

2.2 Finite Fields from Modular Arithmetic

Every field of Section 2.1 is infinite. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* has already met finite ones: it proved that the integers modulo a prime p form a field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.2). This section restates that result in the language of Definition 2.1.1, gives these fields a name of their own, $\mathbb{F}_p$, and computes in them: inverses, linear equations, and the elimination method of Section 2.1, now run modulo p . Finite fields are not a curiosity; coding theory and computer algebra do linear algebra over them every day.

2.2.1 Arithmetic modulo n , recalled

Fix an integer $n \geq 1$. The ring $\mathbb{Z}/n\mathbb{Z}$ of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.4.2 consists of the classes $[a]$ of integers a under congruence modulo n , and two classes are equal exactly when their representatives differ by a multiple of n :

$$[a] = [b] \iff n \mid a - b.$$

This is the class test of *Number Systems* (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1 (a), read with Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.4.2). Sums and products are computed on representatives. The first example collects what is known about this arithmetic, in the language of Definition 2.1.1.

Example. Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$

Let $n \geq 1$, and define $[a] + [b] := [a + b]$ and $[a][b] := [ab]$ for $a, b \in \mathbb{Z}$. Show that these operations are well defined, that they satisfy every clause of Definition 2.1.1 except possibly (F8) and the condition $1 \neq 0$ in (F7), and that $[1] \neq [0]$ holds exactly when $n \geq 2$. Then write out the addition and multiplication tables for $n = 2$.

Solution. All of this was proved in *Number Systems*, and we collect it.

Well-definedness. The formulas use representatives, so the answer must not depend on which representatives are chosen. For the ideal $n\mathbb{Z}$ of $\mathbb{Z}$ this is Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1 (b), and $\mathbb{Z}/n\mathbb{Z}$ is defined as that quotient (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.4.2).

The clauses. By Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (a), $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with zero $[0]$ and one $[1]$: clauses (F1)–(F6) and (F9) hold, and so does (F7) without the condition $1 \neq 0$. The negative of $[a]$ is $[-a]$, since $[a] + [-a] = [a + (-a)] = [0]$.

The condition $1 \neq 0$. By Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (c), $[1] \neq [0]$ if and only if $n \geq 2$. For $n = 1$ every class equals $[0]$, and $\mathbb{Z}/1\mathbb{Z}$ is the zero ring.

Size. By Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (b), each class is $[r]$ for exactly one $r \in \{0, 1, \dots, n-1\}$, the remainder of any representative on division by n . So $\mathbb{Z}/n\mathbb{Z}$ has exactly n elements.

The tables for $n = 2$. Write 0 and 1 for $[0]$ and $[1]$. Since $1 + 1 = 2$ and $2 - 0 = 2 \cdot 1$, the

class test gives $[1] + [1] = [2] = [0]$; the other entries are read off directly:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Here (F8) holds as well: the only non-zero element is 1, and $1 \cdot 1 = 1$. So $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$ is a field. In it $1 + 1 = 0$, and therefore $-1 = 1$.

The tables of $\mathbb{F}_2$ are those of the two-element field of Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Example (A field with two elements that cannot be ordered), with 0 and 1 read as classes. The one surprise is $1 + 1 = 0$: it says that 2 is even, and nothing more. It is also the field promised by the warning on order in Section 2.1, where “ $1 + 1 \neq 0$ ” fails.

2.2.2 Which moduli give fields

For $n \geq 2$, whether $\mathbb{Z}/n\mathbb{Z}$ is a field now comes down to one clause, (F8): does every non-zero class have an inverse? An inverse of $[a]$ is a class $[x]$ with $[ax] = [1]$, that is, an integer x with $n \mid ax - 1$, that is, integers x, y with $ax + ny = 1$. Such a combination is what Bézout’s theorem produces. The linear-algebra volumes cite it in the following special form.

Lemma 2.2.1. Bézout’s Lemma for Integers

Let $a, n \in \mathbb{Z}$ with $n \geq 1$, and suppose that the only positive integer dividing both a and n is 1. Then there are $x, y \in \mathbb{Z}$ with

$$ax + ny = 1.$$

Proof. Since $n \geq 1$, $(a, n) \neq (0, 0)$, so $g := \gcd(a, n)$ is a common divisor of a and n with $g \geq 1$ (Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Definition 3.2.2 and the well-definedness paragraph after it). By hypothesis, $g = 1$. So a and n are coprime, and Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Corollary 3.2.2 gives $x, y \in \mathbb{Z}$ with $ax + ny = 1$. ■

The general statement, for any pair of integers not both zero and with $\gcd(a, n)$ in place of 1, is Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Theorem 3.2.1; the Euclidean algorithm computes the x and y . We keep the special case under its own name because the linear-algebra volumes cite it in this form.

