Cryptography

Algebraic Structures

Prof. Dr. Heiko Knospe

TH Köln – University of Applied Sciences

April 29, 2024

Groups

Definition

A *group* G is a set together with a law of composition

$$\circ : G \times G \to G$$

such that the following properties are satisfied:

- For all $a, b, c \in G$ one has $(a \circ b) \circ c = a \circ (b \circ c)$ (*associative law*).
- There is an *identity* element $e \in G$ such that $e \circ g = g \circ e = g$ for all $g \in G$ (*identity element*).
- For every $g \in G$ there is an *inverse* element $x \in G$ with $g \circ x = x \circ g = e$ (*inverse element*).

The group is called *abelian* or *commutative* if for all $a, b \in G$, one has $a \circ b = b \circ a$ (*commutative law*).

Examples of Groups

- $(\mathbb{Z}, +)$ is an additive abelian group.
- $(\mathbb{R} \setminus \{0\}, \cdot)$ is a multiplicative abelian group.
- $(\mathbb{Z}_n, +)$ (residue classes modulo n) is an additive abelian group with n elements.
- $(\mathbb{Z}_n^*, \cdot)$ (units modulo n) is a multiplicative abelian group with $\varphi(n)$ elements and

$$\mathbb{Z}_n^* = \{x \bmod n \mid x \in \mathbb{Z} \text{ and } \gcd(x, n) = 1\}.$$

- Let p be a prime. Then $(\mathbb{Z}_p^*, \cdot)$ is a multiplicative abelian group containing the $p-1$ residue classes $1, 2, \ldots, p-1 \bmod p$.
- The permutations of $\{1, 2, \ldots, n\}$ (with composition of mappings) form a non-commutative group with $n!$ elements.

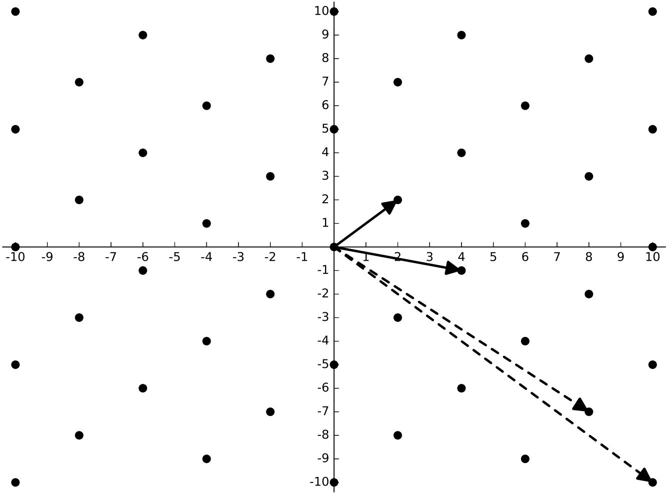
Higher-dimensional Examples

- Any vector space, e.g. $\mathbb{R}^n$, is a group with respect to addition of vectors.
- Let $q \in \mathbb{N}$ be a modulus. Then $\mathbb{Z}_q^n$ is group (with respect to addition of vectors) having q^n elements.
- $\mathbb{Z}^n$ is a group (a *lattice*) with respect to addition of vectors.
- General n-dimensional lattices L can be defined as follows: let $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$ be a set of linearly independent vectors, i.e., a basis. Then take all *integral* combinations of $v_1, v_2, \ldots, v_n$:

  $$L = \{v \in \mathbb{R}^n \mid v = x_1 v_1 + x_2 v_2 + \cdots + x_n v_n \text{ where } x_1, x_2, \ldots, x_n \in \mathbb{Z}\}$$

  The lattice L forms a group (with respect to addition of vectors). High-dimensional lattices are used in *post-quantum cryptography*. Many computations in lattices are efficient, but finding a short, non-zero vector in a random lattice is supposed to be a hard problem, even for quantum computers.

Example of a Lattice and two different Bases



Homomorphism and Isomorphism

Maps between groups should respect their group structure.

Definition

Let $f : G_1 \to G_2$ be a map between two groups G_1, G_2. Then f is called a *group homomorphism* if

$$f(g \circ g') = f(g) \circ f(g')$$

for all $g, g' \in G_1$. A bijective group homomorphism is called an *isomorphism*. If f is an isomorphism, then we say G_1 is *isomorphic* to G_2 and write $G_1 \cong G_2$.

