Algebraic structures

Application of discrete models

1 Ring

We have seen different kinds of mathematical objects which have operations like numbers (e.g. addition, subtraction, multiplication): matrices, polynomials, remainders etc. These operations have many similar properties (e.g. it is always true that $a+b=b+a$), but they also have some differences (e.g. for numbers, $a \cdot b = b \cdot a$, but not for matrices). In this document, we will perform *abstraction*: for all these different mathematical objects, we will examine their common properties, and "forget" their individual characteristics. In this way, any conclusion we will have in general will automatically apply to all particular cases.

Definition 1.1 (ring)**.** Let R be a set with two binary operations: "$+$" and "$\cdot$". The tuple $(R, +, \cdot)$ is called a **ring** if the following properties (*ring axioms*) are satisfied:

A. **additive operation** $(+)$:
   1. closed: $\forall a, b \in R : \ a + b \in R$;
   2. associative: $\forall a, b, c \in R : \ (a + b) + c = a + (b + c)$;
   3. commutative: $\forall a, b \in R : \ a + b = b + a$;
   4. **zero element**: $\exists z \in R : \forall a \in R : \ a + z = a$;
   5. **additive inverse**: $\forall a \in R : \exists x \in R : \ a + x = z$ (z is from above) (x is denoted by $-a$);

M. **multiplicative operation** $(\cdot)$:
   1. closed: $\forall a, b \in R : \ a \cdot b \in R$;
   2. associative: $\forall a, b, c \in R : \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

D. "$\cdot$" is distributive over "$+$":
   $\forall a, b, c \in R : \ a \cdot (b + c) = a \cdot b + a \cdot c \ \wedge \ (b + c) \cdot a = b \cdot a + c \cdot a.$

Example. The integers, i.e. $(\mathbb{Z}, +, \cdot)$ is a ring, because it satisfies all properties listed above. The *zero element* from A/4 is the zero number ($z = 0$), because $a + 0 = a$, and the *additive inverse* from A/5 is the negative of the number ($x = -a$), because $a + (-a) = 0$.

The ring axioms were grouped into three categories: the first two (A and M) contain the properties of the two operations separately, and the third one (D = distributivity) connects the two operations (so that they are not just two independent operations). Notice that rings have much fewer requirements on the multiplicative operation than on the additive operation. This allows more kinds of objects to fit into the definition of rings (e.g. matrices, where multiplication is not commutative). Later we will see other algebraic structures with more requirements on the multiplicative operation.

(Note: although the operations were denoted by "$+$" and "$\cdot$", they can really be any operations, not just addition and multiplication, as long as they satisfy all the requirements above. But since we mostly deal with these two operations anyway, we will often – slightly inaccurately – omit them from the notation, e.g. instead of $(\mathbb{Z}, +, \cdot)$, we will write that "$\mathbb{Z}$ is a ring". Furthermore, we often omit the sign of multiplication, e.g. we write ab instead of $a \cdot b$.)

More examples of rings:

1. Most of the basic number sets are rings:

$$\begin{aligned}
&\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} && \text{(the set of integers)},\\
&\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z} \wedge b \neq 0\} && \text{(the set of rational numbers)},\\
&\mathbb{R} && \text{(the set of real numbers)},\\
&\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\} && \text{(the set of complex numbers)}
\end{aligned}$$

