MA294 Lecture

Timothy Kohl

Boston University

July 19, 2021

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

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

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 $r(x) = \tilde{r}(x)$. □

Factorization of Polynomials

In the Division Algorithm, when $f(x) = q(x)g(x) + r(x)$, if $r(x) = 0$ then $f(x) = q(x)g(x)$ so that $g(x)$ evenly divides $f(x)$ and we have a factorization of $f(x)$ into two *lower degree* polynomials.

We begin with a basic result relating factors with roots.

Definition

If $f(x) \in R[x]$ where say $f(x) = a_n x^n + \cdots + a_1 x + a_0$ then for $\alpha \in R$ one has

$$f(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0$$

which is the result of evaluating $f(x)$ at $x = \alpha$ which yields an element of R.

Note: If $f(x) = x - \alpha$ then clearly $f(\alpha) = 0$.

Theorem

Let F be a field, and suppose $f(x) \in F[x]$ then $x - \alpha$ is a divisor of $f(x)$ if and only if $f(\alpha) = 0$.

Proof.

Assume $deg(f(x)) \geq 1$ then $f(x) = q(x)(x - \alpha) + r(x)$ for some $q(x)$, $r(x)$ so that $f(\alpha) = q(\alpha)(\alpha - \alpha) + r(\alpha)$ which equals $r(\alpha)$.

However $deg(r(x)) < deg(x - \alpha) = 1$ so $r(x)$ is constant, which means $r(x) = 0$. □

Note, if $f(\beta) = 0$ for some $\beta \in F$ as well, then if $\alpha \neq \beta$

$$f(x) = q(x)(x - \alpha)$$
$$\downarrow$$
$$f(\beta) = q(\beta)(\beta - \alpha)$$

so that $f(\beta) = 0$ if and only if $q(\beta) = 0$ meaning that $q(x) = \tilde{q}(x)(x - \beta)$ so, concordantly $f(x) = \tilde{q}(x)(x - \beta)(x - \alpha)$ where $deg(f(x)) = n$ implies $deg(q(x)) = n - 1$ and therefore $deg(\tilde{q}(x)) = n - 2$.

The result of this is the following fact about the roots (potentially repeated) of a polynomial $f(x)$.

Theorem

If F is a field and $f(x) \in F[x]$ where $deg(f(x)) = n$ then $f(x)$ has at most n distinct roots.

In general, finding roots/factors of a polynomial $f(x) \in \mathbb{R}[x]$ is difficult if $deg(f(x)) \geq 5$ since there are no explicit formulas, except for $deg(f(x)) = 2, 3, 4$.

Of course, trial and error can sometimes lead to factorizations of larger degree polynomials.

What about polynomials in $\mathbb{Z}_p[x]$.

Observation: For a given degree n, there are $(p-1)p^n$ polynomials of degree n since if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ then $a_n \neq 0$ but each $a_i \in \mathbb{Z}_p$ for $i = 0, \ldots, n-1$.

So, in principal one could take a given $f(x) \in \mathbb{Z}_p[x]$ and look at all $q(x), g(x) \in \mathbb{Z}_p[x]$ such that $deg(q(x)) + deg(g(x)) = deg(f(x))$ and compute $q(x)g(x)$ to see if it equals $f(x)$.
e.g.

$$f(x) = ax^2 + bx + c$$
$$g(x) = dx + f$$
$$q(x) = hx + k$$

For simplicity though, we can assume that if

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

and $f(\alpha) = 0$ then if

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

where $\tilde{f}(\alpha) = 0$ too.

i.e. One can restrict attention to monic polynomials.

So in $\mathbb{Z}_p[x]$ we have say

$$\begin{aligned} f(x) &= x^2 + ax + b \\ &= (x-\alpha)(x-\beta) \end{aligned}$$

where there are p^2 monic quadratics $f(x)$, so we can ask, how many of these are irreducible, that is *not* factorable as $(x-\alpha)(x-\beta)$.

Since $(x-\alpha)(x-\beta) = (x-\beta)(x-\alpha)$ then there are

$$\underbrace{\frac{1}{2}p(p-1)}_{\alpha \neq \beta} + \underbrace{p}_{\alpha=\beta} = \frac{p^2+p}{2}$$

monic quadratics that are factorable.

As such there are $\frac{p^2-p}{2}$ irreducible (monic) quadratic polynomials $\mathbb{Z}_p$ polynomials.

Note: Sometimes a polynomial will have irreducible factors that are not linear. (degree 1)

Example: $x^4 + 1 \in \mathbb{Z}_3[x]$ is factorable as $(x^2 + x + 2)(x^2 + 2x + 2)$ but neither are linear, and neither are themselves factorable.

Why? Simply plug in $x = 0, 1, 2$ into $q(x) = x^2 + x + 2$ you get

$$q(0) = 2$$
$$q(1) = 1$$
$$q(2) = 2$$

and similarly $x^2 + 2x + 2$ has no roots in $\mathbb{Z}_3$ either.

Finite Fields

As $\mathbb{Z}_p$ is a field, we use the notation $\mathbb{F}_p$ to emphasize the fact that it's a field, albeit one with finitely many elements.