Warning: A bijection between two groups does not necessarily imply that they are isomorphic! For example, there is a bijection between the additive groups $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$, but they are not isomorphic.

Examples of Homomorphisms and Isomorphisms

- The projection map $f : \mathbb{Z} \to \mathbb{Z}_n$, defined by $f(k) = k \bmod n$, is a surjective homomorphism.
- Let $G_1 = (\mathbb{Z}_4, +) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ be the additive group of integers modulo 4 and $G_2 = (\mathbb{Z}_5^*, \cdot) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ the multiplicative group of units modulo 5. The map $f : G_1 \to G_2$, defined by

  $$f(k \bmod 4) = 2^k \bmod 5,$$

  is a well defined homomorphism and bijective (why?). Therefore, f is an isomorphism and

  $$(\mathbb{Z}_4, +) \cong (\mathbb{Z}_5^*, \cdot).$$

Isomorphisms

The isomorphism $(\mathbb{Z}_4, +) \cong (\mathbb{Z}_5^*, \cdot)$ can be generalized to

$$(\mathbb{Z}_{p-1}, +) \cong (\mathbb{Z}_p^*, \cdot), \; f(k \bmod p-1) = g^k \bmod p$$

for a prime number p and a generator g of $\mathbb{Z}_p^*$ (see below). However, the inverse map is hard to compute (for large p): the exponent k is the *discrete logarithm* for which no efficient algorithm is known.

Therefore, the existence of an isomorphism $G_1 \cong G_2$ does not imply that switching between the groups G_1 and G_2 is easy.

Subgroups

Definition

Let G be a group. A *subgroup* H of G is a subset of G, which contains the identity element and is closed under the law of composition and inverse.

Example:
Let $G = (\mathbb{Z}_5^*, \cdot)$ and $H = \{\overline{1}, \overline{4}\}$. Since $4^2 \equiv 1 \bmod 5$, we see that H is a subgroup of G. However, $S = \{\overline{1}, \overline{2}\}$ is not a subgroup of G. (why?)

Subgroups generated by Elements

Each group element generates a subgroup:

Definition

Let G be a group and $g \in G$. The set $< g > = \{g^k \mid k \in \mathbb{Z}\}$ is called the *subgroup generated by g*. Here we used the multiplicative notation. For an additive group, we write $< g > = \{k \cdot g \mid k \in \mathbb{Z}\}$.

The subgroups $< g >$ are in fact *cyclic* groups (see below).

Example: Let $< \overline{4} >$ be the subgroup of the multiplicative group $G = \mathbb{Z}_5^*$ generated by 4 mod 5. Then $< \overline{4} > = \{\overline{1}, \overline{4}\}$, since $4^0 = 1$, $4^1 = 4$, $4^2 = 1 \bmod 5$, $4^3 = 4 \bmod 5$ etc. Furthermore, $4^{-1} = 4 \bmod 5$, $4^{-2} = 1 \bmod 5$, $4^{-3} = 4 \bmod 5$ etc.
However, similar computations show that $< \overline{2} >= \mathbb{Z}_5^*$.

Order of Groups and Subgroups

Definition (Order)

Let G be a group. The order of G, denoted by $\operatorname{ord}(G)$, is the number of elements of G (or infinity). Let $g \in G$. Then the order of the element g, denoted by $\operatorname{ord}(g)$, is the order of the subgroup generated by g, i.e., $\operatorname{ord}(g) = \operatorname{ord}(< g >)$.

Theorem (Lagrange)

Let G be a finite group and $H \subset G$ a subgroup. Then the order of H divides the order of G:

$$ord(H) \mid ord(G)$$

In particular, we have for every $g \in G$: $ord(g) \mid ord(G)$.

Example: If $\operatorname{ord}(G) = 26$, for example $G = (\mathbb{Z}_{26}, +)$ and $g \in G$, then $\operatorname{ord}(g) \in \{1, 2, 13, 26\}$. Can you give elements in $\mathbb{Z}_{26}$ of these orders?

