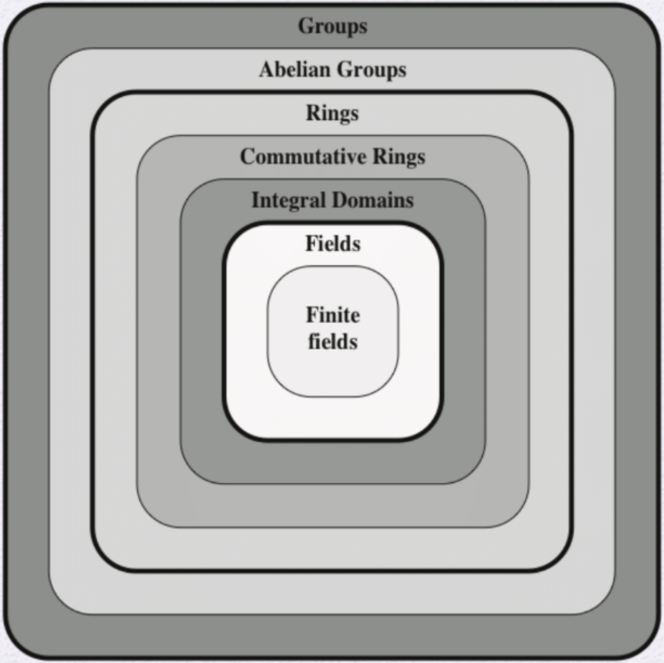
Introduction to Cryptography
Lecture 10

Monika K. Polak

March 2, 2021


Groups
Abelian Groups
Rings
Commutative Rings
Integral Domains
Fields
Finite fields

Types of fields

Group

Abelian group

Ring

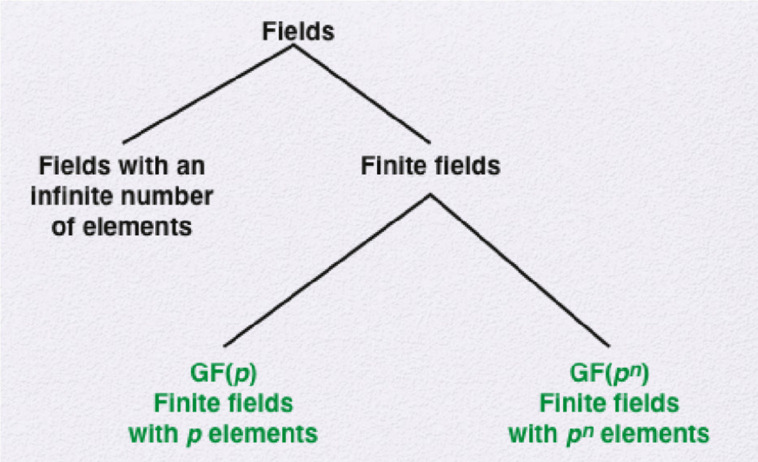
Commutative ring

Integral domain

Field

(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and a 0, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Types of fields



Finite Fields of the Form $GF(p^m)$

Galois' Theorem

An order-n finite field exists if and only if $n = p^m$ for some prime p and some positive integer m.

- p is called the characteristic of this finite field
- The order of an finite field is its number of elements
- We usually use $GF(p^m)$ or $\mathbb{F}_{p^m}$ to represent the finite field of order p^m
- An order-n finite field is unique (up to isomorphism)
- Addition and multiplication modulo a prime number p form a finite field ($\mathbb{Z}_p = GF(p)$)

Finite Fields of the Form $GF(p^m)$

- If $m = 1$ then $\mathbb{Z}_p = GF(p)$
- One way to construct a finite field with $m > 1$ is using the polynomial basis. The field is constructed as a set of p^m polynomials along with two polynomial operations

Remark

Example. Consider $2^3 = 8$. We know $(\mathbb{Z}_8, +, \cdot)$ is not a field

Polynomial Arithmetic

- A polynomial $f(x)$ is a mathematical expression in the form $a_n x^n + a_{n-1} x^{n-1} + ... + a_0$
- The highest exponent of x is the degree of the polynomial
- $a_n, a_{n-1}, ..., a_0$ are called coefficients

Polynomial Arithmetic

We can:

- add polynomials
- subtract polynomials
- multiply polynomials
- divide polynomials

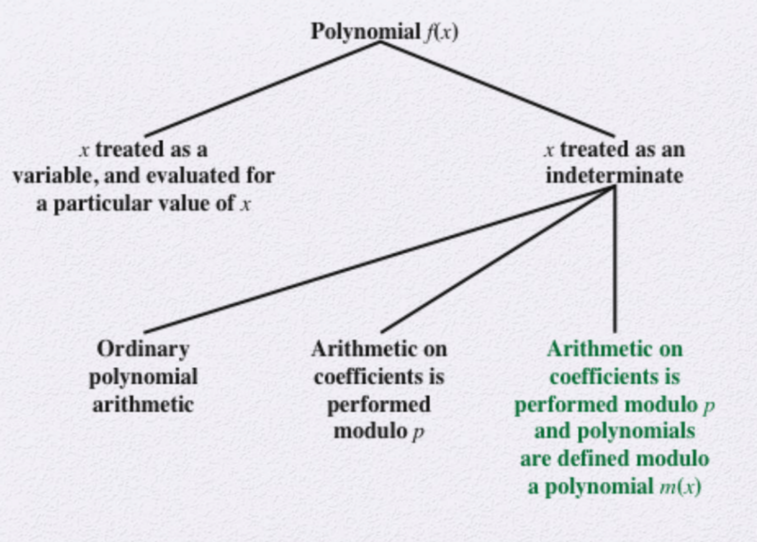
`Examples on whiteboard`

Polynomial Arithmetic over field

If the coefficients are taken from a field F, then we say it is a polynomial over F. With polynomials over field $GF(p)$, you can add and multiply polynomials just like you have always done but the coefficients need to be reduced modulo p.

`Examples on whiteboard`

Treatment of polynomials



Finite Fields of the form $GF(p^m)$

Irreducible polynomial

If a polynomial is divisible only by itself and constants, then we call this polynomial an irreducible polynomial

Polynomial GCD

$gcd[a(x), b(x)]$ is the polynomial of maximum degree that divides both $a(x)$ and $b(x)$

Similar to integers, you can do modular arithmetic with polynomials over a field. Now the operands and modulus are polynomials.
Always remember there are two moduli involved: a polynomial modulus and an integer modulus.

Finite Fields of the form $GF(p^m)$

Irreducible polynomial

If the modulus $g(x)$ is an irreducible polynomial of degree m over $GF(p)$, then the finite field $GF(p^m)$ can be constructed by the set of polynomials over $GF(p)$ whose degree is at most $m-1$, where addition and multiplication are done modulo $g(x)$.

`Examples on whiteboard`

Polynomial Arithmetic Modulo $(x^3 + x + 1)$

	+	000	001	010	011	100	101	110	111
		0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

	×	000	001	010	011	100	101	110	111
		0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

Thanks for Your attention.