Theorem 2.2.2. $\mathbb{Z}/n\mathbb{Z}$ Is a Field Exactly for Prime n

Let $n \geq 2$ be an integer. Then $\mathbb{Z}/n\mathbb{Z}$ is a field (Definition 2.1.1) if and only if n is prime.

Idea. By Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$), only (F8) is in question. If $n = p$ is prime and $[a] \neq [0]$, then $p \nmid a$, so the only positive common divisor of a and p is 1, and Lemma 2.2.1 hands over $ax + py = 1$, that is, $[a][x] = [1]$. If instead $n = rs$ with $1 < r, s < n$, then $[r][s] = [n] = [0]$ with both factors non-zero, which Theorem 2.1.1 (f) forbids in a field. Number Systems ran this argument, with Number Systems: From $\backslash(\backslash n N \backslash)$

to $\mathbb{Z}/n\mathbb{Z}$, Theorem 3.5.1 in the role of the lemma.

Proof. By Number Systems: From $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$, Theorem 3.5.2, $\mathbb{Z}/n\mathbb{Z}$ is a field in the sense of Number Systems: From $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$, Definition 2.3.1 if and only if n is prime. By the remark after Definition 2.1.1, a field in that sense is the same as a field in the sense of Definition 2.1.1. This proves the theorem. ■

So for each prime p there is a field with exactly p elements, and for each composite $n \geq 4$ the ring $\mathbb{Z}/n\mathbb{Z}$ is not a field. The fields deserve a short name.

2.2.3 The fields with p elements

Definition 2.2.1. The Field $\mathbb{F}_p$

Let p be a prime. The field $\mathbb{F}_p$ is $\mathbb{Z}/p\mathbb{Z}$, with the operations of [Example \(Arithmetic on \$\mathbb{Z}/n\mathbb{Z}\$ and the Field \$\mathbb{F}_2\$ \)](#). It has exactly p elements (Number Systems: From $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$, Theorem 3.4.3 (b)), which we write $0, 1, \dots, p-1$, without brackets: the number $r \in \{0, \dots, p-1\}$ stands for the class $[r]$. For integers a, b , “ $a = b$ in $\mathbb{F}_p$ ” means $[a] = [b]$, that is, $p \mid a - b$.

So $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_{11}, \dots$ are fields, by [Theorem 2.2.2](#), while $\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$ are not. To decide that a given p is prime, the remark after Number Systems: From $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$, Lemma 3.3.4 says it is enough to check that no $d \geq 2$ with $d \cdot d \leq p$ divides p .

Computing in $\mathbb{F}_p$ is computing with integers and replacing the answer by its remainder on division by p . The words “in $\mathbb{F}_p$ ” must be said whenever an equation would be false in $\mathbb{Z}$: “ $3 \cdot 5 = 1$ in $\mathbb{F}_7$ ” is true, because $15 - 1 = 2 \cdot 7$; “ $3 \cdot 5 = 1$ ” alone is false. Every result of Section 2.1 now holds in $\mathbb{F}_p$. For instance, by Corollary 2.1.2 the only elements of $\mathbb{F}_p$ whose square is 1 are 1 and $-1 = p-1$.

Quick check. Find the inverse of 3 in $\mathbb{F}_7$.

Solution. The inverse is the $x \in \{1, \dots, 6\}$ with $7 \mid 3x - 1$. Testing the candidates in turn, the products 3, 6, 9, 12, 15 leave remainders 3, 6, 2, 5, 1, and $3 \cdot 5 = 15 = 2 \cdot 7 + 1$. So $3^{-1} = 5$ in $\mathbb{F}_7$, and by Theorem 2.1.1 (c) it is the only inverse.

For small p , trial is fast. For larger p the Euclidean algorithm of *Number Systems* finds the inverse directly: if $ax + py = 1$, then $\gcd(a, p) = 1$ by Number Systems: From $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$, Corollary 3.2.2, and Number Systems: From $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$, Theorem 3.5.1 gives $[a]^{-1} = [x]$.