Euler's Theorem

Theorem (Euler)

Let G be a finite group and $g \in G$, then

$$g^{ord(G)} = e.$$

This follows from $g^{\operatorname{ord}(g)} = e$ and $\operatorname{ord}(g) \mid \operatorname{ord}(G)$.

We apply Euler's Theorem to $G = \mathbb{Z}_n^*$. In this case, $\operatorname{ord}(G) = \varphi(n)$. For all $x \in \mathbb{Z}$ with $\gcd(x, n) = 1$, i.e., for $x \bmod n \in \mathbb{Z}_n^*$, we have:

$$x^{\varphi(n)} \equiv 1 \bmod n.$$

For a prime modulus p, it follows that

$$x^{p-1} \equiv 1 \bmod p \quad \text{and} \quad x^p \equiv x \bmod p.$$

Cyclic Groups

Definition

Let G be a group and $g \in G$. If $< g > = G$ then G is called a *cyclic group* and we say that g is a *generator* of G.

The elements of a cyclic group G with generator g are

$$G = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, g^3, \ldots\}.$$

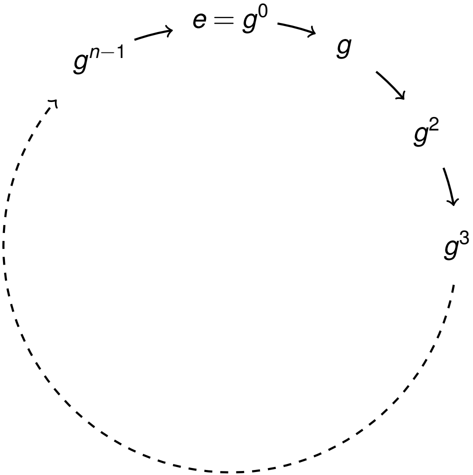
If $\operatorname{ord}(g) = n$ then $g^n = e$ and thus

$$G = \{e, g, g^2, g^3, \ldots, g^{n-1}\}.$$

The map $f : \mathbb{Z}_n \to G$, $f(k \bmod n) = g^k$, is an isomorphism and hence

$$G \cong \mathbb{Z}_n.$$

Illustration of Cyclic Groups



Generators of the Integers modulo n

Finding generators of the *additive* group $G = (\mathbb{Z}_n, +)$ is easy: G is cyclic of order n and 1 mod n is a generator. In general, an integer x is a generator modulo n if and only if $\gcd(x, n) = 1$.

For the *multiplicative* group $G = (\mathbb{Z}_n^*, \cdot)$, finding generators is more difficult. It depends on n whether G is cyclic or not. If a generator exists, then we call it a *primitive root* modulo n.

Example: $G = (\mathbb{Z}_5^*, \cdot)$ is cyclic of order 4 and $< 2 > = \mathbb{Z}_5^*$. Hence 2 mod 5 is a primitive root modulo 5.

Theorem

Let p be a prime; then $(\mathbb{Z}_p^*, \cdot)$ *is a cyclic group of order* $p - 1$*. The number of primitive roots is* $\varphi(p - 1)$*.*

Computing the Order and finding Generators

Let $g \in G$ and $n = \mathrm{ord}(G)$. How can we find $\mathrm{ord}(g)$ or verify if g is a generator of G ? Using the definition, i.e., computing all powers $g^0, g^1, g^2, \ldots, g^{n-1}$ is inefficient. However, we know that $\mathrm{ord}(g) \mid n$. Hence it is sufficient to compute g^a for the non-trivial divisors a of n. If $g^a = e$ then $\mathrm{ord}(g) \mid a$.

Furthermore, if $g^a \neq e$ for all $a \mid n$ and $a < n$, then g is a generator of G. In fact, it suffices to check the exponents $a = \frac{n}{p}$ for all prime factors p of n.

Example: Let $G = \mathbb{Z}_{53}^*$. Since 53 is a prime, G is a cyclic group of order 52. We want to check whether $g = 2 \bmod 53$ is a generator of G. The factorization $52 = 2^2 \cdot 13$ yields the prime factors 2 and 13. One computes $g^{52/13} = 2^4 = 16 \neq 1$ and $g^{52/2} = 2^{26} \equiv 52 \bmod 53 \neq 1$. Therefore, $g = 2 \bmod 53$ is a generator of G.