   with the usual addition and multiplication. The zero element is the number 0, and the additive inverse of any number is its negative ($-a$). On the other hand, the set of natural numbers ($\mathbb{N}$) is *not* a ring, as it has no additive inverse: e.g. there is no natural number x such that $2+x=0$.
2. The set of $n \times n$ matrices, e.g. $\mathbb{R}^{n\times n}$ (for a fixed n) is a ring, with matrix addition and matrix multiplication. The zero element is the zero matrix, i.e. the matrix with all zeros, e.g. $\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$. The additive inverse of an $A \in \mathbb{R}^{n\times n}$ is the matrix $-A \in \mathbb{R}^{n\times n}$ where all the elements are negated (e.g. if $A = \left(\begin{smallmatrix}2&1\\0&-3\end{smallmatrix}\right)$, then $-A = \left(\begin{smallmatrix}-2&-1\\0&3\end{smallmatrix}\right)$), because then $A + (-A) = \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$.
3. The set of polynomials, e.g. $\mathbb{R}[x]$ is also a ring. The zero element is the zero polynomial ($0 \in \mathbb{R}[x]$), and the additive inverse of p is $-p = -1 \cdot p$ (e.g. if $p = 2x^2 - 3$, then $-p = -2x^2 + 3$).
4. The residue classes for a given $m \in \mathbb{N}^+$ also form a ring: $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ (see the document called Congruences). Reminder: the operations are performed modularly, i.e. the result of each operation is the remainder of the integer result when divided by m, e.g. in $\mathbb{Z}_5$, $\overline{3} + \overline{4} = \overline{2}$ and $\overline{3} \cdot \overline{3} = \overline{4}$. The zero element is the residue class $\overline{0}$. The additive inverse of an $\overline{a} \in \mathbb{Z}_m$ is $-\overline{a} = \overline{m - a}$, e.g. in $\mathbb{Z}_5$, the additive inverses of $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$ are $\overline{0}, \overline{4}, \overline{3}, \overline{2}, \overline{1}$ respectively (since $\overline{0} + \overline{0} = \overline{0}$, $\overline{1} + \overline{4} = \overline{0}$ etc.).
5. The even numbers, $2\mathbb{Z} := \{2k \mid k \in \mathbb{Z}\}$ also form a ring. Since $2\mathbb{Z} \subseteq \mathbb{Z}$, and we already know that $\mathbb{Z}$ is a ring, many ring axioms are inherited automatically (associativity, commutativity and distributivity). The others must be checked: $2\mathbb{Z}$ is closed under the operations (A/1, M/1), because the sum and product of even numbers are even; the zero element is inherited, because 0 is even; and so is the additive inverse, because the negative of even numbers are also even.
   On the other hand, the odd numbers ($2\mathbb{Z} + 1$) do *not* form a ring, because they are not closed under addition (A/1): e.g. $1 + 3 = 4$, i.e. the sum of two odd numbers are not odd.
6. The following example demonstrates that the two ring operations need not necessarily be addition and multiplication, they can be any operations. Let H be an arbitrary set, and consider all possible subsets of H – in other words, take the power set of H, i.e. 2^H (e.g. if $H = \{a, b\}$, then $2^H = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$). Then $(2^H, \triangle, \cap)$ is a ring, i.e. the subsets of H with the symmetric difference ($\triangle$) and set intersection ($\cap$) operations (see: Discrete mathematics I) form a ring. All ring axioms are satisfied, but here the additive operation is $\triangle$, and the multiplicative operation is $\cap$. For example, the (first half of the) distributivity is: $\forall A, B, C \in 2^H : A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$. The zero element of the ring is the empty set, $\emptyset$ (since $A \triangle \emptyset = A$), and the additive inverse of each set is itself (since $A \triangle A = \emptyset$).
7. The simplest possible ring is a set with a single element: $\{a\}$, where the operations are defined in the only possible way: $a + a = a$ and $a \cdot a = a$. Then $(\{a\}, +, \cdot)$ is a ring, because all ring axioms are trivially satisfied (e.g. commutativity is $a + a = a + a$ etc.). The zero element of the ring is its only element (a), and the additive inverse of a is a itself. This ring is called the **zero ring** (because its only element is the zero element).

Theorem 1.2 (properties of rings)**.**

1. *The zero element is unique (i.e. if z_1 and z_2 are both zero elements, then $z_1 = z_2$).*
2. *The additive inverse is unique (i.e. if x_1 and x_2 are both additive inverses of a, then $x_1 = x_2$).*
3. *The additive inverse of the zero element is itself: $-z = z$.*
4. *The additive inverse of the additive inverse is the original element: $-(-a) = a$.*
5. *The zero element absorbs any element by multiplication: $\forall a \in R : za = z \ \wedge \ az = z$.*

(These are simple consequences of the ring axioms. For example, for the first one, since z_1 is a zero element, $z_1 + z_2 = z_2$, but since z_2 is also a zero element, $z_1 + z_2 = z_1$, so $z_1 = z_2$.)