Example. Inverses in $\mathbb{F}_7$ and in $\mathbb{F}_{101}$

- (i) List the inverses of the non-zero elements of $\mathbb{F}_7$. (ii) Find the inverse of 17 in $\mathbb{F}_{101}$.

Solution.

- (i) In $\mathbb{F}_7$:

$$1 \cdot 1 = 1, \quad 2 \cdot 4 = 8 = 1, \quad 3 \cdot 5 = 15 = 1, \quad 6 \cdot 6 = 36 = 1,$$

since $8 - 1 = 7$, $15 - 1 = 2 \cdot 7$ and $36 - 1 = 5 \cdot 7$. So $1^{-1} = 1$, $2^{-1} = 4$, $4^{-1} = 2$, $3^{-1} = 5$, $5^{-1} = 3$, $6^{-1} = 6$, using (F6) for the reversed pairs. Each element of $\mathbb{F}_7^\times := \mathbb{F}_7 \setminus \{0\}$ appears exactly once as an inverse, as it must: the inverse of a^{-1} is a (Theorem 2.1.1 (g)), so two elements with the same inverse are equal. The elements 1 and 6 = -1 are their own inverses, and by Corollary 2.1.2 no others are.

- (ii) First, 101 is prime, by the criterion recalled after Definition 2.2.1: no d with $2 \leq d \leq 10$ divides it (the remainders of 101 on division by 2, 3, ..., 10 are 1, 2, 1, 1, 5, 3, 5, 2, 1), and $11 \cdot 11 = 121 > 101$. Run the Euclidean algorithm on (101, 17):

$$101 = 5 \cdot 17 + 16, \quad 17 = 1 \cdot 16 + 1.$$

Back-substitute from the last line:

$$1 = 17 - 16 = 17 - (101 - 5 \cdot 17) = 6 \cdot 17 - 101.$$

So $17 \cdot 6 + 101 \cdot (-1) = 1$, hence $\gcd(17, 101) = 1$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 3.2.2), and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.1 gives $17^{-1} = 6$ in $\mathbb{F}_{101}$. Check: $17 \cdot 6 = 102 = 101 + 1$.

Since $\mathbb{F}_p$ is a field, each result of Section 2.1 about equations holds there word for word; what changes is how the numbers are computed. An elimination of the same kind as Section 2.1's opening one, done over $\mathbb{F}_5$, looks like this.

Example. Elimination over $\mathbb{F}_5$

Solve the system $2x + y = 3$, $3x + 2y = 4$ over $\mathbb{F}_5$.

Solution. In $\mathbb{F}_5$ the inverses are $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$ and $4^{-1} = 4$, since $2 \cdot 3 = 6 = 5 + 1$ and $4 \cdot 4 = 16 = 3 \cdot 5 + 1$.

By elimination. Scale the first equation by $2^{-1} = 3$. In $\mathbb{F}_5$, $3 \cdot 2 = 1$, $3 \cdot 1 = 3$ and $3 \cdot 3 = 9 = 4$, so the scaled equation reads $x + 3y = 4$. Taking 3 times it away from the second equation removes x and leaves

$$(2 - 9)y = 4 - 12, \quad \text{that is,} \quad 3y = 2 \quad \text{in } \mathbb{F}_5,$$

since $-7 = -10 + 3$ and $-8 = -10 + 2$. Multiply by $3^{-1} = 2$: $y = 4$. Then $x = 4 - 3y = 4 - 12 = -8 = 2$ in $\mathbb{F}_5$.

By the formula. With $a = 2$, $b = 1$, $c = 3$, $d = 2$, $e = 3$, $f = 4$, the coefficient $ad - bc =$

$4 - 3 = 1$ is non-zero, so Proposition 2.1.3 (b) applies:

$$x = \frac{3 \cdot 2 - 1 \cdot 4}{1} = 2, \quad y = \frac{2 \cdot 4 - 3 \cdot 3}{1} = -1 = 4 \text{ in } \mathbb{F}_5.$$

The two methods agree. Check: $2 \cdot 2 + 4 = 8 = 3$ and $3 \cdot 2 + 2 \cdot 4 = 14 = 4$ in $\mathbb{F}_5$. By Proposition 2.1.3 (b), $(x, y) = (2, 4)$ is the only solution.

