Math 620: §4.1 Fields; Roots of Polynomials

Due on Friday, November 20, 2015

Boynton 10:00

Kailee Gray

4.1: 2,6,9,11,13,17,18

Exercise 4.1.2: Let p be a prime number and let n be a positive integer. How many polynomials are there of degree n over $\mathbb{Z}_p$?

Consider some polynomial over $\mathbb{Z}_p$ of degree n: $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Then, $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}_p$ so there are p choices for each of the $n+1$ a_i's with the exception of a_n. Since $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ has degree n, the leading coefficient must be non-zero; thus there are $p-1$ choices for a_n. Hence, there are $p^n(p-1)$ possible polynomials of degree n over $\mathbb{Z}_p$.

Exercise 4.1.6: Let p be a prime number. Find all roots of $x^{p-1} - 1$ in $\mathbb{Z}_p$.

By corollary 1.4.12 (Fermat), since p is prime, $x^p \equiv x \pmod{p}$ for any integer x. We are looking for roots in $\mathbb{Z}_p$ so consider $x \pmod{p}$. Then, $x \in \mathbb{Z}_p$ and so $\gcd(x,p) = 1$ which allows us, as long as $x \neq 0$, to divide both sides of $x^p \equiv x \pmod{p}$ by x to obtain $x^{p-1} \equiv 1 \pmod{p}$. This is equivalent to $x^{p-1} - 1 \equiv 0 \pmod{p}$. Thus, any $x \in \mathbb{Z}_p$, except $x = 0$, is a root of $x^{p-1} - 1$ in $\mathbb{Z}_p$.

Exercise 4.1.9: Let a be a nonzero element of a field F. Show that $(a^{-1})^{-1} = a$ and $(-a)^{-1} = -a^{-1}$.

Proof. Let a be a nonzero element of a field F. Since a is nonzero, a^{-1} and $(a^{-1})^{-1}$ exist;

$$\begin{aligned}
(a^{-1})^{-1} &= (a^{-1})^{-1} \\
(a^{-1})^{-1}a^{-1} &= (a^{-1})^{-1}a^{-1} \\
1 &= (a^{-1})^{-1}a^{-1} \\
1a &= (a^{-1})^{-1}a^{-1}a \\
a &= (a^{-1})^{-1}.
\end{aligned}$$

Since a is nonzero, $-a$ is nonzero and $(-a)^{-1}$ exists such that $(-a)^{-1}(-a) = 1$;

$$\begin{aligned}
(-a)^{-1}(-a) &= 1 \\
-(-a)^{-1}a &= 1 \\
-(-a)^{-1}a(-a^{-1}) &= 1(-a^{-1}) \\
-(-(-a)^{-1}a(a^{-1})) &= -a^{-1} \\
(-a)^{-1} &= -a^{-1}
\end{aligned}$$

□

Exercise 4.1.11: Show that the set $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ is closed under addition, subtraction, multiplication, and division.

Proof. Consider $a + b\sqrt{3}, c + d\sqrt{3} \in \mathbb{Q}(\sqrt{3})$.

(addition) Then, $a + b\sqrt{3} + c + d\sqrt{3} = a + c + (b + d)\sqrt{3}$. Since addition in $\mathbb{Q}$ is closed, $a + c \in \mathbb{Q}$ and $b + d \in \mathbb{Q}$. Thus, $\mathbb{Q}(\sqrt{3})$ is closed under addition.

(subtraction) Then, $(a+b\sqrt{3})-(c+d\sqrt{3}) = a-c+(b-d)\sqrt{3} = a+(-c)+(b+(-d))\sqrt{3}$. $c, d \in \mathbb{Q}$ implies $-c, -d \in \mathbb{Q}$. Addition in $\mathbb{Q}$ is closed so $a + (-c) \in \mathbb{Q}$ and $b + (-d) \in \mathbb{Q}$. Thus, $\mathbb{Q}(\sqrt{3})$ is closed under subtraction.

(multiplication) Note $(a+b\sqrt{3})(c+d\sqrt{3}) = ac+(bc)\sqrt{3}+(ad)\sqrt{3}+(bd)3 = ac+3bd+(bc+ad)\sqrt{3}$. Multiplication and addition in $\mathbb{Q}$ is closed so $a, b, c, d \in \mathbb{Q}$ implies $ac+3bd, bc+ad \in \mathbb{Q}$. Therefore, $ac + 3bd + (bc + ad)\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Thus, $\mathbb{Q}(\sqrt{3})$ is closed under multiplication.

