to be prepared for 27.10.2022

Exercise 11. For $m \in \mathbb{Z}$ let $\mathbb{Z}_m$ denote the group $\mathbb{Z}/m\mathbb{Z}$. Prove the following statement:

If $k, n \in \mathbb{Z}$ are relatively prime then $\mathbb{Z}_{kn} \cong \mathbb{Z}_k \oplus \mathbb{Z}_n$.

Exercise 12. Let R be a ring of prime characteristic p and $a, b \in R$. Prove:

$$\begin{aligned}(a+b)^p &= a^p + b^p \\ (a+b)^{p^n} &= a^{p^n} + b^{p^n}, \text{ for } n \in \mathbb{N}.\end{aligned}$$

Exercise 13. Let $p \in \mathbb{Z}$ be a prime. Implement an algorithm that inverts elements of the field $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle$.

Apply this algorithm to performing inversion in $\mathbb{F}_p[x]/\langle f \rangle$, where $f \in \mathbb{F}_p[x]$ is irreducible. You may use the mathematica notebook

$$http://www.risc.jku.at/education/courses/ws2022/CA/Examples.nb$$

Exercise 14. Let K denote a finite field. Let q be the order of K (i.e., K has q elements) and consider the polynomial $f = x^q - x \in K[x]$.

1. Prove that there is a unique prime $p \in \mathbb{N}$ such that $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle$ is a subfield of K. Conclude that $q = p^n$ for some $n \in \mathbb{N}$.
2. Show that the polynomial f has every element of K as a root.
3. Write down the factorization of f into irreducible factors.

Exercise 15. If K is an arbitrary field, a (univariate) polynomial function over K is a mapping $\varphi: K \to K$ that results from plugging in field elements into a fixed polynomial $f \in K[x]$, that is,

$$\exists_{f \in K[x]} \forall_{a \in K} \, \varphi(a) = f(a).$$

The set P_K of all polynomial functions $K \to K$ has the structure of an algebra over K. Describe this algebra in case that K is a finite field. How many elements has P_K?