Exercise 8.1. [6pts]

(a) Find $\langle(3,2)\rangle \in \mathbb{Z}_4 \times \mathbb{Z}_3$. Write multiples of $(3,2)$ one by one until all elements of $\langle(3,2)\rangle$ are exhausted.
(b) Find $\langle(3,2)\rangle \in U_5 \times \mathbb{Z}_3$. Write multiples of $(3,2)$ one by one until all elements of $\langle(3,2)\rangle$ are exhausted. I'd like to emphasize that the first group in the product is multiplicative.

Solution: (a)

$$\begin{array}{lllll} 0(3,2)=(0,0) & 1(3,2)=(3,2) & 2(3,2)=(2,1) & 3(3,2)=(1,0) & 4(3,2)=(0,2) \\ 5(3,2)=(3,1) & 6(3,2)=(2,0) & 7(3,2)=(1,2) & 8(3,2)=(0,1) & 9(3,2)=(3,0) \\ 10(3,2)=(2,2) & 11(3,2)=(1,1) & 12(3,2)=(0,0). & & \end{array}$$

(b)

$$\begin{array}{lllll} 0(3,2)=(1,0) & 1(3,2)=(3,2) & 2(3,2)=(4,1) & 3(3,2)=(2,0) & 4(3,2)=(1,2) \\ 5(3,2)=(3,1) & 6(3,2)=(4,0) & 7(3,2)=(2,2) & 8(3,2)=(1,1) & 9(3,2)=(3,0) \\ 10(3,2)=(4,2) & 11(3,2)=(2,1) & 12(3,2)=(1,0). & & \end{array}$$

□

Exercise 8.2. [2pts] Consider any ring R. Show that if its characteristic $\chi(R) \neq 0$, then for any $a \in R$ we have $n \cdot a = 0$.

Solution:

$$\begin{aligned} n \cdot a &= \underbrace{a + \ldots + a}_{n} \\ &= a(\underbrace{1 + \ldots + 1}_{n}) \\ &= a \cdot 0 = 0. \end{aligned}$$

□

Exercise 8.3. [2pts] Let F be a field and $f(x) \in F[x]$. Show that if $f(x)$ is divisible by a polynomial $g(x) = a_n x^n + \ldots$ of degree n, then it is divisible by some monic polynomial of degree n.

Solution: If $g(x) \mid f(x)$, then

$$\begin{aligned} f(x) &= q(x)g(x) \quad \text{for some } q(x) \in F[x] \\ &= q(x)(a_n x^n + \ldots) \\ &= [a_n q(x)] \cdot \frac{a_n x^n + \ldots}{a_n}, \end{aligned}$$

where $\frac{a_n x^n + \ldots}{a_n}$ is monic.

□

Exercise 8.3 is very useful when we want to show that $f(x)$ does not have divisors of degree n, it eliminates non-monic divisors from consideration. For instance, there are 20 linear polynomials in $\mathbb{Z}_5[x]$

$$x, x+1, x+2, x+3, x+4, 2x, 2x+1, \ldots, 4x+4,$$

and only 5 of them are monic. Now, say we need to check that a cubic $f(x) = 2x^3 + x + 2$ is irreducible.

$$\begin{aligned} f(x) \text{ is NOT irreducible} \quad &\Leftrightarrow \quad f(x) = g(x)h(x), \quad \text{where } g(x), h(x) \text{ are non-constant} \\ &\Leftrightarrow \quad f(x) = g(x)h(x), \quad \text{where } g(x) \text{ or } h(x) \text{ is linear (because } \deg(f) = 3) \\ &\Leftrightarrow \quad f(x) \quad \text{has a linear factor} \\ &\Leftrightarrow \quad f(x) \quad \text{has a linear monic factor } x - \alpha \\ &\Leftrightarrow \quad f(\alpha) = 0 \quad \text{for some } \alpha \in \mathbb{Z}_5. \end{aligned}$$

Now, $f(x) = 2x^3 + x + 2$ is not irreducible because $f(1) = 0$ and, hence, has a factor $x - 1$. This works for quadratic or linear f, because a quartic f can be a product of two quadratic polynomials.

Exercise 8.4. [5pts] Check if the following polynomials are irreducible or not.