(division) Note $c + d\sqrt{3} \neq 0$ and

$$\frac{a + b\sqrt{3}}{c + d\sqrt{3}} = \frac{a + b\sqrt{3}}{c + d\sqrt{3}} \cdot \frac{c - d\sqrt{3}}{c - d\sqrt{3}} = \frac{ac - 3bd + (bc - ad)\sqrt{3}}{c^2 - 3d^2} = \frac{ac - 3bd}{c^2 - 3d^2} + \frac{bc - ad}{c^2 - 3d^2}\sqrt{3}$$

Multiplication, addition, and subtraction is closed in $\mathbb{Q}$ and division is closed in $\mathbb{Q} - \{0\}$ so $a, b, c, d \in \mathbb{Q}$ implies $\frac{ac-3bd}{c^2-3d^2} \in \mathbb{Q}$ and $\frac{bc-ad}{c^2-3d^2} \in \mathbb{Q}$ as long as $c^2 - 3d^2 \neq 0$. Suppose $c^2 - 3d^2 = 0$. Then, $c^2 = 3d^2$ and $c = \pm\sqrt{3}d$. Notice $\sqrt{3}$ is an irrational number so $\sqrt{3}d$ is irrational as long as $d \neq 0$. Since $c = \pm\sqrt{3}d$, if $d = 0$, $c = 0$, but $c + d\sqrt{3} \neq 0$. Thus, c^2 is irrational which implies c is irrational. However, $c + d\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ implies $c, d \in \mathbb{Q}$. Hence, $c^2 - 3d^2 \neq 0$. Thus, $\mathbb{Q}(\sqrt{3})$ is closed under division. $\square$

Exercise 4.1.13: Show Let $F = \left\{ \textbf{all matrices of the form } \begin{bmatrix} a & b \\ -b & a \end{bmatrix},\ a, b \in \mathbb{R} \right\}$ is a field under the operations of matrix addition and multiplication.

Proof. Consider $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}, \begin{bmatrix} c & d \\ -d & c \end{bmatrix}, \begin{bmatrix} e & f \\ -f & e \end{bmatrix} \in F$ with $a, b, c, d, e, f \in \mathbb{R}$.

(closure, +)

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} \in F \text{ since } a+c, b+d \in \mathbb{R}$$

(closure, $\cdot$)

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} \in F \text{ since } ac-bd, ad+bc \in \mathbb{R}$$

(associative, +)

$$\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \right) + \begin{bmatrix} e & f \\ -f & e \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} + \begin{bmatrix} e & f \\ -f & e \end{bmatrix} = \begin{bmatrix} (a+c)+e & (b+d)+f \\ -(b+d)-f & (a+c)+e \end{bmatrix}$$

$$= \begin{bmatrix} a+(c+e) & b+(d+f) \\ -b-(d+f) & a+(c+e) \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c+e & d+f \\ -(d+f) & c+e \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix} + \begin{bmatrix} e & f \\ -f & e \end{bmatrix} \right)$$

(associative, $\cdot$)

$$\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \right) \cdot \begin{bmatrix} e & f \\ -f & e \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} \cdot \begin{bmatrix} e & f \\ -f & e \end{bmatrix} =$$

$$\begin{bmatrix} e(ac-bd)-f(ad+bc) & e(ad+bc)+f(ac-bd) \\ -e(ad+bc)-f(ac-bd) & e(ac-bd)-f(ad+bc) \end{bmatrix} =$$

$$\begin{bmatrix} eac-ebd-fad-fbc & ead+ebc+fac-fbd \\ -ead-ebc-fac+fbd & eac-ebd-fad-fbc \end{bmatrix} =$$

$$\begin{bmatrix} a(ec-fd)-b(ed+fc) & a(ed+fc)+b(ec-fd) \\ -a(ed+fc)-b(ec-fd) & a(ec-fd)-b(ed+fc) \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} ec-fd & ed+fc \\ -(ed+fc) & ec-fd \end{bmatrix} =$$

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix} \cdot \begin{bmatrix} e & f \\ -f & e \end{bmatrix} \right)$$

(commutative, $+$)

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} = \begin{bmatrix} c+a & d+b \\ -(d+b) & c+a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} + \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

(commutative, $\cdot$)

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} = \begin{bmatrix} ca-db & cb+da \\ -(da+cb) & -bd+ca \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \cdot \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

(distributive from the right)

$$\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \right) \cdot \begin{bmatrix} e & f \\ -f & e \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} \cdot \begin{bmatrix} e & f \\ -f & e \end{bmatrix} =$$

$$\begin{bmatrix} ae+ce-fb-fd & af+cf+be+de \\ -be-de-af-cf & -bf-df+ae+ce \end{bmatrix} = \begin{bmatrix} ae-bf & af+be \\ -be-af & -bf+ae \end{bmatrix} + \begin{bmatrix} ce-df & cf+de \\ -de-cf & -df+ce \end{bmatrix} =$$

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} e & f \\ -f & e \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \cdot \begin{bmatrix} e & f \\ -f & e \end{bmatrix}$$

(distributive from the left)

$$\begin{bmatrix} e & f \\ -f & e \end{bmatrix} \cdot \left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \right) = \begin{bmatrix} e & f \\ -f & e \end{bmatrix} \cdot \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} =$$

$$\begin{bmatrix} ea+ec-fb-fd & eb+ed+fa+fc \\ -fa-fc-eb-ed & -fb-fd+ea+ec \end{bmatrix} = \begin{bmatrix} ea-fb & eb+fa \\ -fa-eb & -fb+ea \end{bmatrix} + \begin{bmatrix} ec-fd & ed+fc \\ -fc-ed & -fd+ec \end{bmatrix} =$$

$$\begin{bmatrix} e & f \\ -f & e \end{bmatrix} \cdot \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} e & f \\ -f & e \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$