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Let $a, b \in \mathbb{N}$ be relatively prime, i.e. $\gcd(a, b) = 1$. Let $n = ab$, then the natural map $f : \mathbb{Z}_n \to \mathbb{Z}_a \times \mathbb{Z}_b$, $f(k \ mod\ n) = (k \ mod\ a,\ k \ mod\ b)$ is well defined and gives an isomorphism of additive groups and even rings:

$$\mathbb{Z}_n \cong \mathbb{Z}_a \times \mathbb{Z}_b$$

How is f^{-1} defined? Let $(k_1 \bmod a,\ k_2 \bmod b) \in \mathbb{Z}_a \times \mathbb{Z}_b$. We need to find $k \in \mathbb{Z}$ with $k \equiv k_1 \bmod a$ and $k \equiv k_2 \bmod b$. Since $\gcd(a, b) = 1$, the Extended Euclidean Algorithm gives $x, y \in \mathbb{Z}$ such that $ax + by = 1$. This implies $ax \equiv 1 \bmod b$ and $by \equiv 1 \bmod a$. Now set

$$k = k_1 by + k_2 ax.$$

Then $k \equiv k_1 by \equiv k_1 \bmod a$, and $k \equiv k_2 ax \equiv k_2 \bmod b$, as desired.

Chinese Remainder Theorem II

The Chinese Remainder Theorem (CRT) can be generalized to arbitrary finite abelian groups (and even to rings, see below).

Theorem (Fundamental Theorem of Abelian Groups)

Let G be a finite abelian group. Then G is isomorphic to a product of cyclic groups $\mathbb{Z}_{p^k}$ of prime-power order.

Examples:

1. An abelian group G of order 15 is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_5$.
2. For a group G of order 4, there are two (non-isomorphic) possibilities: $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Ring

Definition

A *ring* (or more precisely, a commutative ring with unity) is a set R with two operations (addition $+$ and multiplication $\cdot$) such that:

- $(R, +)$ is an abelian group. The identity element is denoted by 0.
- $(R, \cdot)$ satisfies the associative law, is commutative and has an identity element denoted by 1. The existence of an inverse element is not required.
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ for all $x, y, z \in R$ (distributivity).

Examples: $\mathbb{Z}$ and $\mathbb{Z}_n$ are rings with respect to addition and multiplication of integers and residue classes, respectively.

Ring Homomorphism

Ring homomorphisms are compatible with addition and multiplication.

Definition

Let $f : R_1 \to R_2$ be a map between the rings R_1 and R_2. Then f is called a *ring homomorphism* if

1. $f(x + y) = f(x) + f(y)$ for all $x, y \in R_1$, and
2. $f(x \cdot y) = f(x) \cdot f(y)$ for all $x, y \in R_1$, and
3. $f(1) = 1$.

A bijective ring homomorphism is called an *isomorphism*: $R_1 \cong R_2$.

Ring Isomorphism

Example: Let $p, q \in \mathbb{N}$ be different prime numbers and $n = pq$, then the Chinese Remainder Theorem gives a *ring isomorphism* f:

$$\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q, \; f(x \bmod n) = (x \bmod p, \; x \bmod q).$$

Hence f gives not only an isomorphism of additive groups, but also of multiplicative groups:

$$\mathbb{Z}_n^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

This can be leveraged for RSA decryption: the computations are done modulo p and q instead of modulo n. Since p and q are smaller, computations are more efficient. However, one has to apply f^{-1} at the end to obtain a result modulo n.

Units

Definition

Let R be a ring, then the subset of invertible elements with respect to multiplication is called the *units* of R and denoted by R^*. The units form an abelian group.

Examples:

$$\mathbb{Z}^* = \{1, -1\}$$

$$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$$

$$\mathbb{Z}_n^* = \{x \bmod n \mid x \in \mathbb{Z} \text{ and } \gcd(x, n) = 1\}$$

Field

Definition

A ring K is called a *field*, if $0 \neq 1$ and all nonzero elements are invertible, i.e., $K^* = K \setminus \{0\}$.

Examples: $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field.
$\mathbb{Z}_n$ is a field if and only if n is a prime.

Definition

Let p be a prime. Then the field $(\mathbb{Z}_p, +, \cdot)$ with p elements is called the Galois Field $GF(p)$.