The ring's definition mentions only two operations ($+$ and $\cdot$), but what about the other two fundamental operations? For example, subtraction can be defined using addition and additive inverse:

Definition 1.3 (subtraction)**.** For a ring R and $a, b \in R$: $\boldsymbol{a - b} := a + (-b)$.

It follows from the definition that $(a - b) + b = a$ and $(a + b) - b = a$, as expected.

(Note: if the additive operation of the ring is not addition, then this operation is also not called subtraction, but the **inverse** of that operation. E.g. for $(2^H, \triangle, \cap)$ above, the inverse of $\triangle$ is itself, because the additive inverse of each element is itself. Similarly, division will be the inverse of the multiplication, but that needs some preparations first.)

2 Integral domain

The definition of the ring is general enough, but sometimes we need more requirements, especially on the multiplicative operation. So let's introduce some further notions.

The additive operation is always commutative, but the multiplicative operation is not necessarily:

Definition 2.1. A ring R is **commutative** if the multiplicative operation ($\cdot$) is commutative, i.e.

$$\forall a, b \in R : \ a \cdot b = b \cdot a.$$

Example. Almost all of the above examples are commutative rings. The exception is the matrices, e.g. if $A = \left(\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 2 & 2 \\ 2 & 2 \end{smallmatrix}\right)$, then $AB = \left(\begin{smallmatrix} 4 & 4 \\ -4 & -4 \end{smallmatrix}\right)$, but $BA = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

We can create the analogue of the zero element for the multiplicative operation:

Definition 2.2. $e \in R$ is the **identity element** of the ring R if

$$\forall a \in R : \ ae = a \ \wedge \ ea = a.$$

A ring that contains an identity element is called a **ring with identity**.

Example. Most of the example rings listed above have an identity element:

1. The identity of the number rings ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) is 1.
2. The identity of a matrix ring is the *identity matrix*, e.g. $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathbb{R}^{2\times 2}$.
3. The identity of a polynomial ring is the constant polynomial 1.
4. The identity of $\mathbb{Z}_m$ is the residue class $\overline{1}$.
5. The ring of even numbers ($2\mathbb{Z}$) has no identity element.
6. The identity element of the ring $(2^H, \triangle, \cap)$ is H itself, since for all $A \in 2^H$ (i.e. $A \subseteq H$) sets, $A \cap H = A$ and $H \cap A = A$. (So here the zero and identity elements are the two "extremes".)
7. The identity element of the zero ring is its only element. (Note: this is the only ring where the identity and zero elements coincide, because in larger rings, the absorption property of the zero element ($za = z$) prevents it from being also the identity element.)

Theorem 2.3. *The identity element is unique, i.e. if e_1 and e_2 are both identities, then $e_1 = e_2$.*

The following notion is unheard of in number rings, and it can be very annoying, so we try to avoid it as much as possible:

Definition 2.4. $a \in R \setminus \{z\}$ is a **zero divisor** in the ring R if

$$\exists b \in R \setminus \{z\} : ab = z \ \vee \ ba = z,$$

where z is the zero element.

In other words, R has no zero divisors if $ab = z$ implies that either $a = z$ or $b = z$. The number rings have no zero divisors, because if $ab = 0$, then $a = 0$ or $b = 0$. This property was fundamental to solving equations, because it ensured that e.g. if $(x-1)(x-2) = 0$, then $x = 1$ or $x = 2$, and there is no other solution. With zero divisors, this would be much more complicated.

Example. For matrices, $\left(\begin{smallmatrix} 2 & 2 \\ 2 & 2 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, i.e. $\left(\begin{smallmatrix} 2 & 2 \\ 2 & 2 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ are zero divisors in $\mathbb{R}^{2\times 2}$.

Example. In $\mathbb{Z}_6$, $\overline{2} \cdot \overline{3} = \overline{0}$ (because $2 \cdot 3 = 6$), i.e. $\overline{2}$ and $\overline{3}$ are zero divisors in $\mathbb{Z}_6$.

