Due date: 8.10.2019

Notation

$\mathbb{N} = \{0, 1, 2, ...\}$ denotes the set of natural numbers (non-negative integers).

$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ denotes the set of integers.

$\mathbb{Q}$ denotes the set of rational numbers (integer fractions).

$\mathbb{R}$ denotes the set of real numbers.

$\mathbb{C}$ denotes the set of complex numbers.

1 Recap: Algebraic structures

This section gives a short recap of basic algebraic structures used in computer algebra and is intended primarily for students of the AI programme. You may skip this section and the exercises therein if you feel comfortable with these constructions. Additional material on these preliminary structures may be found in the recommended textbook of this course: Winkler [1, Section 1.3 (Algebraic preliminaries)].

Basic algebraic structures

In this course we focus our interest on algebraic structures which consist of an underlying set and typically two binary operations (to be defined below) with certain properties.

Definition 1 (Binary operation)
A binary operation $\circ$ *on a set S is a mapping that combines two elements of S to form a third, in the usual notation $\circ : S \times S \to S$. Binary operations are typically written in infix notation, i.e. instead of $\circ(u, v)$ we write $u \circ v$, where $u, v \in S$.*

The binary operation $\circ$ is called associative *if*

$$\forall u, v, w \in S : (u \circ v) \circ w = u \circ (v \circ w).$$

Since it does not matter how we put the parentheses in this case they are usually omitted and we write just $u \circ v \circ w$.

A binary operation $\circ$ is called commutative *if the order of the operands is irrelevant, i.e.*

$$\forall u, v \in S : u \circ v = v \circ u.$$

Now we are ready to define our first algebraic structure.

Definition 2 (Ring)
A ring *consists of a set R together with two binary operations $+$ and $\cdot$ acting on R such that the following axioms are satisfied:*

1. a) *The binary operation $+$ is associative.*
   b) *The binary operation $+$ is commutative.*
   c) *There is a fixed element in R, denoted by 0, such that $\forall r \in R : 0 + r = r$. (additive identity)*
   d) *For each element $r \in R$ there is an element $-r \in R$ such that $r + (-r) = 0$. (additive inverse)*
2. a) *The binary operation $\cdot$ is associative.*
   b) *There is a fixed element in R, denoted by 1, which is different from 0 and satisfies $\forall r \in R : 1 \cdot r = r \cdot 1 = r$. (multiplicative identity[1])*
3. a) $\forall r, s, t \in R : r \cdot (s + t) = (r \cdot s) + (r \cdot t)$. *(left distributivity)*
   b) $\forall r, s, t \in R : (r + s) \cdot t = (r \cdot t) + (s \cdot t)$. *(right distributivity)* ■

The operations $+$ and $\cdot$ are called *addition* and *multiplication*, respectively and the corresponding identities are also known as *zero* and *one*. For the sake of brevity, we often neglect to mention the operations and identities explicitly and just call the underlying set R a ring. One can show—and you should do so—that the additive and multiplicative identity of a ring are unique, as well as the inverse of each element. We will not really consider general rings in this course, but rather those of the following subclass.

Definition 3 (Commutative ring)
A ring is called commutative *if multiplication is commutative.* ■

The archetypical example of a commutative ring is the set of integers $\mathbb{Z}$ together with the usual addition and multiplication. The numbers 0 and 1 act as additive and multiplicative identity, respectively. Another commutative ring can be formed from the power set $\mathcal{P}(S)$ of a non-empty set S. Symmetric difference plays the role of addition with the empty set as additive identity. The intersection of sets together with S itself constitute multiplication and the multiplicative identity.

Exercise
Find a simple example of a non-commutative ring (think back to the golden days of your linear algebra classes).

[1] This condition is a matter of debate. The textbook for example does not require rings to have a multiplicative identity and calls those who do *rings with identity*. However, all rings which we will encounter have such an identity, thus we may forget about the non-unital case at this point. Also, some authors relax the condition that $1 \neq 0$. However, there is only one ring where the additive and multiplicative identity coincide—known as the *zero ring*—containing a single element. This object is so boring to study that we exclude it right away.

