Algebraic structures

Exercises

Application of discrete models

Mathematical questions

1. Which of the following structures are rings, integral domains and/or fields? For those that are not, which property is not satisfied?
a) $\mathbb{N}$, b) $\mathbb{Z}$, c) $\mathbb{Q}$, d) $\mathbb{R}$, e) $\mathbb{C}$,
f) $2\mathbb{Z}$, g) $2\mathbb{Z}+1$, h) $\mathbb{Q}\setminus\mathbb{Z}$,
i) $\mathbb{Z}_2$, j) $\mathbb{Z}_3$, k) $\mathbb{Z}_4$, l) $\mathbb{Z}_5$,
m) $\mathbb{R}[x]$, n) $\mathbb{Z}[x]$, o) $\mathbb{Z}_7[x]$, p) $\mathbb{Z}_8[x]$,
q) $\mathbb{Q}^{5\times5}$, r) $\mathbb{R}^{4\times4}$, s) $\mathbb{Z}^{2\times3}$.

2. What is the zero element and identity element (if any) of the following rings:
a) $\mathbb{Z}$, b) $\mathbb{Z}_3$, c) $2\mathbb{Z}$, d) $\mathbb{Z}^{3\times3}$, e) $\mathbb{Z}[x]$?

3. What is a zero divisor? Give examples in *two* different rings.

4. For which m does $\mathbb{Z}_m$ have zero divisors? For those m, which elements are zero divisors?

5. Find the multiplicative inverses of the following elements, if they exist:
a) $4 \in \mathbb{Q}$, b) $-1 \in \mathbb{Z}$, c) $2 \in \mathbb{Z}$, d) $i \in \mathbb{C}$, e) $\overline{3} \in \mathbb{Z}_5$, f) $\overline{3} \in \mathbb{Z}_6$, g) $\overline{1} \in \mathbb{Z}_7$,
h) $2x^2 \in \mathbb{R}[x]$, i) $2 \in \mathbb{R}[x]$, j) $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \in \mathbb{R}^{2\times2}$, k) $\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right) \in \mathbb{R}^{2\times2}$.

6. a) At most how many roots can a quadratic polynomial in $\mathbb{Z}_5[x]$ have?
b) At most how many roots can a quadratic polynomial in $\mathbb{Z}_6[x]$ have?

7. Calculate the quadratic polynomial $p \in \mathbb{Z}_7[x]$ for which $p(\overline{2}) = \overline{4}$, $p(\overline{3}) = \overline{2}$ and $p(\overline{4}) = \overline{6}$.

Programming exercises

8. Solve each of the following exercises for an arbitrary input ring. Each function receives a list that contains the elements of the ring. (That is, **not** a Sage structure like `Zmod(10)`, but the list of elements, e.g. `list(Zmod(10))`.) Don't use **anything else** about the elements than the two ring operations (`a + b` and `a * b`) and equality comparison (`a == b`, `a != b`), in addition to the abstract fact that they form a ring.

a) Decide whether the ring is commutative.
Try it for $\mathbb{Z}_{10}$ (`list(Zmod(10))`) and $\mathbb{Z}_3^{2\times 2}$ (`list(Mat(Zmod(3), 2))`).

b) Return the zero element of the ring.
Try it for $\mathbb{Z}_{10}$ and $\mathbb{Z}_3^{2\times 2}$.

c) Return the identity element of the ring if it has one, otherwise return `None`.
Try it for $\mathbb{Z}_{10}$, $2\mathbb{Z}_{20}$ and $2\mathbb{Z}_{10}$. (Here $2\mathbb{Z}_m$ means the even elements of $\mathbb{Z}_m$, and can be created e.g. like this: `list(Zmod(10))[::2]`.) Is the result surprising?

d) Return a zero divisor in the ring if it has one, otherwise return `None`.
Try it for $\mathbb{Z}_5$ and $\mathbb{Z}_6$.

e) Decide whether the ring is an integral domain.
Which of $\mathbb{Z}_1, \mathbb{Z}_2, \ldots, \mathbb{Z}_{20}$ are integral domains?

9. Create the polynomial $p \in \mathbb{Z}_{11}[x]$ which has almost all $c \in \mathbb{Z}_{11}$ as roots, except the following two: $\overline{0}, \overline{1} \in \mathbb{Z}_{11}$. All roots are simple, except for $c = \overline{2}$, which is a double root.

10. Find a quadratic polynomial in $\mathbb{Z}_6[x]$ for which all six elements of $\mathbb{Z}_6$ are roots. (Hint: quadratic polynomials have the form ax^2+bx+c, and each coefficient has only finitely many possibilities.)

11. We know that $1/x$ is not a polynomial. There is not even such a polynomial that has the same values as $1/x$ for all $x \neq 0$ – at least not with numbers. But over finite rings, it is possible. Create the polynomial $p \in \mathbb{Z}_{97}[x]$ of degree 95 for which $\forall a \in \mathbb{Z}_{97} \setminus \{\overline{0}\} : p(a) = 1/a = a^{-1}$.

12. a) Rewrite Shamir's secret sharing from the previous exercise list (exercise 13.) for $\mathbb{Z}_p$, where p is a prime number, which is an additional parameter of the function that generates the secret shares. The coefficients are arbitrary random elements of $\mathbb{Z}_p$.

b) Repeat the test of the security flaw of Shamir's secret sharing from the previous exercise list (exercise 14.), now in $\mathbb{Z}_{89}$ (changeing the range of y_5 appropriately). How different it is?