(a) $f(x) = x^3 + 2x - 1 \in \mathbb{Z}_3[x]$
(b) $f(x) = x^3 + 2x^2 + 2x + 1 \in \mathbb{Z}_5[x]$
(c) To check if $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible you will need to consider linear factors and (irreducible) quadratic factors (which easy because $\mathbb{Z}_2[x]$ has a unique irreducible quadratic polynomial mentioned in class).

Solution:

(a) $f(x) = x^3 + 2x - 1 \in \mathbb{Z}_3[x]$ is cubic. It is irreducible because it has no zeros in $\mathbb{Z}_3$:

$$f(0) = 2 \qquad\qquad f(1) = 2 \qquad\qquad f(2) = 2.$$

(b) $f(x) = x^3 + 2x^2 + 2x + 1 \in \mathbb{Z}_5[x]$ is cubic. It is not irreducible because it has zeros in $\mathbb{Z}_5$:

$$f(0) = 1 \qquad f(1) = 1 \qquad f(2) = 1 \qquad f(3) = 2 \qquad f(4) = 0.$$

(c) $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ has no zeros in $\mathbb{Z}_2$ and, hence, has no linear factors. To check if it has a quadratic irreducible factor, divide by $x^2 + x + 1$ to get

$$f(x) = x^2(x^2 + x + 1) + (x + 1),$$

where $x + 1$ is a non-trivial remainder of division. Therefore, $f(x)$ is irreducible.

□

Exercise 8.5. [5pts] Find the remainder of division of $2x^6 + x^2 - 1$ by $x^2 + 3x + 2$ in $\mathbb{Z}_5[x]$.

Solution: $2x^6 + x^2 - 1 = (2x^4 + 4x^3 + 4x^2 + 3) \cdot (x^2 + 3x + 2) + (x + 3)$. □

Exercise 8.6. [10pts] For $f(x) = 4x^4 - x^3 + 3x^2 + x - 2$ and $g(x) = 4x^5 + x^3$ in $\mathbb{Z}_5[x]$ use the Euclidean algorithm to find

(a) $\gcd(f(x), g(x))$. [Hint. Do not forget that gcd must be monic].
(b) Polynomials $\alpha(x), \beta(x) \in \mathbb{Z}_5[x]$ satisfying $\gcd(f(x), g(x)) = \alpha(x)f(x) + \beta(x)g(x)$.

Solution: Running the Euclidean algorithm we obtain the following:

$$\begin{aligned} g(x) &= (x-1)f(x) + \mathbf{2x^3 + 2x^2 + 3x + 3} \quad \Rightarrow \quad \gcd(f,g) &&= \gcd(f(x), 2x^3 + 2x^2 + 3x + 3) \\ f(x) &= 2x(2x^3 + 2x^2 + 3x + 3) + (\mathbf{2x^2 + 3}) &&= \gcd(2x^2 + 3, 2x^3 + 2x^2 + 3x + 3) = 1 \\ 2x^3 + 2x^2 + 3x + 3 &= (x+1)(2x^2 + 3) + \mathbf{0} &&= \gcd(2x^2 + 3, 0) = 2x^2 + 3. \end{aligned}$$

Multiplying by 3 we get $\gcd(2x^2 + 3, 0) = x^2 + 4$. Next, we express $2x^2 + 3$ as a linear combination of $f(x)$ and $g(x)$:

$$\begin{aligned} 2x^2 + 3 &= f(x) - 2x(2x^3 + 2x^2 + 3x + 3) \\ &= f(x) - 2x(g(x) - (x-1)f(x)) \\ &= (2x^2 - 2x + 1)f(x) - 2xg(x). \end{aligned}$$

To get a linear combination for $x^2 + 4$ multiply by 3:

$$\begin{aligned} x^2 + 4 = 3(2x^2 + 3) &= (6x^2 - 6x + 3)f(x) - 6xg(x) \\ &= (x^2 - x + 3)f(x) - xg(x). \end{aligned}$$

Hence, $\alpha(x) = x^2 - x + 3$ and $\beta(x) = -x$. $\square$

Definition 8.1. A **vector space** over a field F is a set V equipped with two operations:

- **(addition)** $+ : V \times V \to V$;
- **(scalar multiplication)** $\cdot : F \times V \to V$.

satisfying the following conditions for $a, b, c \in V$ and $\alpha, \beta \in F$:

- $a + b = b + a$ and $(a + b) + c = a + (b + c)$.
- $a + 0 = 0 + a$ and $a + (-a) = 0$.
- $\alpha(\beta a) = (\alpha\beta)a$ and $1a = a$.
- $(\alpha + \beta)a = \alpha a + \beta a$ and $\alpha(a + b) = \alpha a + \alpha b$.