Theorem 2.5 (zero divisors in $\mathbb{Z}_m$)**.**

1. *$\overline{a} \in \mathbb{Z}_m$ is a zero divisor if and only if $\overline{a} \neq \overline{0}$ and* $\gcd(a, m) \neq 1$.
2. *$\mathbb{Z}_m$ has zero divisors if and only if m is a composite number.*

So for prime numbers, $\mathbb{Z}_p$ has no zero divisors.

Rings that have all the good properties listed above will come very useful later:

Definition 2.6. The ring R is called an **integral domain** if

0. it has at least two elements,
1. it is commutative,
2. it has an identity element and
3. it has no zero divisors.

Example. The four basic number rings ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) are all integral domains, so are the polynomial rings based on them ($\mathbb{Z}[x]$, $\mathbb{R}[x]$ etc.), and $\mathbb{Z}_p$ for prime numbers.

(The reason for the "at least two elements" criterion is to exclude the zero ring, therefore ensure that the identity element is not the same as the zero element, which would lead to complications later.)

3 Field

There is one more important property: the analogue of the additive inverse $(-a)$ for multiplication:

Definition 3.1. Let R be a ring with identity. The **multiplicate inverse** of $a \in R$ is x if

$$ax = e \ \wedge \ xa = e,$$

where e is the identity element. Notation: a^{-1}. (It is sometimes simply called the **inverse** of a.) An element is called **invertible** if it has a multiplicative inverse.

Example. The multiplicative inverse of $2 \in \mathbb{Q}$ is $1/2$, as $2 \cdot 1/2 = 1$. For any $a \in \mathbb{Q} \setminus \{0\}$, $a^{-1} = 1/a$.

Example. In $\mathbb{Z}$, only 1 and -1 are invertible (the inverse of either one is itself).

Example. The multiplicative inverse of the matrix $A = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 5 \end{smallmatrix}\right) \in \mathbb{R}^{2\times 2}$ is $A^{-1} = \left(\begin{smallmatrix} -5 & 2 \\ 3 & -1 \end{smallmatrix}\right)$, because $AA^{-1} = I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $A^{-1}A = I$. On the other hand, $B = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 6 \end{smallmatrix}\right)$ is not invertible, because $\det B = 0$.

Example. The multiplicative inverse of $\overline{3} \in \mathbb{Z}_{10}$ is $\overline{7}$, because $\overline{3} \cdot \overline{7} = \overline{1}$. In general, the multiplicative inverse in $\mathbb{Z}_m$ coincides with the *modular inverse* (see: Congruences), i.e. $\overline{a} \in \mathbb{Z}_m$ is invertible if and only if $\gcd(a, m) = 1$. In $\mathbb{Z}_{10}$, this means that exactly $\overline{1}$, $\overline{3}$, $\overline{7}$ and $\overline{9}$ are invertible.

Theorem 3.2 (properties of the multiplicative inverse)**.**

1. *The multiplicative inverse is unique.*
2. *The multiplicative inverse of the identity element is itself:* $e^{-1} = e$.
3. *The multiplicative inverse of the multiplicative inverse is the original element:* $(a^{-1})^{-1} = a$.
4. *The zero element is not invertible.*
5. *A zero divisor is not invertible.*

Now we can define the other most important algebraic structure besides the ring:

Definition 3.3. The ring R is called a **field** if

0. it has at least two elements,
1. it is commutative,
2. it has an identity element and
3. all nonzero elements are invertible.

Notice that any field is also an integral domain, because their definitions differ only in point 3, and an invertible element cannot be a zero divisor (see the above theorem).

(Point 3 had to exclude the zero element, because it can never be invertible in any ring, since multiplying any element by it results in the zero element. This corresponds to the fact that numbers cannot be divided by 0.)

Example. From the rings listed so far, the following ones are fields:

1. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ – they are called **number field**s.
2. $\mathbb{Z}_p$ for any prime number p, because all of its non-$\overline{0}$ elements are invertible.

On the other hand, the ring of integers, $\mathbb{Z}$ is *not* a field, because only 1 and -1 are invertible.