Quick check. Which elements $x \in \mathbb{F}_{11}$ satisfy $x^2 = 1$?

Solution. Exactly 1 and 10. By Corollary 2.1.2, $x^2 = 1$ if and only if $x = 1$ or $x = -1$, and $-1 = 10$ in $\mathbb{F}_{11}$, since $10 - (-1) = 11$. Check: $10^2 = 100 = 9 \cdot 11 + 1$.

Warning. A non-zero class of $\mathbb{Z}/n\mathbb{Z}$ need not have an inverse. In $\mathbb{Z}/6\mathbb{Z}$ the equation $[2]x = [1]$ has **no** solution, since $[2]x$ is always one of $[0], [2], [4]$; and $[2]x = [4]$ has **two** solutions, $x = [2]$ and $x = [5]$ (as $10 - 4 = 6$). So division by $[a]$ modulo n is allowed when n is prime and $[a] \neq [0]$, or more generally when $\gcd(a, n) = 1$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 3.5.1), and not otherwise.

Remark (No order on $\mathbb{F}_p$). For $n \geq 2$, no relation $<$ makes $\mathbb{Z}/n\mathbb{Z}$ an ordered commutative ring (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 3.4.3 (e). So the inequalities of *Number Systems* have no meaning in $\mathbb{F}_p$, as the warning on order in Section 2.1 said. The representatives $0, 1, \dots, p-1$ are ordered as integers, but that order is not compatible with the arithmetic: $0 < p-1$ as integers, and adding 1 to both sides would give $1 < 0$, since $(p-1) + 1 = 0$ in $\mathbb{F}_p$.

2.2.4 Exercises

2.2.4.1 A. Check your understanding

Exercise. A1

- (a) True or false: $\mathbb{Z}/8\mathbb{Z}$ is a field. Justify your answer.
- (b) List the inverses of $1, 2, 3, 4$ in $\mathbb{F}_5$.
- (c) Compute $4 \cdot 4 + 3$ in $\mathbb{F}_5$.
- (d) True or false: $x^2 = x$ for every $x \in \mathbb{F}_2$.
- (e) How many elements does $\mathbb{F}_{13}$ have, and is $13 = 0$ in $\mathbb{F}_{13}$?

Solution.

- (a) False. $8 = 2 \cdot 4$ is not prime, so Theorem 2.2.2 applies; concretely $[2][4] = [8] = [0]$ with $[2] \neq [0]$ and $[4] \neq [0]$, which Theorem 2.1.1 (f) forbids in a field.

- (b) $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$, as in [Example \(Elimination over \$\mathbb{F}_5\$ \)](#).
- (c) $4 \cdot 4 + 3 = 19 = 3 \cdot 5 + 4$, so the answer is 4.
- (d) True: $0 \cdot 0 = 0$ and $1 \cdot 1 = 1$ in $\mathbb{F}_2$. (This agrees with Exercise (B1) (c): the solutions of $x^2 = x$ in any field are 0 and 1, and $\mathbb{F}_2$ has no other elements.)
- (e) 13 is prime (neither 2 nor 3 divides it, and $4 \cdot 4 = 16 > 13$), so $\mathbb{F}_{13}$ is defined and has 13 elements. And $13 = 0$ in $\mathbb{F}_{13}$, since $13 \mid 13 - 0$.

2.2.4.2 B. Practice

Exercise. B1

- (a) Solve $3x + 5 = 2$ in $\mathbb{F}_7$.
- (b) Solve the system $x + 2y = 3$, $3x + y = 1$ over $\mathbb{F}_7$.

Solution.