Example: The smallest field is $GF(2)$.

Finite Fields

$GF(p)$ is a field of prime order. Can we construct finite fields of other orders?

Proposition

Let K be a finite field. Then $ord(K) = p^n$, where p is a prime number and $n \in \mathbb{N}$.

However, the obvious candidates are not necessarily fields. In fact, $\mathbb{Z}_{p^n}$ is a ring with p^n elements, but not a field if $n \geq 2$. Note that $p \bmod p^n$ is nonzero in $\mathbb{Z}_{p^n}$, but not invertible.

The construction of a field $GF(p^n)$ of order p^n is a bit more involved and requires polynomial rings.

Polynomial Rings

Definition

Let K be a field, then $K[x]$ is called the *ring of polynomials* over K. $K[x]$ contains all expressions

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $a_i \in K$ and $n \geq 0$ is an integer. The *degree* $\deg(f)$ of f is equal to n if $a_n \neq 0$. The degree of constant polynomials is 0. A polynomial is called *monic* if $a_n = 1$.

Polynomials can be added and multiplied in the obvious way.

Proposition

The polynomials $(K[x], +, \cdot)$ *over* K *form a ring.*

Division of Polynomials

Obviously, $K[x]$ *is not a field* since polynomials of degree ≥ 1 cannot be inverted multiplicatively. But we have a *division with remainder*. Let $f(x), g(x) \in K[x]$ with $g(x) \neq 0$. Then the division $f(x) : g(x)$ gives a quotient $q(x) \in K[x]$ and a remainder $r(x) \in K[x]$ such that

$$f(x) = q(x)g(x) + r(x) \text{ , where} \deg(r) < \deg(g).$$

Obviously, $g(x)$ divides $f(x)$ if and only if the remainder is 0.

Example: Let $f(x) = x^6 + x^5 + x^3 + x^2 + x + 1$ and $g(x) = x^4 + x^3 + 1$ be polynomials in $GF(2)[x]$. The quotient of $f(x) : g(x)$ is $q(x) = x^2$, the remainder is $r(x) = x^3 + x + 1$, and we have an equation

$$x^6 + x^5 + x^3 + x^2 + x + 1 = x^2(x^4 + x^3 + 1) + (x^3 + x + 1).$$

Residue Classes

We define *residue classes* of polynomials:

Definition

Let $g \in K[x]$ be a polynomial with $\deg(g) \geq 1$, then $g(x)$ defines an equivalence relation on $K[x]$:

$$f_1(x) \sim f_2(x) \text{ if } f_1(x) - f_2(x) = q(x)g(x) \text{ for some } q(x) \in K[x].$$

Equivalent polynomials f_1 and f_2 have the *same remainder* when divided by $g(x)$. We say they are *congruent modulo* $g(x)$ and write $f_1(x) \equiv f_2(x) \bmod g(x)$. The set of equivalence classes or *residue classes modulo* $g(x)$ is denoted by $K[x]/(g(x))$.

Example (see above):
$x^6 + x^5 + x^3 + x^2 + x + 1 \equiv x^3 + x + 1 \bmod (x^4 + x^3 + 1)$.

Quotient Ring

Proposition

Let $g \in K[x]$ and $n = \deg(g) \geq 1$, then $K[x]/(g(x))$ is again a ring called quotient ring, factor ring or residue class ring, with the operations induced by $K[x]$. Each residue class has a unique standard representative, a polynomial of degree less than n.

The ring structure can be easily verified. The standard representative can be found by division with remainder: let $f(x) \in K[x]$ be any representative of a residue class. We divide $f(x)$ by $g(x)$ and obtain polynomials $q(x)$, $r(x)$ with

$$f(x) = q(x)g(x) + r(x), \ \deg(r) < n.$$

This equation implies $f(x) \equiv r(x) \bmod g(x)$, and $r(x)$ is the standard representative of the class $f(x) \bmod g(x)$.

Polynomial Rings over $GF(p)$ and their Quotient Rings

Proposition

Let p be a prime and $g \in GF(p)[x]$ a polynomial of degree n. Then the quotient ring $GF(p)[x]/(g(x))$ has p^n elements.

In fact, the standard representatives of $GF(p)[x]/(g(x))$ are the polynomials

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}.$$

Since there are p possible elements for each coefficient a_i and n coefficients, there are p^n such polynomials.

