10.1 Fields

a) The neutral element of the operation $\oplus$ is $(0, 0)$. We further have $(1, 0) \otimes (0, 1) = (0, 0)$. Hence, $F \times F$ has zero divisors. Since no field can have zero divisors, $F \times F$ is not a field.

b) Since $F$ is a field, $F^* = F \setminus \{0\}$ is a group. Therefore, by Corollary 5.10, for any $a \in F^*$, we have $1 = a|F^*| = a^{q-1}$. Hence, all $q - 1$ elements of $F^*$ are roots of the polynomial $x^{q-1} - 1$. The claim follows by Lemma 5.29 and Theorem 5.31.

c) Since $F$ has at least three elements, there exists an $a \in F \setminus \{0, 1\}$. Let $f : F \rightarrow F$ be the function defined by $f : x \mapsto a \cdot x$. We argue that $f$ is a bijection. Since $F^* = F \setminus \{0\}$ is a group and $a \in F^*$, it follows by Lemma 5.3. that for all $x_1, x_2 \in F^*$ such that $f(x_1) = f(x_2)$, we have $x_1 = x_2$. Also, $f(0) = 0$. Hence, $f$ is injective. Since $F$ is finite, this means that $f$ is also surjective.

It follows that
$$\sum_{x \in F} x = \sum_{x \in F} f(x) = a \cdot \sum_{x \in F} x.$$

Thus, $(1 - a) \cdot \sum_{x \in F} x = 0$. Since $F$ has no zero divisors and $a \neq 1$, we have $\sum_{x \in F} x = 0$.

10.2 Computing on polynomials

a) In $\mathbb{Z}_7$, the multiplicative inverse of 5 is 3, because $3 \cdot 5 \equiv 1 \pmod{7}$. Therefore, the first coefficient of the result is 3. The rest of the computation proceeds analogously:

$$\begin{align*}
(x^5 + 6x^2 + 5) : (5x^2 + 2x + 1) &= 3x^3 + 3x^2 + x + 3 \\
-\left(\frac{x^5 + 6x^4 + 3x^3}{x^4 + 4x^3 + 6x^2 + 5}ight) &= (x^4 + 6x^3 + 3x^2 + 5) \\
&\quad - (5x^3 + 2x^2 + x) \\
&\quad + x^2 + 6x + 5 \\
&\quad \text{Rest: } 2
\end{align*}$$

b) The irreducible polynomials of degree 4 over $GF(2)$ are $x^4 + x^3 + 1$, $x^4 + x + 1$ and $x^4 + x^3 + x^2 + x + 1$. 
We show this by eliminating all reducible polynomials of degree four. A polynomial \( p(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \) is reducible if it is divisible by a polynomial of degree one or two (if it is divisible by a polynomial of degree three, then it must also be divisible by one of degree one).

By Lemma 5.29, the polynomials \( p(x) \) divisible by a polynomial of degree one are exactly those for which \( p(0) = 0 \) or \( p(1) = 0 \). Hence, we have to eliminate the polynomials for which \( a_0 = 0 \) or \( a_3 + a_2 + a_1 + a_0 = 0 \). Remaining are the polynomials: \( x^4 + x^3 + 1, x^4 + x + 1, x^4 + x^2 + 1 \) and \( x^4 + x^3 + x^2 + x + 1 \).

Furthermore, over \( \text{GF}(2) \) there is only one irreducible polynomial of degree two, namely \( x^2 + x + 1 \) (the other polynomials: \( x^2, x^2 + 1 \) and \( x^2 + x \) can be eliminated in the same way we did above). Hence, we have to also eliminate \( (x^2 + x + 1)^2 = x^4 + x^2 + 1 \).

c) Since 2 is a double root, it follows that \( a(x) = (x - 2)^2b(x) \), where \( b(x) \) is a polynomial of degree 2.

We know that \( 2 = a(3) = (3 - 2)^2 b(3), 3 = a(4) = (4 - 2)^2 b(4) \) and \( 5 = a(6) = (6 - 2)^2 b(6) \). Hence, we have \( b(3) = 2, b(4) = 3 \cdot 4^{-1} = 6 \) and \( b(6) = 5 \cdot 2^{-1} = 6 \). In order to determine \( b(x) \), we apply Lagrange’s interpolation:

\[
b(x) = 2\frac{(x - 4)(x - 6)}{(3 - 4)(3 - 6)} + 6\frac{(x - 3)(x - 6)}{(4 - 3)(4 - 6)} + 6\frac{(x - 3)(x - 4)}{(6 - 3)(6 - 4)}
\]

\[
= 3(x + 3)(x + 1) + 4(x + 4)(x + 1) + (x + 4)(x + 3)
\]

\[
= x^2 + 4x + 2
\]

Therefore, \( a(x) = (x - 2)^2(x^2 + 4x + 2) = x^4 + 4x^2 + x + 1 \) and \( a(0) = 1 \).

