Fields

Tim Smits

*Starred problems are optional problems that relate the concepts to other areas of math.

1. Check that $\mathbb{Q}$ is a field by carefully verifying the field axioms.

2. Below are a list of vector spaces that you saw in lecture:

   (i) $\mathbb{R}[x]$

   (ii) $\mathbb{R}(x)$

   (iii) $\mathbb{R}^2$

   (iv) $\text{Mat}_{2\times 2}(\mathbb{R})$

   Each space has a natural multiplication operation, e.g. multiplication in $\mathbb{R}[x]$ is the usual multiplication of polynomials, while multiplication in $\mathbb{R}^2$ is defined pointwise, i.e. $(a, b) \cdot (c, d) = (ac, bd)$, and so on. For each space, answer the following:

   (a) Identify what the "0" and "1" element are.

   (b) Is the space a field? If so, explain why (but not necessarily rigorously), and if not, explicitly give a counter-example to one of the field axioms.

3.* Polynomial arithmetic over finite fields works as you would expect it to. E.g., the polynomial $f(x) = x^2 + \bar{2} \in \mathbb{F}_3[x]$ has roots at $\bar{1}$ and $\bar{2}$, because $f(\bar{1}) = f(\bar{2}) = \bar{0}$, so $f(x)$ factors as $(x + \bar{1})(x + \bar{2})$.

   Let $f(x) = (x^2 + \overline{16})(x^2 + \overline{13}) \in \mathbb{F}_p[x]$, where p is one of the primes listed below. For each choice of p, find all the roots of $f(x)$, and factor $f(x)$ further, if possible.

   (i) $p = 2$

   (ii) $p = 3$

   (iii) $p = 5$

   (iv) $p = 7$

4.* The polynomial $x^2 + 1$ has no real root, so is *irreducible* over $\mathbb{R}$ (meaning $x^2 + 1 \in \mathbb{R}[x]$ cannot factor further). By defining a symbol i with $i^2 + 1 = 0$, we can construct a "larger" field $\mathbb{C}$ where $x^2 + 1$ has a root, where by "larger" we mean in the sense that $\mathbb{R} \subset \mathbb{C}$. Below, we will mimic the construction with a finite field instead.

   (a) List all the degree 2 polynomials in $\mathbb{F}_2[x]$, and show that $x^2 + x + \bar{1}$ is the only irreducible one.

   Define a symbol α with the property $\alpha^2 + \alpha + \bar{1} = \bar{0}$, and consider the set $S = \{a + b\alpha : a, b \in \mathbb{F}_2\}$. Explicitly as a set, we have $S = \{\bar{0}, \bar{1}, \alpha, \alpha + \bar{1}\}$, and addition and multiplication work similarly to that of $\mathbb{C}$, except now we have the algebraic relation $\alpha^2 = \alpha + \bar{1}$ instead of $i^2 = -1$.

   (b) Write down the addition and multiplication tables for S.

   Your tables in (b) will show that S is a field with 4 elements, which we will now denote $\mathbb{F}_4$. The complex numbers $\mathbb{C}$ have the property that every non-constant polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$ (i.e. $\mathbb{C}$ is *algebraically closed*).

(c) Show that $\mathbb{F}_4$ is *not* algebraically closed by explicitly finding a polynomial $f(x) \in \mathbb{F}_4[x]$ that does not have a root in $\mathbb{F}_4$. (Hint: look for a quadratic polynomial).

Solutions

1. We'll take our definition of $\mathbb{Q}$ to be $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$ with operations given by $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, where two fractions $\frac{a}{b}$ and $\frac{c}{d}$ are considered equal if $ad = bc$.

   F1 Pick $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. Then $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{cd}$, while $\frac{c}{d} + \frac{a}{b} = \frac{cb+da}{db}$. Since the addition and multiplication in the numerator and denominator are happening in $\mathbb{Z}$ and we know addition/multiplication there is commutative, we can appropriately swap everything, so $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{b}{a}$. Similarly, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}$.