Example

Polynomial rings and their quotient rings are often used in modern cryptography, e.g. for ring-based lattices.

Let $R = GF(17)[x]/(x^4 + 1)$. This ring has 17^4 elements which can be represented by polynomials of degree < 4 over $GF(17)$:

$$f(x) = a_0 + a_1 x + a_2 x + a_3 x^3 \text{ with } a_0, a_1, a_2, a_3 \in GF(17)$$

Hence elements in R can be identified with vectors in $GF(17)^4$. Addition is the obvious addition of residue classes modulo 17 in each coordinate.

However, multiplication is more complicated: polynomials have to be multiplied and the result is reduced modulo $x^4 + 1$, which means that x^4 is replaced by -1, x^5 by $-x$ and x^6 by $-x^2$.

Example (NTT)

The *Number Theoretic Transform* (NTT) can help to speed up the multiplication. For the above polynomial x^4+1 over $GF(17)$, one has the following factorization:

$$x^4+1=(x-2)\cdot(x-8)\cdot(x-9)\cdot(x-15)$$

In other words, the residue classes $2,8,9,15$ mod 17 are roots (zeros) of the polynomial x^4+1 (and they are in fact 8-th root of unity) over $GF(17)$. The Chinese Remainder Theorem yields a ring isomorphism

$$\begin{aligned} NTT: GF(17)[x]/(x^4+1) &\cong \\ & GF(17)[x]/(x-2)\times GF(17)[x]/(x-8)\times GF(17)[x]/(x-9)\times GF(17)[x]/(x-15)\cong \\ & GF(17)^4 \end{aligned}$$

The NTT maps a polynomial $f(x)$ mod (x^4+1) to the vector $(f(2),f(8),f(9),f(15))\in GF(17)^4$. After applying the NTT, multiplication is component-wise and hence more efficient.

Example (Inverse NTT)

How can we find the inverse NTT map?

$$NTT^{-1}: \ GF(17)^4 \longrightarrow GF(17)[x]/(x^4+1)$$

NTT^{-1} maps a vector $(y_0, y_1, y_2, y_3) \in GF(17)^4$ to a polynomial $f(x)$ of degree < 4 such that

$$(f(2), f(8), f(9), f(15)) = (y_0, y_1, y_2, y_3) \in GF(17)^4$$

The polynomial f is given by interpolation and there are explicit formulas (e.g., Lagrange interpolation).

Irreducible Polynomials

Now we want to construct a *field* with p^n elements. To this end, we use *irreducible* polynomials of degree n over $GF(p)$.

Definition

A polynomial $g(x) \in K[x]$ is called *irreducible*, if it cannot be factored into two polynomials of smaller degree. Otherwise, the polynomial is called *reducible*.

Irreducible polynomials can be seen as the *prime elements* in the polynomial ring.

Example: We have seen above that $x^4 + 1$ is reducible in $GF(17)[x]$.

Properties and Examples of Irreducible Polynomials

Irreducible polynomials in $K[x]$ do not possess any zeros $a \in K$, since otherwise a linear factor $(x - a)$ can be split off. However, there are reducible polynomials (of degree ≥ 4) without zeros!

Example: $g(x) = x^4 + x^2 + 1$ has no zeros over $GF(2)$, but $g(x) = (x^2 + x + 1)^2$ in $GF(2)[x]$. Hence $g(x)$ is reducible.

Degree	Irreducible Polynomials over $GF(2)$
2	$x^2 + x + 1$
3	$x^3 + x + 1,\ x^3 + x^2 + 1$
4	$x^4 + x + 1,\ x^4 + x^3 + x^2 + x + 1,$ $x^4 + x^3 + 1$
5	$x^5 + x^2 + 1,\ x^5 + x^3 + x^2 + x + 1,$ $x^5 + x^3 + 1,\ x^5 + x^4 + x^3 + x + 1,$ $x^5 + x^4 + x^3 + x^2 + 1,\ x^5 + x^4 + x^2 + x + 1$

Euclidean Algorithm for Polynomials

Definition

Let $f(x), g(x) \in K[x]$ be nonzero polynomials, then the *greatest common divisor* $gcd(f,g)$ is the monic polynomial of highest possible degree that divides $f(x)$ and $g(x)$.