Elements of V are called **vectors** and elements of F are called **scalars**.

Exercise 8.7. [+5pts] Show that the set of complex numbers $\mathbb{C}$ with standard complex addition and multiplication is a vector space over a field $\mathbb{R}$.

Solution:

- Addition is associative and commutative on $\mathbb{C}$.
- $0 \in \mathbb{C}$. If $a \in \mathbb{C}$, then $-a \in \mathbb{C}$.
- $1 \in \mathbb{C}$. Multiplication on $\mathbb{C}$ is associative. Hence, for any $\alpha, \beta \in \mathbb{R}$ and $a \in \mathbb{C}$ we have $\alpha(\beta a) = (\alpha\beta)a$.
- Multiplication is distributive in $\mathbb{C}$. Hence, for any $\alpha, \beta \in \mathbb{R}$ and $a \in \mathbb{C}$ we have $\alpha(a+b) = \alpha a+\alpha b$.

$\square$

Exercise 8.8. [+5pts] Let F be a vector space. Show that $F^n = \{\, (\alpha_1, \dots, \alpha_n) \mid \alpha_1, \dots, \alpha_n \in F \,\}$ with $+$ and $\cdot$ defined by

$$(\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n),$$
$$c(\alpha_1, \dots, \alpha_n) = (c\alpha_1, \dots, c\alpha_n)$$

is a vector space over F.

Solution:

- Addition is commutative because

$$(\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n),$$
$$(\beta_1, \dots, \beta_n) + (\alpha_1, \dots, \alpha_n) = (\beta_1 + \alpha_1, \dots, \beta_n + \alpha_n).$$

  Addition is associative because

$$((\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n)) + (\gamma_1, \dots, \gamma_n) = ((\alpha_1 + \beta_1) + \gamma_1, \dots, (\alpha_n + \beta_n) + \gamma_n),$$
$$(\alpha_1, \dots, \alpha_n) + ((\beta_1, \dots, \beta_n)) + (\gamma_1, \dots, \gamma_n) = (\alpha_1 + (\beta_1 + \gamma_1), \dots, \alpha_n + (\beta_n + \gamma_n)).$$

- $(0 \dots, 0)$ is the trivial element in F^n because

$$(0 \dots, 0) + (\alpha_1, \dots, \alpha_n) = (\alpha_1, \dots, \alpha_n).$$

  If $(\alpha_1, \dots, \alpha_n) \in F^n$, then $(-\alpha_1, \dots, -\alpha_n) \in F^n$.
- For any $\alpha, \beta \in F$ and $(\alpha_1, \dots, \alpha_n) \in F^n$

$$\alpha(\beta a) = (\alpha(\beta\alpha_1), \dots, \alpha(\beta\alpha_n))$$
$$(\alpha\beta)a = ((\alpha\beta)\alpha_1), \dots, (\alpha\beta)\alpha_n).$$

  and

$$1 \cdot (\alpha_1, \dots, \alpha_n) = (\alpha_1, \dots, \alpha_n).$$

- For any $\alpha, \beta \in F$ and $(\alpha_1, \dots, \alpha_n) \in F^n$

$$(\alpha + \beta)a = ((\alpha + \beta)\alpha_1, \dots, (\alpha + \beta)\alpha_n)$$
$$\alpha a + \beta a = (\alpha\alpha_1, \dots, \alpha\alpha_n) + (\beta\alpha_1, \dots, \beta\alpha_n).$$

similarly

$$\alpha((\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n)) = (\alpha(\alpha_1 + \beta_1), \ldots, \alpha(\alpha_n + \beta_n))$$
$$\alpha(\alpha_1, \ldots, \alpha_n) + \alpha(\beta_1, \ldots, \beta_n) = (\alpha\alpha_1 + \alpha\beta_1, \ldots, \alpha\alpha_n + \alpha\beta_n)$$

$\square$