Before we move on to the next algebraic structure, let us consider a family of commutative rings which will be our daily bread in computer algebra.

Definition 4 (Univariate polynomial ring)
Let R be a commutative ring. The polynomial ring *over R in one variable x, denoted by $R[x]$, consists of the set of all sequences $(p_0, p_1, p_2, \ldots)$ in R where only finitely many of the p_i are non-zero. Such sequences are typically written in the form*

$$p(x) = \sum_{i=0}^{n} p_i x^i = p_0 + p_1 x + p_2 x^2 + \cdots + p_n x^n,$$

where $p_i = 0$ for all $i > n$, $n \in \mathbb{N}$. The elements of $R[x]$ are called polynomials *in the variable x and the ring elements $p_0, p_1, p_2, \ldots$ of the above polynomial are called the* coefficients *of $p(x)$. Furthermore, a polynomial $p(x)$ is called* constant *if the coefficients $p_i = 0$ for all $i > 0$. A* monomial *is a polynomial where exactly one coefficient is non-zero.*

To give $R[x]$ the structure of a ring, consider two polynomials[2] $f = \sum_{i=0}^{n} f_i x^i$ and $g = \sum_{i=0}^{n} g_i x^i$ and define

$$f + g := \sum_{i=0}^{n} (f_i +_R g_i) x^i \quad \text{and} \quad f \cdot g := \sum_{i=0}^{2n} \left(\sum_{j=0}^{i} f_j \cdot_R g_{i-j} \right) x^i,$$

where $+_R$ and $\cdot_R$ are addition and multiplication of the base ring R. The additive and multiplicative identity in $R[x]$ are the same as in R, but now considered as constant polynomials. ∎

Nothing extraordinary happens in this definition: We write polynomials in the common power-of-x notation, addition is defined coefficientwise as expected and a closer look at the multiplication rule will show that this is just the usual expansion (distribution of multiplication over addition) and collecting terms of the same power of x. There is also a relatively straightforward construction for polynomial rings in more than one variable. You may look it up in the textbook [1, Section 1.3 (Algebraic preliminaries)]. We shall denote a polynomial ring over a commutative ring R in n variables $x_1, \ldots, x_n$ by $R[x_1, \ldots, x_n]$.

Exercise
Give a simple argument why the antecedent definition of polynomial multiplication is commutative (recall that the base ring is assumed to be commutative). Hence, a polynomial ring will always be a commutative ring.

Weird phenomenons can happen in general rings. For example, consider the set of 2×2 matrices over $\mathbb{Z}$ with the usual matrix addition and multiplication. If we multiply the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

then the product of two non-zero matrices suddenly yields the zero-matrix. This phenomenon is so common that it has its own name, though we define it only for commutative rings.

[2] We take the upper bound of summation large enough such that both polynomials can be written in this form, i.e. we perform automatic zero-padding of potentially shorter polynomials.

Definition 5 (Zero divisor)
Let R be a commutative ring. A non-zero element[3] *$r \in R$ is called* zero divisor *if there exists a non-zero element $s \in R$ such that $r \cdot s = 0$.* ■

Computations in the presence of zero divisors are more complicated. One thing we can no longer use in this case is the cancellation law, cf. next exercise. For this reason we shall specialise our class of rings yet again.

Definition 6 (Integral domain)
An integral domain *or simply* domain *is a commutative ring without zero divisors.* ■

Exercise (Cancellation law)
Let I be an integral domain. Show that for all $r, s, t \in I$ the following holds:

$$(r \cdot s = r \cdot t \wedge r \neq 0) \;\Rightarrow\; s = t.$$

Exercise
Continuing the exercise on commutativity of polynomial rings: If I is an integral domain, show that the polynomial ring $I[x]$ is an integral domain as well. By using the fact that $R[x_1, \ldots, x_n] \cong (R[x_1, \ldots, x_{n-1}])[x_n]$ (the two objects are isomorphic as rings, R being a commutative ring) conclude that the multivariate polynomial ring $I[x_1, \ldots, x_n]$ is an integral domain as well.