- (a) Adding -5 to both sides gives $3x = 2 - 5 = -3 = 4$ in $\mathbb{F}_7$. Since $3 \cdot 5 = 15 = 1$ in $\mathbb{F}_7$, $3^{-1} = 5$, and Proposition 2.1.3 (a) gives $x = 5 \cdot 4 = 20 = 6$. Check: $3 \cdot 6 + 5 = 23 = 3 \cdot 7 + 2$.
- (b) Here $a = 1$, $b = 2$, $c = 3$, $d = 1$, $e = 3$, $f = 1$, and $ad - bc = 1 - 6 = -5 = 2 \neq 0$ in $\mathbb{F}_7$. Since $2 \cdot 4 = 8 = 1$, $2^{-1} = 4$. By Proposition 2.1.3 (b),

$$x = (3 \cdot 1 - 2 \cdot 1) \cdot 4 = 4, \quad y = (1 \cdot 1 - 3 \cdot 3) \cdot 4 = -32 = 3,$$

since $-32 = -5 \cdot 7 + 3$. Check: $4 + 2 \cdot 3 = 10 = 3$ and $3 \cdot 4 + 3 = 15 = 1$ in $\mathbb{F}_7$. Hence $(x, y) = (4, 3)$, and it is the only solution.

Exercise. B2: Which Are Fields?

Determine which of $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{F}_5$, $\mathbb{Z}/1\mathbb{Z}$ and $\mathbb{Z}/91\mathbb{Z}$ are fields. Justify your answer.

Solution. $\mathbb{Z}/9\mathbb{Z}$: **not a field**, since $[3][3] = [9] = [0]$ with $[3] \neq [0]$, against Theorem 2.1.1 (f). $\mathbb{F}_5$: **a field**, by [Theorem 2.2.2](#), since 5 is prime. $\mathbb{Z}/1\mathbb{Z}$: **not a field**, since $[1] = [0]$ there ([Example \(Arithmetic on \$\mathbb{Z}/n\mathbb{Z}\$ and the Field \$\mathbb{F}_2\$ \)](#)), against the condition $1 \neq 0$ of (F7). $\mathbb{Z}/91\mathbb{Z}$: **not a field**, since $91 = 7 \cdot 13$ is not prime ([Theorem 2.2.2](#)); concretely $[7][13] = [91] = [0]$.

Exercise. B3

Find all solutions of $x^2 = 2$ in $\mathbb{F}_7$, and all solutions of $x^2 = 2$ in $\mathbb{F}_5$.

Solution. In $\mathbb{F}_7$, $3^2 = 9 = 2$. By Corollary 2.1.2, $x^2 = 2 = 3^2$ holds exactly for $x = 3$ and $x = -3 = 4$. Check: $4^2 = 16 = 2 \cdot 7 + 2$.

In $\mathbb{F}_5$ the squares of 0, 1, 2, 3, 4 are 0, 1, 4, 9 = 4, 16 = 1. None is 2, so $x^2 = 2$ has no solution in $\mathbb{F}_5$.

2.2.4.3 C. Going deeper

Exercise. C1: A Field with Four Elements

Let F be the set of formal expressions $a + b\alpha$ with $a, b \in \mathbb{F}_2$: four symbols 0, 1, α and $\beta := 1 + \alpha$, where $a + b\alpha = c + d\alpha$ means $a = c$ and $b = d$. Define

$$\begin{aligned}(a + b\alpha) + (c + d\alpha) &:= (a + c) + (b + d)\alpha, \\ (a + b\alpha)(c + d\alpha) &:= (ac + bd) + (ad + bc + bd)\alpha,\end{aligned}$$

with all arithmetic of coefficients in $\mathbb{F}_2$. (The product is what multiplying out gives if α^2 is replaced by $1 + \alpha$.)

- Write out the addition and multiplication tables of F .
- Prove that F is a field.
- Show that there is no bijection $\varphi: F \rightarrow \mathbb{Z}/4\mathbb{Z}$ with $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in F$. So this four-element field is not $\mathbb{Z}/4\mathbb{Z}$ in disguise.

Solution (Hint 1). For (c): where must φ send 0?

Solution (Hint 2). For (c): look for a non-zero element of $\mathbb{Z}/4\mathbb{Z}$ whose square is zero, and ask which element of F is sent to it.

Solution.

- Using the formulas, with $1 + 1 = 0$ in $\mathbb{F}_2$:

+	0	1	α	β	·	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

For instance, $\alpha\alpha = (0 + 1\alpha)(0 + 1\alpha) = (0 + 1) + (0 + 0 + 1)\alpha = 1 + \alpha = \beta$, and $\alpha\beta = (0 + 1\alpha)(1 + 1\alpha) = (0 + 1) + (0 + 1 + 1)\alpha = 1$.

