Due date: 15.10.2019

1 Short digression: Finite fields

This section is meant for those who have not seen finite fields before.

1.1 Finite fields obtained from integers modulo a prime

Recall from the previous exercise sheet that a field is an algebraic structure which consists of an underlying set and two binary operations $+$ and $\cdot$ called addition and multiplication, respectively. Furthermore, for all elements of the underlying set, there exist elements which are inverse with respect to addition and for all elements but the additive identity (zero) there exists a multiplicative inverse. We call the operation of adding an element with the (additive) inverse of another *subtraction* and multiplication of an element with the (multiplicative) inverse of another *division*. In short, a field is some set for which the typical arithmetic operations addition, subtraction, multiplication and division is defined. Of course, in order to have inverses, we need two (different) elements which behave like the usual zero and one in arithmetic.

Well known examples of fields are the numbers $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ with the usual arithmetic operations. All of them are examples of infinite fields, i.e. fields where the underlying set contains infinitely many elements. But there are also fields which have only finitely many elements.

Definition 1 (Finite field)
A finite field *is a field where the underlying set is finite. The number of elements of a finite field F is called the* order *of F.* ■

Since every finite field must contain at least the additive and multiplicative identity, there can not exist a finite field of order less than two. In this section we will discuss finite fields of order $p \in \mathbb{P}$, where the latter denotes the set of prime numbers.

In general, the finite field[1] of order q is usually denoted by $\mathbb{F}_q$ or $GF(q)$, where the abbreviation GF stands for *Galois field*. The order of a finite field is subject to certain restrictions as we will see at the end of this section. Perhaps the easiest example of a finite field is $\mathbb{F}_2$ which we construct in the following way:

- The underlying set is $\{0, 1\}$.

[1] There are many ways to construct a finite field of a certain fixed order q with the only restriction that q must be a prime or a positive power of a prime number. All of these constructions are essentially the same (in mathematical terms: they are isomorphic), hence we speak of "the finite field" of order q and not "a finite field" of order q.

- Addition is defined by $0+0=0$, $0+1=1$ and $1+1=0$ (this suffices since addition is commutative).
- Multiplication is defined by $0\cdot 0=0$, $0\cdot 1=0$ and $1\cdot 1=1$ (recall that multiplication is also commutative).

The astute reader will notice that this is just addition and multiplication followed by taking the remainder upon division by 2 (i.e. take the result modulo[2] 2).

Exercise
Verify that $\mathbb{F}_2$ is indeed a field. There is no need to check distributivity, associativity and commutativity. Also, it should be clear what the respective identities are. What you should check, however, is what the additive and multiplicative inverses are.

Exercise
Let us see if this construction works for the integers modulo 5: Let $\mathbb{Z}_5=\{0,1,2,3,4\}$ and define the binary operations

$$+ : \mathbb{Z}_5\times\mathbb{Z}_5\to\mathbb{Z}_5,\ (a,b)\mapsto (a+_{\mathbb{Z}} b) \bmod 5,$$
$$\cdot : \mathbb{Z}_5\times\mathbb{Z}_5\to\mathbb{Z}_5,\ (a,b)\mapsto (a\cdot_{\mathbb{Z}} b) \bmod 5,$$

where $+_{\mathbb{Z}}$ and $\cdot_{\mathbb{Z}}$ is the usual integer addition and multiplication. Complete the following tables for addition and multiplication:

$+$	0	1	2	3	4
0					
1					
2					
3					
4					

$\cdot$	0	1	2	3	4
0					
1					
2					
3					
4					

As in the previous exercise, verify the existence of additive and multiplicative inverses with respect to the identities 0 (zero) and 1 (one).

It turns out that the construction in the previous exercise works for all prime numbers. Let n be a positive integer. By

$$\mathbb{Z}_n := \{0,1,\dots,n-1\}$$

we denote the set of integers modulo[3] n. The finite field of prime order p, $\mathbb{F}_p$, can be constructed by taking as underlying set $\mathbb{Z}_p$ and define addition and multiplication as the usual integer addition and multiplication followed by reduction modulo p. This method works only if the order of the field is a prime number.