To summarize fields, here is the full definition without the use of rings, in a similar format than the definition of rings above:

Definition 3.4 (field)**.** $(F, +, \cdot)$ is a **field** if the following properties (*field axioms*) are satisfied:

A. **additive operation** $(+)$:
   1. closed: $\forall a, b \in F : \ a + b \in F$;
   2. associative: $\forall a, b, c \in F : \ (a + b) + c = a + (b + c)$;
   3. commutative: $\forall a, b \in F : \ a + b = b + a$;
   4. **zero element**: $\exists z \in F : \forall a \in F : \ a + z = a$;
   5. **additive inverse**: $\forall a \in F : \exists x \in F : \ a + x = z$ (where z is the zero element);

M. **multiplicative operation** $(\cdot)$:
   1. closed: $\forall a, b \in F : \ a \cdot b \in F$;
   2. associative: $\forall a, b, c \in F : \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$;
   3. commutative: $\forall a, b \in F : \ a \cdot b = b \cdot a$;
   4. **identity element**: $\exists e \in F \setminus \{z\} : \forall a \in F : \ a \cdot e = a$;
   5. **multiplicative inverse**: $\forall a \in F \setminus \{z\} : \exists x \in F : \ a \cdot x = e$ (where e is the identity elem.);

D. "$\cdot$" is distributive over "$+$":
   $\forall a, b, c \in F : \ a \cdot (b + c) = a \cdot b + a \cdot c$.

Note that fields (unlike rings) have the same requirements for the multiplicative operation than for the additive one (except for the multiplicative inverse of the zero element, which is impossible).

(Note: because the multiplication is now known to be commutative, certain properties were simplified compared to the ring's definition, e.g. now the distributivity can be stated in only one direction.)

In fields, we can finally define the fourth fundamental operation, division (similarly to subtraction, see above, after the rings):

Definition 3.5 (division)**.** For a field F and $a, b \in F$, $b \neq z$: $\boldsymbol{a/b} := ab^{-1}$.

Example. In $\mathbb{Q}$, it means that $5/2 = 5 \cdot 2^{-1} = 5 \cdot (1/2)$.

It follows from the definition that $(a/b)\, b = a$ and $(ab)/b = a$, as expected.

4 Rings in Sage

Sage denotes the number rings ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) by double letters (instead of double-lined letters):

```
sage: ZZ
Integer Ring
sage: QQ
Rational Field
sage: RR              # avoid RR and CC, they can only be represented numerically
Real Field with 53 bits of precision
```

The names of rings can be used for type conversion:

```
sage: type(QQ(12))   # ZZ -> QQ conversion
<class 'sage.rings.rational.Rational'>
sage: type(6/3)      # fractions are always in QQ, even if they are integers
<class 'sage.rings.rational.Rational'>
sage: type(ZZ(6/3))  # but they can be converted to ZZ
<class 'sage.rings.integer.Integer'>
sage: ZZ(2/3)        # but this one can't
[...]
TypeError: no conversion of this rational to integer
sage: RR(2/3)        # QQ -> RR: approximation, should be avoided
0.666666666666667
```

Matrix rings (e.g. $\mathbb{Z}^{3\times3}$) can be created by the `Mat()` function:

```
sage: Mat(ZZ, 3)     # 3×3 integer matrices
Full MatrixSpace of 3 by 3 dense matrices over Integer Ring
sage: M = Mat(ZZ, 3)
sage: M([[3,1,-4], [2,5,6], [1,4,8]])
[ 3  1 -4]
[ 2  5  6]
[ 1  4  8]
sage: M.one()        # identity element
[1 0 0]
[0 1 0]
[0 0 1]
```

The ring $\mathbb{Z}_m$ can be created by the `Zmod(m)` function:

```
sage: Zmod(10)
Ring of integers modulo 10
sage: Z10 = Zmod(10)
sage: Z10(34)        # ZZ -> Zmod(10) conversion
4
sage: Z10(34) * 13   # 13 is converted automatically
2
sage: type(Z10(34))
<class 'sage.rings.finite_rings.integer_mod.IntegerMod_int'>
```