Now then, let us get on to the next algebraic structure. To shorten the definition a bit, let us state it in terms of the previous structures and not give the extensive classical definition.

Definition 7 (Field)
A field is a commutative ring where all non-zero elements have a multiplicative inverse. More specifically, a set K with binary operations $+$ and $\cdot$ is a field if the following conditions hold:

1. *The set K with $+$ as addition and $\cdot$ as multiplication has the structure of a commutative ring.*
2. *For each element $x \in K^*$ there is an element $x^{-1} \in K^*$ such that $x \cdot x^{-1} = 1$, where $K^* = K \setminus \{0\}$ denotes the underlying set without the additive identity.* ■

Exercise
Show that every field is an integral domain, i.e. there can not be any zero-divisors.

Fields are often denoted by the letter K from the German word "Körper". The sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ together with the usual arithmetic operations are all examples of fields, whereas $\mathbb{Z}$ lacks inverse elements for integers other than -1 and 1. This brings us to yet another concept for rings.

[3] There is another definition of zero divisor which allows the additive identity zero to be a zero divisor. The version given here is the one used in the textbook.

Definition 8 (Unit)
Let R be a ring. A unit $u \in R$ *is an element with a two-sided multiplicative inverse, i.e. there exists an element $v \in R$ such that*

$$u \cdot v = v \cdot u = 1,$$

where $\cdot$ and 1 are the respective multiplication operation and unit in R. ■

An alternative definition of a field would thus be a commutative ring where every non-zero element is a unit.

Exercise
Let K be a field. What are the units in the polynomial ring $K[x]$?

To conclude this section, let us define one last subclass of rings. The definition seems quite innocent, but proving that something fulfils all conditions can be tricky. For us it will be sufficient to get the gist of how such an object behaves. First we need a preliminary definition.

Definition 9 (Irreducible element)
Let I be an integral domain. An element $r \in I$ is called irreducible *if it is non-zero, non-unit and can not be written as the product of two non-units. An element which is not irreducible is called* reducible. ■

For example, in $\mathbb{Q}[x]$ the units are all rational numbers different from zero (interpreted as constant polynomials). The polynomial $x^2 - 1$ is reducible, since it can be written as the product $x^2 - 1 = (x + 1) \cdot (x - 1)$.

Definition 10 (Unique factorisation domain (UFD))
A unique factorisation domain *is an integral domain which satisfies the following properties:*

1. *Every non-zero element can be written as a finite product of irreducible elements and a unit. We assume that the empty product yields the multiplicative identity, hence a unit is already in factored form.*
2. *Every such product factorisation is unique up to ordering and multiplication by units.* ■

The uniqueness part of a UFD is typically the trickiest part to proof. To give a simple example of what this is about, consider once again the set of integers $\mathbb{Z}$ together with the usual addition and multiplication. The numbers 1 and -1 are the units of this domain. Now, since our earliest days of university mathematics we know that a natural number greater than one has a unique factorisation into prime numbers. This factorisation is unique up to permutation of the prime factors. Integers different from -1, 0 and 1 can be factored in a similar way, but now two factors could be multiplied by -1 without changing the result. For example, $-84 = (-2) \cdot 2 \cdot 3 \cdot 7 = 2 \cdot 2 \cdot 3 \cdot (-7) = (-1) \cdot 2 \cdot 3 \cdot 7 \cdot 2$. The irreducible factors of each factorisation are identical up to multiplication by the unit -1. Changing the order of the factors won't hurt in a commutative ring either. Now, working in a UFD means that these

trivialities are the only way how factorisations of non-zero and non-unit elements might differ. How to actually compute such a factorisation is of course another story.

A polynomial ring in any number of variables over a UFD will also be a UFD. The examples so far might suggest that having a factorisation which are essentially unique is quite common. The following exercise shows that this is not the case.