[2] Here we assume that the operation modulo p always yields a non-negative integer, i.e. something in the range $\{0,1,\dots,p-1\}$.
[3] Mathematicians typically prefer to define such an object as the quotient of $\mathbb{Z}$ by the ideal generated by n. Since we have not yet discussed ideals, let us stick to the simpler definition given here.

Exercise
Show that $\mathbb{Z}_4$ with addition and multiplication modulo 4 is not a finite field.

In general, the set $\mathbb{Z}_n$ with addition and multiplication as defined above has the structure of a commutative ring.

Polynomials over finite fields are somewhat peculiar. For example, let K be an infinite field. Given a multivariate polynomial $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$, then f vanishes at every point in K^n, i.e.

$$\forall\, (a_1, \dots, a_n) \in K^n \,:\, f(a_1, \dots, a_n) = 0$$

if and only if f is the zero polynomial. In other words, if a polynomial over an infinite field always yields zero when the variables are substituted by coefficients in the ground field, then this polynomial must be the zero polynomial. Over finite fields this is no longer true, i.e. there are polynomials different from the zero polynomial which vanish on all points over the ground field. An example for such a polynomial is given in the following exercise. But this is not enough: Given a finite field of some fixed (not necessarily prime) order, there is a simple way to construct a univariate polynomial which vanishes at all points of the ground field. You might want to look at the exercise section for this.

Exercise
Let $\mathbb{F}_2$ be the (previously defined) finite field of order 2. Show that the polynomial

$$f(x, y) = x^2 \cdot y + x \cdot y^2 \in \mathbb{F}_2[x, y]$$

vanishes at all points in $\mathbb{Z}_2^2$. Can you find a non-zero polynomial in $\mathbb{F}_2[x, y, z]$ which vanishes at all points in $\mathbb{Z}_2^3$ and involves all three variables?

1.2 Finite fields in general

In the previous section we have seen how to construct finite fields of prime order. It is only natural to ask[4] whether there are finite fields whose number of elements is not a prime number. The following theorem answers this question.

Theorem 1
Let F be a finite field. Then there exists a prime $p \in \mathbb{P}$ and a non-negative integer k such that the order of F is p^k. ∎

So there are no finite fields whose order is not a power of a prime. We might consider the construction for finite fields of order p^k for $k > 1$ later when we turn to ideals of a ring. If you can not wait until then, you should consult the appendix in the lecture notes for details.

One last thing which we want to define is the *characteristic* of a field. Although we won't need this for something other than fields, the notion is defined for the more general class of rings.

[4] Well, at least natural for a mathematician.

Definition 2 (Characteristic of a ring)
Let R be a ring. The characteristic *of R is the minimal number of times one has to add the multiplicative identity in order to get the additive identity. In other words, let $0/1$ be the additive/multiplicative identity of R, respectively. The characteristic of R is the smallest natural number c such that*

$$\underbrace{1 + 1 + \cdots + 1}_{c \text{ summands}} = 0.$$

If no such number exists, then the characteristic of R is defined to be zero. ∎

By this definition, the infinite fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ all have characteristic zero. Finite fields can not have zero characteristic, but are always of prime characteristic.

Exercise
Let F be a finite field.

1. *Show that the characteristic of F is positive.*
2. *Show that the characteristic of F is a prime number. Hint: If c is the characteristic of F and not a prime number, then there exist integers p, q such that $1 < p < c$ and $1 < q < c$ satisfying $c = p \cdot q$. Using distributivity of multiplication over addition we see that*

$$0 = \underbrace{1 + 1 + \cdots + 1}_{c \text{ summands}} = (\underbrace{1 + 1 + \cdots + 1}_{p \text{ summands}}) \cdot (\underbrace{1 + 1 + \cdots + 1}_{q \text{ summands}})$$

Using the fact that c is the minimal number such that a sum of this form yields zero and a property of fields discussed in the previous exercise sheet, you should be able to draw the conclusion.

2 Exercises

Exercise 1
We have seen in the lecture that arithmetic in finite fields can be very efficient due to a number of useful identities. Let us investigate an easy way to compute multiplicative inverses. Let F be a finite field of order q. Show that

$$\forall a \in F \setminus \{0\} : a^{-1} = a^{q-2}.$$

As usual, we assume that $a^0 = 1$. This requires $q - 3$ multiplications to compute the (multiplicative) inverse in a finite field of order at least three. Can you think of a simple trick to make this more efficient?