- Let $x = a + b\alpha$, $y = c + d\alpha$, $z = e + g\alpha$ with $a, b, c, d, e, g \in \mathbb{F}_2$. Since $\mathbb{F}_2$ is a field (Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$)), the coefficients obey every rule of Section 2.1, and in addition $u + u = (1 + 1)u = 0$ for every $u \in \mathbb{F}_2$.

Addition works on each coefficient separately, so (F1) and (F2) for F are (F1) and (F2) for $\mathbb{F}_2$, applied twice; the element $0 = 0 + 0\alpha$ satisfies (F3); and $-x = x$ satisfies (F4), since $a + a = 0$ and $b + b = 0$.

(F6). Exchanging (a, b) with (c, d) leaves the product formula as it was: $ac + bd = ca + db$ and $ad + bc + bd = cb + da + db$, by (F1) and (F6) in $\mathbb{F}_2$.

(F7). With $1 = 1 + 0\alpha$, $x \cdot 1 = (a \cdot 1 + b \cdot 0) + (a \cdot 0 + b \cdot 1 + b \cdot 0)\alpha = a + b\alpha = x$. And $1 \neq 0$, because the first coefficients 1 and 0 of $\mathbb{F}_2$ differ.

(F9). Since $y + z = (c + e) + (d + g)\alpha$,

$$\begin{aligned} x(y + z) &= (a(c + e) + b(d + g)) \\ &\quad + (a(d + g) + b(c + e) + b(d + g))\alpha, \end{aligned}$$

and multiplying out the coefficients regroups this as $((ac + bd) + (ae + bg)) + ((ad + bc + bd) + (ag + be + bg))\alpha = xy + xz$.

(F5). Write $xy = h + k\alpha$ with $h = ac + bd$ and $k = ad + bc + bd$. Then $(xy)z = (he + kg) + (hg + ke + kg)\alpha$, and multiplying out,

$$\begin{aligned} he + kg &= ace + adg + bce + bde + bdg, \\ hg + ke + kg &= acg + ade + adg + bce + bce + bde, \end{aligned}$$

where the second line uses $bdg + bdg = 0$. On the other side, $yz = l + m\alpha$ with $l = ce + dg$ and $m = cg + de + dg$, and $x(yz) = (al + bm) + (am + bl + bm)\alpha$. Multiplying out gives $al + bm = ace + adg + bce + bde + bdg$ and $am + bl + bm = acg + ade + adg + bce + bce + bde$, again using $bdg + bdg = 0$. The coefficients agree, so $(xy)z = x(yz)$.

(F8). From the table, $1 \cdot 1 = 1$ and $\alpha\beta = \beta\alpha = 1$. So every non-zero element has an inverse: $1^{-1} = 1$, $\alpha^{-1} = \beta$, $\beta^{-1} = \alpha$.

This proves that F is a field.

- (c) Assume, for a contradiction, that φ is such a bijection. To begin, $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$ in $\mathbb{Z}/4\mathbb{Z}$. Adding $-\varphi(0)$ to both sides gives $\varphi(0) = [0]$; this is additive cancellation, whose proof (Theorem 2.1.1 (b), first half) uses only (F1)–(F4), which hold in the commutative ring $\mathbb{Z}/4\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 3.4.3 (a)). Surjectivity provides $x \in F$ with $\varphi(x) = [2]$; this x is not 0, because $\varphi(0) = [0] \neq [2]$. But

$$\varphi(xx) = \varphi(x)\varphi(x) = [2][2] = [4] = [0] = \varphi(0),$$

and injectivity turns this into $xx = 0$. By (b), F is a field, so Theorem 2.1.1 (f) gives $x = 0$, a contradiction. Hence no such φ exists.

Marking scheme. (10 points)

- 2: (a) both tables correct, with at least one product computed from the formula.
- 1: (b) addition clauses (F1)–(F4), coefficientwise, with $-x = x$.
- 1: (b) (F6) and (F7), including $1 \neq 0$.
- 2: (b) (F5) and (F9) by expanding coefficients, with $u + u = 0$ in $\mathbb{F}_2$ used and named.
- 1: (b) (F8) from the table.
- 1: (c) $\varphi(0) = [0]$, with the cancellation justified in $\mathbb{Z}/4\mathbb{Z}$.
- 2: (c) an $x \neq 0$ with $\varphi(x) = [2]$ by surjectivity, then $xx = 0$ by injectivity, contradicting the absence of zero divisors in F . A solution that instead takes x with $\varphi(x) = [1]$ by surjectivity and uses $x + x = 0$ in F (from the addition table) to get $[0] = \varphi(0) = \varphi(x + x) = [1] + [1] = [2]$ earns these 2 points; $\varphi(0) = [0]$ still earns the line above.