Exercise
Let us define an innocent looking ring (integral domain) with an underlying set $\mathbb{Z}[\sqrt{-5}] := \left\{a + b\sqrt{-5} \;\middle|\; a, b \in \mathbb{Z}\right\}$*. Addition and multiplication is defined as follows*[4]*:*

$$\begin{aligned}(a + b\sqrt{-5}) + (c + d\sqrt{-5}) &= (a + c) + (b + d)\sqrt{-5}\\ (a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) &= (a \cdot c) + (a \cdot d\sqrt{-5}) + (b \cdot c\sqrt{-5}) + (b \cdot d \cdot \sqrt{-5}^2)\\ &= (a \cdot c + b \cdot d \cdot (-5)) + (a \cdot d + b \cdot c)\sqrt{-5}.\end{aligned}$$

We did not use different symbols for the ring operations in $\mathbb{Z}[\sqrt{-5}]$ *and the base ring* $\mathbb{Z}$*. Make sure to understand which operation is used at what point. Note: There is also an addition symbol which is not a ring operation.*

Now show that this integral domain is not a UFD. Hint*: For a pure integer* $9 + 0\sqrt{-5}$ *consider its prime factorisation and a factorisation of the form* $(x + y\sqrt{-5}) \cdot (x + (-y)\sqrt{-5}) = x^2 + (-y^2)\sqrt{-5}^2$.

Quotient field

Sometimes during computations it becomes convenient to divide by elements even though we work in a ring and not a full field. This is exactly what the quotient field construction does: Given a nice enough ring R, the quotient field builds from R a field in which we can embed the ring in a natural way. Even better, the construction is not bloated, i.e. the resulting field is the smallest possible. As was mentioned before, the ring R should be a benevolent one. Recall from the previous exercises that a field is necessarily free of zero divisors, hence our quotient field construction will work for integral domains.

There is no need to let terror grip your heart when reading the definition below. Actually, this construction is very well known to you, only written in more general terms. Recall that the integers $\mathbb{Z}$ with the usual arithmetic is an integral domain, but not a field. To invert elements we would need fractions, in other words, the quotient field of $\mathbb{Z}$ turns out to be the field of rational numbers $\mathbb{Q}$. Adding two rational numbers requires to bring them first over a common denominator, whereas multiplication is performed by multiplying numerators and denominators. You may ask why we need the equivalence classes[5] below. For the same

[4] This construction should remind you somewhat of the complex numbers in classical notation $a + bi$.
[5] If you do not recall what an equivalence class on a set is and how such a thing can be obtained from an equivalence relation, this is an excellent time to look it up.

reason as in $\mathbb{Q}$, since we want that $\frac{4}{6}$ and $\frac{2}{3}$ denote the same number (they are in the same equivalence class).

Definition 11 (Quotient field)
Let I be an integral domain with addition $+_I$ and multiplication $\cdot_I$. The quotient field *or* field of fractions *of I, denoted by $Q(I)$, has as underlying set the set of formal fractions of elements in I modulo the equivalence relation*

$$\frac{a}{b} \sim \frac{a'}{b'} \Leftrightarrow a \cdot_I b' = a' \cdot_I b$$

for all $a, a' \in I$ and $b, b' \in I \setminus \{0\}$. In other words, $Q(I)$ consists of the set

$$\left\{ \frac{a}{b} \,\middle|\, a, b \in I \wedge b \neq 0 \right\} / \sim.$$

Addition $(+)$ and multiplication $(\cdot)$ of such fractions is defined as follows:

$$\frac{a}{b} + \frac{c}{d} := \frac{(a \cdot_I d) +_I (b \cdot_I c)}{b \cdot_I d}$$
$$\frac{a}{b} \cdot \frac{c}{d} := \frac{a \cdot_I c}{b \cdot_I d}$$

for all $\frac{a}{b}, \frac{c}{d} \in Q(I)$. The additive and multiplicative identities are $\frac{0}{1}$ and $\frac{1}{1}$, respectively. ∎

You will verify in the exercise below that addition and multiplication is indeed well defined, i.e. is compatible with the equivalence class structure. There is a natural way to embed an integral domain in its quotient field by the map

$$\phi : I \to Q(I),\ r \mapsto \frac{r}{1},$$

which is precisely the same if we would treat an integer $a \in \mathbb{Z}$ as a rational number $\frac{a}{1} \in \mathbb{Q}$.