10.3 The ring \( F[x]_{m(x)} \)

a) We have

\[
\text{GF}(3)[x]_{x^2+2} = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}.
\]

By Lemma 5.36,

\[
\text{GF}(3)[x]_{x^2+2}^* = \{a(x) \in \text{GF}(3)[x]_{x^2+2} \mid \gcd(a(x), x^2 + 2) = 1\}.
\]

The task is to find all polynomials \( a(x) \in \text{GF}(3)[x] \) of degree at most one, such that \( \gcd(a(x), x^2 + 2) = 1 \). Note first that over \( \text{GF}(3) \), we have \( x^2 + 2 = x^2 - 1 = (x + 1)(x - 1) = (x + 1)(x + 2) \). Hence, all polynomials \( b(x) \) of degree at most one, for which \( \gcd(b(x), (x + 1)(x + 2)) \neq 1 \) are \( p(x + 1) \) and \( q(x + 2) \) for some \( p, q \in \text{GF}(3) \). These polynomials are: \( x + 1, x + 2, 2x + 2 \) and \( 2x + 1 \).

The polynomials of degree at most one that are left are in \( \text{GF}(3)[x]_{x^2+2}^* \). Therefore, \( \text{GF}(3)[x]_{x^2+2}^* = \{1, 2, x, 2x\} \).

b) The inverse of \( x \in \text{GF}(3)[x]_{x^2+2}^* \) is a polynomial \( p(x) \in \text{GF}(3)[x]_{x^2+2}^* \), such that \( x \cdot p(x) \equiv 1_{x^2+2} \) (where 1 is the constant polynomial). Since all the polynomials in \( \text{GF}(3)[x]_{x^2+2}^* \) have degree at most 1 (Definition 5.34), we have \( p(x) = ax + b \) for some
10.4 Finite fields

(a) We can construct the field \( F = \text{GF}(9) = \text{GF}(3^2) \) as the extension field of \( \text{GF}(3) \) (cf. Example 5.64).

\( \text{GF}(9) \) consists of the 9 polynomials of degree at most 2 over \( \text{GF}(3) \). Hence, the elements of \( \text{GF}(9) \) are \( \{0, 1, 2, x, 2x, x + 1, x + 2, 2x + 1, 2x + 2\} \).

In order to fully specify \( \text{GF}(9) \), we also need to determine the operations: addition and multiplication. To this end, note that \( \text{GF}(9) = \text{GF}(3)[x]_{m(x)} \) for some irreducible polynomial \( m(x) \) of degree 2.

(2 Points)

Since the operations in \( \text{GF}(3)[x]_{m(x)} \) are already defined, the task is simply to find such polynomial. For example, \( m(x) = x^2 + 1 \) is irreducible, because \( m(x) \) has no roots in \( \text{GF}(3) \): \( m(0) = 1, m(1) = 2 \) and \( m(2) = 2 \). Irreducibility follows by Corollary 5.30.

(2 Points)

(b) We have \( F^* = \text{GF}(3)[x]_{x^2 + 1}^{*} = \text{GF}(3)[x]_{x^2 + 1} \setminus \{0\} \). The order of \( F^* \) is \(|F| - 1 = 8 \). Let \( a \) (a candidate for a generator) be any element in \( F^* \). By the Lagrange’s theorem, it follows that \( \text{ord}(a) \mid 8 \). Hence, \( \text{ord}(a) \) can only be equal to 1, 2, 4 or 8.

(2 Points)

Further, \( a \) is a generator if and only if \( \text{ord}(a) = 8 \). Therefore, to prove that \( a \) is a generator it is enough to show that \( a^4 \neq 1 \) (this is because if the order of \( a \) is 1, 2 or 4, we have \( a^4 = 1 \)).

(2 Points)

For example, for \( (x + 1) \in F^* \), we have \( (x + 1)^4 = 2 \). Hence, \( x + 1 \) is a generator.

(1 Point)

10.5 A safe in a monkey house

(a) The polynomial \( a(x) \) is uniquely determined by the \( t \) values \( s_i = a(\alpha_i) \), known to the remaining monkeys. Hence, the monkeys can use the Lagrange’s interpolation formula to reconstruct \( a(x) \) and compute the secret code \( s = a(0) \).

(b) Without loss of generality, assume that the clan consists of the monkeys \( M_1, \ldots, M_t \). We show that, given their shares \( s_1, \ldots, s_{t-1} \), any \( s' \in \text{GF}(q) \) could be the secret code (and, hence, there are \( q \) possibilities for the secret code \( s \)). That is, we argue that for each \( s' \), there exists a polynomial \( a'(x) \) of degree at most \( t - 1 \) such that \( a'(\alpha_1) = s_1, \ldots, a'(\alpha_{t-1}) = s_{t-1} \) and \( a'(0) = s' \). Indeed, the \( t - 1 \) values \( a'(\alpha_1), \ldots, a'(\alpha_{t-1}) \), together with \( a'(0) \), give \( t \) values that uniquely determine \( a'(x) \).

For the clan of greedy monkeys this means that their shares on their own are practically worthless. They give no information about \( s \). The monkeys could simply try all possibilities for \( s \) without knowing any shares at all.