An easier way to create the elements $\overline{a} \in \mathbb{Z}_m$ is using the `mod(a, m)` function, which is equivalent to the conversion `Zm = Zmod(m); Zm(a)`, but without creating the ring `Zmod(m)`. However, don't confuse `mod()` with the operator `%`, because the latter returns an integer:

```
sage: mod(34, 10)       # same as Z10(34) above
4
sage: mod(34, 10) ^ 2   # it remains modular
6
sage: (34 % 10) ^ 2     # NOT the same: it is an integer
16
sage: type(mod(34, 10))
<class 'sage.rings.finite_rings.integer_mod.IntegerMod_int'>
sage: type(34 % 10)
<class 'sage.rings.integer.Integer'>
```

The elements of finite rings (e.g. $\mathbb{Z}_m$) can be enumerated:

```
sage: list(Zmod(10))
[0, 1, 2, 3, 4, 5, 6, 7, 8, 9]
sage: [4*a for a in Zmod(10)]
[0, 4, 8, 2, 6, 0, 4, 8, 2, 6]
sage: for a in Zmod(10):
....:     print(a, a^2)
0 0
1 1
2 4
3 9
4 6
5 5
6 6
7 9
8 4
9 1
```

5 Polynomials over rings

The previous document (Basics of polynomials) discussed polynomials, but only when the coefficients are numbers (e.g. $\mathbb{Z}[x]$, $\mathbb{R}[x]$). Now it is time to generalize them to rings.

In this section, let K be an arbitrary commutative ring, and consider $K[x]$, the set of **polynomials over K**, i.e. the polynomials whose coefficients are from the ring K.

For example, $\mathbb{Z}_4[x]$ is the set of polynomials over the residue classes modulo 4 ($\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$):

```
sage: P4.<x> = Zmod(4)[]
sage: P4
Univariate Polynomial Ring in x over Ring of integers modulo 4
sage: p = 2*x + 3
sage: q = 3*x + 1
sage: p * q
2*x^2 + 3*x + 3
sage: p + q
x
```

Why is $p+q = x$? Because in $\mathbb{Z}_4$, $\overline{2}+\overline{3} = \overline{1}$ and $\overline{3}+\overline{1} = \overline{0}$, so $p+q = \overline{1}x+\overline{0} = x$. In general, operations in $\mathbb{Z}_m[x]$ can be performed by first calculating the result in $\mathbb{Z}[x]$, and then taking each coefficient modulo m. For example, in $\mathbb{Z}[x]$, the above $p \cdot q = 6x^2 + 11x + 3$, so in $\mathbb{Z}_4[x]$, $p \cdot q = \overline{2}x^2 + \overline{3}x + \overline{3}$.

Back to arbitrary K, it is easy to prove that $K[x]$ is also a ring, and it inherits most of the additional properties of the coefficient ring K:

Theorem 5.1 (properties of $K[x]$)**.**

1. *If K is a commutative ring, then $K[x]$ is also a commutative ring.*
2. *If K is a ring with identity, then $K[x]$ is also a ring with identity.*
3. *If K has no zero divisors, then $K[x]$ has no zero divisors either.*
4. *If K is an integral domain, then $K[x]$ is also an integral domain.*

So for example $K[x]$ inherits the identity element of K, and if K has no zero divisors, then $K[x]$ doesn't introduce them either. But there is one property that cannot be fully inherited:

Theorem 5.2. *The polynomial $x \in K[x]$ has no multiplicative inverse.*

So the ring $K[x]$ can never be a field, regardless of whether K is a field or not.

Example. $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$ are integral domains, but none of them are fields.

Example. $\mathbb{Z}_p[x]$ (for prime p) is also an integral domain, but not a field (even though $\mathbb{Z}_p$ is a field).