Exercise
Show that addition and multiplication of fractions in a quotient field is well defined. In other words, show that for fractions $\frac{a}{b} \sim \frac{a'}{b'}$ and $\frac{c}{d} \sim \frac{c'}{d'}$ in $Q(I)$ the following holds:

$$\left(\frac{a}{b} + \frac{c}{d}\right) \sim \left(\frac{a'}{b'} + \frac{c'}{d'}\right) \quad \text{and} \quad \left(\frac{a}{b} \cdot \frac{c}{d}\right) \sim \left(\frac{a'}{b'} \cdot \frac{c'}{d'}\right).$$

Exercise
The definition of the quotient field does not explicitly say how the additive and multiplicative inverses look like. For $\frac{a}{b}, \frac{c}{d} \in Q(I)$ with $c \neq 0$, what are

$$-\left(\frac{a}{b}\right) \quad \text{and} \quad \left(\frac{c}{d}\right)^{-1}$$

as elements of $Q(I)$?

Exercise
Let K be a field. What would the construction of the quotient field $Q(K)$ yield? Are the fields K and $Q(K)$ related in some way?

2 Exercises

The exercises are meant as an invitation to become acquainted with a computer algebra system (CAS) of your choice. Subsequent exercise sheets contain problems which have to be solved on a computer from time to time. Furthermore, some of the projects (to be discussed later) will contain explicit programming tasks, so it is a good idea to familiarise yourself with a CAS early on.

The following selection lists some of the most popular and user-friendly systems.

1. Wolfram Mathematica (https://www.wolfram.com/mathematica/): Requires a license
2. Maple (https://www.maplesoft.com/products/maple/): Requires a license
3. SageMath (https://www.sagemath.org/): Downloadable for free at http://www.sagemath.org/download.html

A more extensive list can be found here:
https://en.wikipedia.org/wiki/List_of_computer_algebra_systems

Should you decide to use a CAS other than Mathematica, Maple or SageMath, be aware that some of the methods and procedures of this course might not be available.

Exercise 1
Pick a CAS of your choice and perform some arithmetic computations with integers, integers modulo a prime number, polynomials, etc. Find out how to solve a system of linear equations in this system. Read the help pages on solving polynomial equations.

Exercise 2
Given the matrix

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 2 & 3 \\ 0 & 0 & 0 & 3 & 4 \end{bmatrix}.$$

Compute all solutions of the linear system $A \cdot [x_1, x_2, x_3, x_4, x_5]^T = [1, 2, 3, 4, 5]^T$. *You should do this with the aid of a CAS.*

Exercise 3
Consider the polynomial $f(x) = x^5 - x^4 + x^3 - x^2 + x - 2$. *Use a CAS to perform the following tasks:*

1. *Compute the roots of* f *numerically. You have influence on floating point precision if you want to.*

2. *Generate a picture of the graph of the polynomial function* $f : [a, b] \to \mathbb{R},\ x \mapsto f(x)$. *Choose the boundaries* a *and* b *of the intervall in such a way that you can "see" the real roots of* $f(x)$.
3. *Compute the roots of* $f(x)$ *symbolically. What output does your CAS generate?*
4. *Compute the roots of the polynomial* $g(x) = 2x^2 + 2x^3 + 2x^4 + x^5 - x^6 + 3x + 1$.

Exercise 4
Use a CAS to compute greatest common divisors (GCD) in different domains.

1. *Compute the integer GCD of the numbers* $a = 215712$ *and* $b = 739914$.
2. *Compute the polynomial GCD of* $f(x) = 6x^5 + 2x^4 - 19x^3 - 6x^2 + 15x + 9$ *and* $g(x) = 5x^4 - 4x^3 + 2x^2 - 2x - 2$.

References

[1] Franz Winkler. *Polynomial Algorithms in Computer Algebra*. Springer-Verlag Wien, 1996.