Fatal errors (0 for the step): “ F is $\mathbb{Z}/4\mathbb{Z}$ because both have four elements”; using in (c) that $\mathbb{Z}/4\mathbb{Z}$ is a field. A solution of (b) that checks (F5) and (F9) by listing all 64 triples from the tables earns the same points.

By Theorem 2.2.2, $\mathbb{Z}/4\mathbb{Z}$ is not a field, so a field with four elements cannot be found among the

rings $\mathbb{Z}/n\mathbb{Z}$; part (c) shows that F is not even a disguised copy of $\mathbb{Z}/4\mathbb{Z}$. Chapter 5 builds this field again, from polynomials over $\mathbb{F}_2$, and explains where the rule $\alpha^2 = 1 + \alpha$ comes from.

Exercise. C2: Find the error

Here is a claim with a proof.

Claim. Let p be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof. (1) By [Example \(Arithmetic on \$\mathbb{Z}/n\mathbb{Z}\$ and the Field \$\mathbb{F}_2\$ \)](#), only (F8) needs checking. (2) Let $[a] \neq [0]$; then $a \neq 0$. (3) Put $[a]^{-1} := [1/a]$. (4) Then $[a][1/a] = [a \cdot (1/a)] = [1]$. (5) So every non-zero class has an inverse, and $\mathbb{Z}/p\mathbb{Z}$ is a field.

Is the claim true? Does the proof prove it? If not, name the line that fails, the error, and give a counterexample to the step.

Solution. The **claim is true**: it is [Theorem 2.2.2](#), direction $(\Leftarrow)$.

The **proof is wrong**, at line (3), and line (4) inherits the fault. The classes of $\mathbb{Z}/p\mathbb{Z}$ are classes of **integers**, and “[1/a]” names a class only when $1/a$ is an integer, that is, when $a = 1$ or $a = -1$. The rule $[x][y] = [xy]$ of Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Definition 3.4.2 is stated for integers x, y only; line (4) applies it to the non-integer $1/a$, a general “fact” that no result supplies. This is entry (N9) of Logic and Proof, Example (What is not allowed): citing a line that is not available. The proof also never uses that p is prime, a sign that something is wrong: the same lines would “prove” that $\mathbb{Z}/6\mathbb{Z}$ is a field.

A counterexample to the step: $p = 5$, $a = 2$. Then $1/2 \notin \mathbb{Z}$, so $[1/2]$ is not an element of $\mathbb{Z}/5\mathbb{Z}$. (The inverse of $[2]$ exists, but it is $[3]$, which line (3) does not produce.)

A repair: since p is prime and $p \nmid a$, the only positive common divisor of a and p is 1; [Lemma 2.2.1](#) gives $ax + py = 1$, and then $[a][x] = [ax] = [1]$, because $p \mid ax - 1$.

Exercise. C3

Find all solutions of $x^2 + x + 1 = 0$ in $\mathbb{F}_2$, in $\mathbb{F}_3$ and in $\mathbb{F}_7$.

Solution. Each field is finite, so we can test every element; this finds all solutions.

In $\mathbb{F}_2$: the values at $x = 0, 1$ are 1 and $3 = 1$. **No solution.**

In $\mathbb{F}_3$: the values at $x = 0, 1, 2$ are 1, 3 = 0 and 7 = 1. The **only solution is** $x = 1$.

In $\mathbb{F}_7$: the values at $x = 0, 1, \dots, 6$ are the remainders of 1, 3, 7, 13, 21, 31, 43 on division by 7, namely 1, 3, 0, 6, 0, 3, 1. The **solutions are** $x = 2$ **and** $x = 4$, since $7 = 1 \cdot 7$ and $21 = 3 \cdot 7$.

The three answers differ in number (none, one, two), although the equation looks the same. Section 2.5 returns to this equation with completing the square, which needs $1 + 1$ to be invertible: it is in $\mathbb{F}_3$ and $\mathbb{F}_7$, and it is not in $\mathbb{F}_2$.