Now consider the statements from the previous document (Basics of polynomials), and see what conditions we need for the coefficient ring K in order for these statements to remain valid:

1. First of all, if K were not commutative, then even the multiplication of two polynomials were problematic, e.g. for $2x \cdot 2x = 4x^2$, we need that $x \cdot 2 = 2 \cdot x$. That's why we restricted K to be a commutative ring.
2. If K has no identity element, then we encounter problems with the root factors: the leading coefficient of $x - c$, though not indicated, is the identity element (e.g. $1x - c$); so if K has no identity, then $x - c \notin K[x]$. Therefore, K should be a ring with identity.

3. The theorem about the degree of the product of two polynomials (Theorem 1.7. part 3.), i.e. $\deg(p \cdot q) = \deg p + \deg q$ is true only if K has no zero divisors. For example, in $\mathbb{Z}_6[x]$, we have $(\overline{2}x + \overline{1})(\overline{3}x + \overline{1}) = \overline{5}x + \overline{1}$, i.e. the product is not a quadratic polynomial, because the original leading coefficient has vanished due to zero divisors: $\overline{2}x \cdot \overline{3}x = \overline{0}x^2$.
4. Zero divisors also break another important theorem, namely that a polynomial of degree n can have at most n roots (Theorem 4.5.): e.g. in $\mathbb{Z}_6[x]$, the polynomial $p = x^2 + x$ has *four* roots: $\overline{0}, \overline{2}, \overline{3}, \overline{5} \in \mathbb{Z}_6$ (and so the root factor form is not unique: $p = (x - \overline{2})(x - \overline{3}) = x(x - \overline{5})$). The theorem only remains true if we add the condition that "K has no zero divisors". (We used this in the proof when saying "if $p(c) = 0$, then one of the factors must be 0".)

But if K is an integral domain, i.e. it doesn't have any of the problems listed above, then all theorems and definitions of the previous document remain valid. Also, if we only require that K is a commutative ring with identity (i.e. we allow zero divisors), then all theorems except the two mentioned above (and their consequence, Lagrange interpolation) remains true.

5.1 Shamir's secret sharing – continued

In the previous document, we introduced Shamir's secret sharing, based on Lagrange interpolation. However, the way it was described (using integers and rational numbers) is not how it is used in practice, so we need to extend the description.

We have seen that Lagrange interpolation doesn't work in $\mathbb{Z}[x]$ (because of the divisions), only in $\mathbb{Q}[x]$ or $\mathbb{R}[x]$. Now we can state generally that it works over any *field*, including $\mathbb{Z}_p[x]$, where p is a prime number.

In practice, Shamir's secret sharing is done in $\mathbb{Z}_p[x]$, where p is a large enough prime number to contain the secret S. Continuing the example described in the previous document, let $n = 5$, $k = 3$ and $S = 67$, and generate a quadratic polynomial similarly, but now in $\mathbb{Z}_{89}[x]$ instead of $\mathbb{Z}[x]$:

$$p = \overline{13}x^2 + \overline{38}x + \overline{67} \in \mathbb{Z}_{89}[x].$$

It is then evaluated in five places (and we get the same values as before, but modulo 89):

$$p(\overline{1}) = \overline{29}, \quad p(\overline{2}) = \overline{17}, \quad p(\overline{3}) = \overline{31}, \quad p(\overline{4}) = \overline{71}, \quad p(\overline{5}) = \overline{48}.$$

The secret can be recovered in the same way, but now the calculations are in $\mathbb{Z}_{89}$ instead of $\mathbb{Q}$.

$\mathbb{Z}_p$ has many advantages over the "naive" method: first, being a field, the problem described in the previous document can no longer happen (though we still get that $S = \overline{5}a + \overline{2}$, but now this leaks no information about S at all, because the linear congruence $5a \equiv S - 2 \pmod{89}$ is solvable for any S, see: Congruences); also, being finite, it is trivial to choose random numbers from $\mathbb{Z}_p$.

6 Author

This document was written by Uray M. János, partly using the following sources:

[1] https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa (Hungarian)

[2] https://en.wikipedia.org/wiki/Ring_(mathematics)

[3] https://en.wikipedia.org/wiki/Integral_domain

[4] https://en.wikipedia.org/wiki/Field_(mathematics)

Errors and suggestions can be reported here: uray.janos@inf.elte.hu.