   F2 Pick $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$. Then $(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{(ad+bc)f+(bd)e}{(bd)f} = \frac{adf+bcf+bde}{bdf}$. On the other hand, $\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} + \frac{cf+de}{df} = \frac{a(df)+b(cf+de)}{b(df)} = \frac{adf+bcf+bde}{bdf}$. Here we use the fact that multiplication distributes over addition in the integers, and multiplication of integers is associative. Similarly, we have $(\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{(ac)e}{(bd)f} = \frac{ace}{bdf}$ while $\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a(ce)}{b(df)} = \frac{ace}{bdf}$.

   F3 It's clear from the definition of addition and multiplication that $\frac{0}{1}$ and $\frac{1}{1}$ satisfy the definition of the "0" and "1" element for a field, respectively.

   F4 For any $\frac{a}{b} \in \mathbb{Q}$, we have $\frac{a}{b} + \frac{-a}{b} = \frac{ab-ba}{b^2} = \frac{ab-ab}{b^2} = \frac{0}{b^2} = \frac{0}{1}$, because we know what additive inverses in the integers look like. The last equality follows from what it means for rational numbers to be equal. If $\frac{a}{b} \neq \frac{0}{1}$, then $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = \frac{1}{1}$.

   F5 Pick $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$. We have $\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \cdot \frac{cf+de}{df} = \frac{a(cf+de)}{b(df)} = \frac{acf+ade}{bdf}$ because multiplication in the integers is associative/distributes. On the other hand, $\frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{(ac)(bf)+(bd)(ae)}{(bd)(bf)} = \frac{b(acf+ade)}{b^2df} = \frac{acf+ade}{bdf}$ (again, we use that multipliation in the integers works nicely, and the last equality follows from what it means for two rational numbers to be equal).

2. (i) $\mathbb{R}[x]$ is not a field, because x is not invertible. To explicitly see this, if x was invertible, then by definition it has some multiplicative inverse, say $f(x) \in \mathbb{R}[x]$, so that $xf(x) = 1$. Then plugging in $x = 0$ says $0 = 1$, which is clearly false. (Note that $\frac{1}{x}$ is *not* a polynomial, because by definition polynomials can only contain non-negative powers of x).

   (ii) $\mathbb{R}(x)$ is a field; the same proof that $\mathbb{Q}$ is a field generalizes.

   (iii) $\mathbb{R}^2$ is not a field; $(1,0) \cdot (0,1) = (0,0)$, so $(1,0)$ (also $(0,1)$) is not invertible.

   (iv) $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ is not a field. Matrix multiplication is not commutative: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, while $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. (Note that the first computation shows that neither of these matrices have multiplicative inverses).

3. (i) Roots: $\bar{0}, \bar{1}$ and $f(x) = x^2(x+\bar{1})^2$.

   (ii) Roots: No roots, and $f(x) = (x^2+\bar{1})^2$.

   (iii) Roots: $\bar{2}, \bar{3}$ and $f(x) = (x+\bar{2})(x+\bar{3})(x^2+\bar{3})$.

   (iv) Roots: $\bar{1}, \bar{6}$ and $f(x) = (x+\bar{1})(x+\bar{6})(x^2+\bar{2})$.

4. (a) $x^2, x^2+\bar{1}, x^2+x, x^2+x+\bar{1}$ are the four degree two polynomials of $\mathbb{F}_2[x]$. The first three all have a root, while the last one does not (just plug in $\bar{0}$ and $\bar{1}$ to check).

(b)

$+$	$\bar{0}$	$\bar{1}$	α	$\alpha+\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	α	$\alpha+\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\alpha+\bar{1}$	α
α	α	$\alpha+\bar{1}$	$\bar{0}$	$\bar{1}$
$\alpha+\bar{1}$	$\alpha+\bar{1}$	α	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$	α	$\alpha+\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	α	$\alpha+\bar{1}$
α	$\bar{0}$	α	$\alpha+\bar{1}$	$\bar{1}$
$\alpha+\bar{1}$	$\bar{0}$	$\alpha+\bar{1}$	$\bar{1}$	α

(c) Consider $f(x) = x^2 + x + \alpha + \bar{1}$. This is irreducible, because it has no root in $\mathbb{F}_4$: we check $f(\bar{0}) = \alpha + \bar{1}$, $f(\bar{1}) = \alpha + \bar{1}$, $f(\alpha) = \alpha$ and $f(\alpha + \bar{1}) = \alpha$.