x)) + deg(g(x))$.

For example, in $\mathbb{Z}_6[x]$ we have

$$\begin{aligned}(3x^2 + 2x + 1)(2x^2 + 1) &= 6x^4 + 4x^3 + 2x^2 + 3x^2 + 2x + 1 \\ &= 4x^3 + 5x^2 + 1\end{aligned}$$

where this happened because the product of the leading coefficients '3' and '2' equals $6 \equiv 0$ in $\mathbb{Z}_6$.

Indeed, this is more a point about the arithmetic in $\mathbb{Z}_6$ since for the two non-zero elements 2 and 3, their product $2 \cdot 3$ is zero in $\mathbb{Z}_6$.

In contrast, this never happens in $\mathbb{Z}_p$. (More on this later.)

Polynomial Long Division

Just as one can divide one integer by another to yield a unique quotient and remainder. The same holds true for the ring $F[x]$ for any field F.

Theorem

The Division Algorithm for $F[x]$

Let F be a field and let $f(x), g(x) \in F[x]$ where $g \neq 0$ then there exists unique $q(x), r(x) \in F[x]$ such that

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

where either $r(x) = 0$ or $deg(r(x)) < deg(g(x))$.

Proof:

Assume that $deg(f(x)) \geq deg(g(x))$ otherwise, having $f(x) = q(x)g(x) + r(x)$ would imply that $q(x) = 0$ and $r(x) = f(x)$.

Assuming this, then we use an 'inductive' argument keyed to the degree of $f(x)$.

If $deg(f(x)) = 1$ then $f(x) = ax + b$ so $g(x) = c$ (a constant) and therefore $ax + b = (\frac{a}{c}x)c + b$ so $q(x) = (\frac{a}{c}x)$ and $r(x) = b$, i.e. $deg(r(x)) = 0$.

Proof (continued)

If

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

where $a_n \neq 0$ and $b_m \neq 0$ then $m < n$ so let $t = n - m$ and define $q_1(x) = c_t x^t$ where $c_t = \frac{a_n}{b_m}$.

Then

$$\begin{aligned} q_1(x)g(x) &= (b_m \frac{a_n}{b_m})x^n + \dots \\ &= a_n x^n + \dots \end{aligned}$$

which means $deg(f(x) - q_1(x)g(x)) < n$ so by induction we may assume the theorem holds for $f(x) - q_1(x)g(x)$.

So there exists polynomials $q_2(x)$ and $r(x)$ such that $f(x) - q_1(x)g(x) = q_2(x)g(x) + r(x)$ which means

$$f(x) = (q_2(x) + q_1(x))g(x) + r(x) = q(x)g(x) + r(x)$$

i.e. $q(x) = q_1(x) + q_2(x)$ so that indeed, we have a quotient '$q(x)$' and a remainder '$r(x)$' so that $f(x) = q(x)g(x) + r(x)$.

Proof (continued)

The last part to check is that if $f(x) = q(x)g(x) + r(x)$ and $f(x) = \tilde{q}(x)g(x) + \tilde{r}(x)$ that $\tilde{q}(x) = q(x)$ and $\tilde{r}(x) = r(x)$.

But this implies that

$$\begin{aligned} f(x) - f(x) &= (q(x)g(x) + r(x)) - (\tilde{q}(x)g(x) + \tilde{r}(x)) \\ &= (q(x) - \tilde{q}(x))g(x) + (r(x) - \tilde{r}(x)) \end{aligned}$$

but $f(x) - f(x) = 0$ so, by degree considerations $q(x) - \tilde{q}(x) = 0$ and $r(x) - \tilde{r}(x) = 0$ so $q(x) = \tilde{q}(x)$ and $r(x) = \tilde{r}(x)$. $\square$