The greatest common divisor (gcd) of two polynomials can be efficiently computed using the *Extended Euclidean Algorithm*. The algorithm takes two polynomials f and g as input and outputs $gcd(f,g)$ along with two polynomials $a(x)$ and $b(x)$ such that

$$gcd(f,g) = a(x)f(x) + b(x)g(x).$$

Construction of Field Extensions

Proposition

Let $g(x) \in K[x]$ be an irreducible polynomial. Then the quotient ring $K[x]/(g(x))$ is an extension field of K.

Why is this true? Obviously, $K[x]$ is not a field. However, we can use the *Extended Euclidean Algorithm for polynomials* to invert a polynomial f modulo g. Since g is irreducible, we have $gcd(f, g) = 1$ (unless f is zero or a multiple of g). The algorithm outputs polynomials $a(x)$ and $b(x)$ such that

$$1 = a(x)f(x) + b(x)g(x) \implies 1 \equiv a(x)f(x) \bmod g(x).$$

Hence $f(x)$ is invertible modulo $g(x)$ and the inverse is $a(x) \bmod g(x)$.

Construction of $GF(p^n)$

The field $GF(p^n)$ can be defined using an irreducible polynomial over $GF(p)$ of degree n:

Definition

Let $g(x) \in GF(p)[x]$ be an *irreducible polynomial* of degree n, then the residue field $GF(p)[x]/(g(x))$ defines the *Galois Field* $GF(p^n)$ which extends the field $GF(p)$.

In most cases, there is more than one irreducible polynomial of degree n. Therefore, there are several definitions of $GF(p^n)$, but one can show that the resulting fields with p^n elements are isomorphic. However, the multiplication in terms of coefficients depends on the polynomial.

Example: $GF(4)$

The polynomial $g(x) = x^2 + x + 1 \in GF(2)[x]$ has no zeros and is irreducible, and so $GF(2)[x]/(x^2 + x + 1) \cong GF(4)$.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0
$\cdot$				
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Addition and multiplication table for $GF(4)$.

The Field $GF(256)$

Let $g(x) = x^8 + x^4 + x^3 + x + 1 \in GF(2)[x]$. One can show that $g(x)$ is irreducible. Hence $GF(2)[x]/(x^8 + x^4 + x^3 + x + 1) \cong GF(256)$ defines a field of order 256.

This field is used in the block cipher AES. The elements in $GF(2^8)$ are given by polynomials of degree less than 8, which in turn correspond to 8-bit words. The first bit (most significant bit, MSB) corresponds to the coefficient of x^7, the second bit to x^6 etc., and the last bit (least significant bit, LSB) to $x^0 = 1$, i.e., the byte $b_7 b_6 \dots b_1 b_0$ corresponds to the polynomial $b_7 x^7 + b_6 x^6 + \dots + b_1 x + b_0 \in GF(2)[x]$.

Addition in $GF(2^8)$ corresponds to the XOR operation on 8-bit words. Multiplication is given by a multiplication of polynomials, followed by a reduction modulo $g(x)$.

Computations in $GF(256)$

Let $g(x) = x^8 + x^4 + x^3 + x + 1 \in GF(2)[x]$. Suppose we want to multiply x^7 and $(x+1)$ mod $g(x)$:

$$x^7 \cdot (x+1) = x^8 + x^7 \bmod g(x) \equiv x^7 + x^4 + x^3 + x + 1.$$

In hexadecimal notation, this can be written as $\texttt{80} \cdot \texttt{03} = \texttt{9B}$.

```
sage:   R.<x> = PolynomialRing(GF(2),x)
sage:   g=x^8+x^4+x^3+x+1
sage:   K.<a>=R.quotient_ring(g)
sage:   a^7 * (a+1)
a^7 + a^4 + a^3 + a + 1
```

Now we compute the inverse of $x+1$ mod $g(x)$:

```
sage:   1/(a+1)
a^7 + a^6 + a^5 + a^4 + a^2 + a
```

In fact, $(x+1)(x^7 + x^6 + x^5 + x^4 + x^2 + x) \equiv 1 \bmod g(x)$, and so we obtain $\texttt{03}^{-1} = \texttt{F6}$.