(identity, $+$) For any element in F,

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a+0 & b+0 \\ -b+0 & a+0 \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

(identity, $\cdot$) For any element in F,

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \text{. and } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

(inverse, $+$) Notice $-1 \cdot \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = -\begin{bmatrix} -a & -b \\ b & -a \end{bmatrix}$. Then,

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + -1 \cdot \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{. and } -1 \cdot \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

(inverse, $\cdot$) We will show for any $A \in F$, $A \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $A^{-1} = \frac{1}{a^2+b^2} \cdot \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. Note b, a are not both 0, so $a^2 + b^2 \neq 0$. Thus, $A^{-1} \in F$ and:

$$\frac{1}{a^2+b^2} \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \frac{1}{a^2+b^2} \begin{bmatrix} a^2+b^2 & -ab+ba \\ -ba+ab & b^2+a^2 \end{bmatrix} = \frac{1}{a^2+b^2} \begin{bmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Since $(F, \cdot)$ is commutative,

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \cdot \frac{1}{a^2+b^2} \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus, $(F, +, \cdot)$ is a field. $\square$

Exercise 4.1.17: Let $(x_0, y_0), (x_1, y_1), (x_2, y_2)$ be points in the Euclidean plane $\mathbb{R}^2$ such that x_0, x_1, x_2 are distinct. Show that

$$f(x) = \frac{y_0(x-x_1)(x-x_2)}{(x_0-x_1)(x_0-x_2)} + \frac{y_1(x-x_0)(x-x_2)}{(x_1-x_0)(x_1-x_2)} + \frac{y_2(x-x_0)(x-x_1)}{(x_2-x_0)(x_2-x_1)}$$

defines a polynomial $f(x)$ such that $f(x_0) = y_0$, $f(x_1) = y_1$, and $f(x_2) = y_2$.

Proof. Because multiplication and addition are closed in $\mathbb{R}$ and because x_0, x_1, x_2 are distinct and division is closed in $\mathbb{R} - \{0\}$, we can see that the expansion of $f(x)$ will yield a degree 2 polynomial with coefficients in $\mathbb{R}$. Next, compute $f(x_0), f(x_1)$, and $f(x_2)$:

$$f(x_0) = \frac{y_0(x_0-x_1)(x_0-x_2)}{(x_0-x_1)(x_0-x_2)} + \frac{y_1(x_0-x_0)(x_0-x_2)}{(x_1-x_0)(x_1-x_2)} + \frac{y_2(x_0-x_0)(x_0-x_1)}{(x_2-x_0)(x_2-x_1)} = \frac{y_0(x_0-x_1)(x_0-x_2)}{(x_0-x_1)(x_0-x_2)} = y_0$$

$$f(x_1) = \frac{y_0(x_1-x_1)(x_1-x_2)}{(x_0-x_1)(x_0-x_2)} + \frac{y_1(x_1-x_0)(x_1-x_2)}{(x_1-x_0)(x_1-x_2)} + \frac{y_2(x_1-x_0)(x_1-x_1)}{(x_2-x_0)(x_2-x_1)} = \frac{y_1(x_1-x_0)(x_1-x_2)}{(x_1-x_0)(x_1-x_2)} = y_1$$

$$f(x_2) = \frac{y_0(x_2-x_1)(x_2-x_2)}{(x_0-x_1)(x_0-x_2)} + \frac{y_1(x_2-x_0)(x_2-x_2)}{(x_1-x_0)(x_1-x_2)} + \frac{y_2(x_2-x_0)(x_2-x_1)}{(x_2-x_0)(x_2-x_1)} = \frac{y_2(x_2-x_0)(x_2-x_1)}{(x_2-x_0)(x_2-x_1)} = y_2.$$

Thus, $f(x)$ satisfies the given conditions. $\square$

Exercise 4.1.18: Use Lagrange's interpolation formula to find a polynomial $f(x)$ such that $f(1) = 0$, $f(2) = 1$, and $f(3) = 4$.

Then, $x_0 = 1, y_0 = 0, x_1 = 2, y_1 = 1, x_2 = 3, y_2 = 4$, so applying Lagrange's interpolation formula, we have

$$f(x) = \frac{0(x-2)(x-3)}{(1-2)(1-3)} + \frac{1(x-1)(x-3)}{(2-1)(2-3)} + \frac{4(x-1)(x-2)}{(3-1)(3-2)} = -(x-1)(x-3) + 2(x-2)(x-2)$$

$$= (x-1)(-x+3+2x-4) = (x-1)(x-1) = x^2 - 2x + 1.$$

By inspection, we can see that $f(x) = x^2 - 2x + 1$ satisfies the given conditions.