We shall now consider a (actually the) finite field with $9 = 3^2$ elements.

Consider $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$ and observe that $f(0) = 1$, $f(1) = 2$, and $f(2) = 2$ which implies that $f(x)$ is irreducible.

Moreover, consider what happens if we take an arbitrary $p(x) \in \mathbb{F}_p[x]$ and divide it by $x^2 + 1$, i.e.

$$p(x) = q(x)(x^2 + 1) + r(x)$$

where $r(x) = 0$, or $deg(r(x)) < deg(x^2 + 1) = 2$

This means that $r(x) = ax + b$ for some $a, b \in \mathbb{F}_3$ and this is the case regardless of the degree of $p(x)$, so

$$r(x) \in \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

so there are $3^2 = 9$ different remainders.

Consider the parallel with dividing an arbitrary integer n by a *fixed* integer (modulus) m to yield $n = qm + r$ where $r \in \{0, 1, \ldots, m-1\}$ which leads to the construction of the ring $\mathbb{Z}_m$.

We can make $\mathbb{F}_9 = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$ into a ring as well.

First, the addition is simply

$$\underbrace{(ax+b)}_{\in \mathbb{F}_9} + \underbrace{(a'x+b')}_{\in \mathbb{F}_9} = (a+a')x + (b+b') \in \mathbb{F}_9$$

and when we multiply according to the following rule, which stems from the roots of the polynomial $x^2 + 1 = 0$, namely $x^2 = -1 = 2$.

Thus

$$(ax+b)(a'x+b') = aa'x^2 + ab'x + a'bx + bb' = (ab'+a'b)x + (2aa'+bb') \in \mathbb{F}_9$$

and $0 = 0x + 0$ and $1 = 0x + 1$ are the additive and multiplicative identity elements.

In order to establish that $\mathbb{F}_9$ is a field, we need to show that each non-zero element has a multiplicative inverse, for example $(x+1)(x+2) = x^2 + 3x + 2 = x^2 + 2 = 2 + 2 = 1$.

By direct calculation:

$$\begin{aligned} 1^{-1} &= 1 \\ (x+1)^{-1} &= x+2 \\ (2x+1)^{-1} &= 2x+2 \\ 2^{-1} &= 2 \\ (x+2)^{-1} &= x+1 \\ (2x+2)^{-1} &= 2x+1 \\ x^{-1} &= 2x \\ (2x)^{-1} &= x \end{aligned}$$

So $\mathbb{F}_9$ is a field.

In general, one can argue as follows:

Definition

A commutative ring with unity R is a domain (or integral domain) if, for $x, y \in R$, $xy = 0$ implies that $x = 0$ or $y = 0$, or both.

In a domain, one can show that if $x \neq 0$ then $xy = xz$ implies $y = z$.

Why? If $xy = xz$ then $xy - xz = 0$ that is $x(y - z) = 0$.

But being a domain, if $x \neq 0$ then $x(y - z) = 0$ implies that $y - z = 0$, but then $y = z$.

The relevence to $\mathbb{F}_9$ is the following useful fact due to Weddeburn.

Theorem

If R is an integral domain where $|R|$ is finite, then R is a field.

Proof.

Consider $R - \{0\} = \{r_1, r_2, \ldots, r_n\}$ where, we may assume $r_1 = 1$. So now, pick any element $r \in R - \{0\}$ (i.e. $r = r_i$ for some i) and consider $\{rr_1, rr_2, \ldots, rr_n\}$.

We note that $rr_j = rr_k$ implies $r_j = r_k$ because R is a domain, so $\{rr_1, rr_2, \ldots, rr_n\}$ is a permutation of $R - \{0\}$ and so, for some r_j we have $rr_j = 1$ since $1 \in R - \{0\}$. Thus, r has an inverse. □

So applied to $\mathbb{F}_9$ we can easily show that it is a domain (just check the rule for multiplication) and so we can infer it's a field by Weddeburn's theorem.

Another way to view $\mathbb{F}_9$ is by the observation that 'x' in $\mathbb{F}_9$ has the property that $x^2 = 2 = -1$ which is very analgous to the imaginary unit i which has the property that $i^2 = -1$.

The analogy we draw is that $a + bx \leftrightarrow a + bi$ so that $\mathbb{F}_9$ is $\mathbb{F}_3$ with 'i' adjoined, just as $\mathbb{C}$ is $\mathbb{R}$ with 'i' adjoined to 'enlarge' it.

We can also compute powers of elements of the *group* $U(\mathbb{F}_9) = \mathbb{F}_9^*$,

$$
\begin{aligned}
(2x+1)^0 &= 1 \\
(2x+1)^1 &= 2x+1 \\
(2x+1)^2 &= x \\
(2x+1)^3 &= x+1 \\
(2x+1)^4 &= 2 \\
(2x+1)^5 &= x+2 \\
(2x+1)^6 &= 2x \\
(2x+1)^7 &= 2x+2 \\
(2x+1)^8 &= 1
\end{aligned}
$$

which shows that $U(\mathbb{F}_9) = \langle 2x+1 \rangle$, i.e. a cyclic group.