Exercise 2
Let p be a prime number. Consider the (commutative) ring $\mathbb{Z}_p$ of integers modulo p with the usual modular addition and multiplication.

1. *Given an argument why $\mathbb{Z}_p \setminus \{0\}$ is a group under multiplication, i.e. explain why every element has a multiplicative inverse in this set. This proves that $\mathbb{Z}_p$ is actually a field.*
2. *Show that for all $a \in \mathbb{Z}_p \setminus \{0\}$ the identity $a^{p-1} = 1$ holds.*
   Hint (requires a little group theory[5]): The use of Lagrange's theorem on the order of subgroups of a finite group is allowed.
3. *While the above identity holds only for non-zero elements, show that $b^p = b$ for all $b \in \mathbb{Z}_p$.*
4. *Construct a non-zero polynomial in $\mathbb{F}_p[x]$ which vanishes at all points in $\mathbb{Z}_p$.*

Exercise 3
Consider the finite field F of (not necessarily prime) order q. Show that the polynomial

$$x^q - x \in F[x]$$

vanishes at every element of F. This exercise verifies the statement at the end of section 1.1.

Exercise 4
Consider the polynomial

$$f(x) = x^4 + 1 \in \mathbb{F}_p[x],$$

where p is a prime number.

1. *How many factors[6] does $f(x)$ have in $\mathbb{F}_p[x]$?*
   Hint: You should consider the cases $p = 2, 8k + 1, 8k + 3, 8k + 5, 8k + 7$ separately.

[5] You should have had some group theory in one of your basic algebra classes. In particular, you should have heard about cyclic subgroups generated by an element of a group. If this does not ring a bell—even after consulting your favourite algebra textbook—you may skip this part of the exercise for now and go on to the second part.

[6] For example, the polynomial $x^2 + 1$ can be factored into $(x + 1)^2$ in $\mathbb{F}_2[x]$, hence has two factors. The same polynomial can not be factored in $\mathbb{F}_3[x]$. In that case, there is only one factor, namely the polynomial $x^2 + 1$ itself. As a last example, in $\mathbb{F}_5[x]$ we have a factorisation $x^2 + 1 = (x + 2) \cdot (x + 3)$ which has two distinct factors.

2. *Take your favourite CAS from the previous exercise sheet and find out how to factor polynomials over integers modulo a prime. Verify your result of the first part by factoring $f(x)$ for several primes p.*

Exercise 5

The construction in this exercise[7] *is a generalisation of the quotient field of an integral domain. Let R be a commutative ring (with unit) and $S \subseteq R$ a multiplicative monoid*[8] *(that means: $1 \in S$ and the product of elements coming from S lies in S). On the set $R \times S$ we define the relation*

$$(r_1, s_1) \sim (r_2, s_2) \iff \exists s_3 \in S \text{ such that } s_3 \cdot (s_2 \cdot r_1 - s_1 \cdot r_2) = 0.$$

1. *Verify that this is an equivalence relation.*
2. *Let $R[S^{-1}]$ denote the quotient $R \times S/\sim$ and write r/s for the equivalence class of the pair (r, s). Define addition and multiplication on $R[S^{-1}]$ by*

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{s_2 \cdot r_1 + s_1 \cdot r_2}{s_1 \cdot s_2} \qquad \text{and} \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 \cdot r_2}{s_1 \cdot s_2}.$$

   Verify that these are well defined operations turning $R[S^{-1}]$ into a commutative ring (with unit).
3. *Define the map*

$$\eta : R \to R[S^{-1}],\ r \mapsto \frac{r}{1}.$$

   Make sure that this is a well defined homomorphism of rings.
4. *Give a description of the kernel of the map η. Formulate conditions on the monoid S that warrant R being embedded in $R[S^{-1}]$. Is it possible that $R \cong R[S^{-1}]$?*

[7] This problem is slightly more challenging than the others. However, you should at least be able to solve the first half.

[8] Some authors also call this a multiplicatively closed set.