Lecture 03: Groups and Fields

Supplementary reading and cryptographic context

The puzzle: does one point reach them all?

Observed calculation

Work modulo 17. Let S contain the pairs satisfying

$$y^2 \equiv x^3 + 1 \pmod{17},$$

together with one extra symbol $\mathcal{O}$. Starting from $P = (2, 3)$, a rule defined later gives the table on the right.

step k	point reached
0	$\mathcal{O}$
1	$(2, 3)$
2	$(0, 1)$
3	$(16, 0)$
4	$(0, 16)$
5	$(2, 14)$
6	$\mathcal{O}$

Guiding question

There are eighteen points in S. Why does the sequence return to $\mathcal{O}$ after six steps?

We will return after defining the operation and what it means for one element to reach the others.

Roadmap

By the end of this supplement, we will be able to

1. restate the group and field axioms in a dependency-conscious order;
2. move from powers to generators and then to efficient exponentiation;
3. distinguish nonzero residues from invertible residues modulo a composite;
4. introduce optional vocabulary: subgroups, element order, and primitive roots;
5. locate groups and fields inside several cryptographic constructions; and
6. enumerate a small elliptic curve and compute a proper subgroup explicitly.

Recommended reading: [HPS14, Secs. 2.5 and 1.5].

How to use this supplement

Core recap and clarification

- The distributed 14-slide Lecture 03 deck remains the required minimum.
- The first part revisits that material, fills in short arguments, and clarifies notation.
- Definitions appear before substantive use.

Additional reading

- The second part adds optional vocabulary and broader cryptographic context.
- Application slides are previews, not substitutes for later lectures on the complete constructions.
- Any unavoidable preview is explicitly signposted.

Read Hoffstein–Pipher–Silverman Section 2.5 before Section 1.5, so the group vocabulary is available first.

Groups: one operation with inverses

A **binary operation** on a set G is a rule

$$\circ : G \times G \longrightarrow G$$

that combines two elements of G and returns another element of G.

Definition

A **group** is a pair $(G, \circ)$ satisfying:

1. **Associativity:** $(a \circ b) \circ c = a \circ (b \circ c)$.
2. **Identity:** some $e \in G$ satisfies $e \circ a = a = a \circ e$.
3. **Inverse:** every $a \in G$ has $a^{-1} \in G$ with $a^{-1} \circ a = e = a \circ a^{-1}$.

Closure is already encoded by the displayed map $G \times G \to G$.

If $a \circ b = b \circ a$ for every $a, b \in G$, the group is **commutative**, or **abelian**. [HPS14, §2.5]

Two notational languages for the same axioms

Multiplicative notation

operation: ab or $a \circ b$
identity: e or 1
inverse: a^{-1}

Additive notation

operation: $a + b$
identity: 0
inverse: $-a$

Immediate consequences of the axioms

- The identity element is unique.
- The inverse of each element is unique.
- **Cancellation:** $ab = ac$ implies $b = c$, and $ba = ca$ implies $b = c$.

For example, left-multiplying $ab = ac$ by a^{-1} gives $(a^{-1}a)b = (a^{-1}a)c$, hence $b = c$.

A quick check: bitstrings under $\oplus$

$(\{0,1\}^n, \oplus)$

- The bit operation **exclusive OR** (XOR), written $\oplus$, is applied coordinatewise.
- Closure and associativity hold coordinatewise.
- Identity: $0^n = 00\cdots0$.
- Every bitstring is its own inverse: $x \oplus x = 0^n$.
- XOR is commutative.

Example

$$\begin{array}{r} 10110 \\ \oplus\ 01101 \\ \hline 11011 \end{array}$$

This is the algebra used by the classical one-time pad and by many bit-mask operations.

The group one-time pad in three lines

1. Key generation

$$\mathsf{sk} \xleftarrow{\$} G.$$

Choose sk uniformly from G; each element has probability $1/|G|$.

2. Encryption

$$c = \mathsf{Enc}_{\mathsf{sk}}(m) := m \circ \mathsf{sk}.$$

Alice publishes c.

3. Decryption

$$m' = \mathsf{Dec}_{\mathsf{sk}}(c) := c \circ \mathsf{sk}^{-1}.$$

Bob uses the shared key to recover m.

Assumptions used later for privacy

The key is hidden, uniform over all of G (including the identity), and used for only one message. The message, key, and ciphertext all lie in G.

Correctness is an algebraic identity

Definition in this course

Correctness means that decrypting an encryption returns the original message:

$$\mathrm{Dec}_{\mathsf{sk}}(\mathrm{Enc}_{\mathsf{sk}}(m)) = m \qquad \text{for every } m, \mathsf{sk} \in G.$$

$$\begin{aligned} \mathrm{Dec}_{\mathsf{sk}}(\mathrm{Enc}_{\mathsf{sk}}(m)) &= (m \circ \mathsf{sk}) \circ \mathsf{sk}^{-1} \\ &= m \circ (\mathsf{sk} \circ \mathsf{sk}^{-1}) && \text{associativity} \\ &= m \circ e = m. && \text{inverse and identity} \end{aligned}$$

Independent check. Commutativity was not used; the order of factors must remain exactly as written.

Finite and infinite examples

Infinite example

$(\mathbb{Z}, +)$ is a group:

- identity: 0;
- inverse of a: $-a$;
- addition is associative and closed.

Finite example

$(\mathbb{Z}_n, +)$ is a group, where

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

and addition is reduced modulo n.

The same set may participate in different structures depending on which operation is chosen. Always specify both the set and the operation.

Nonexamples: locate the failed axiom

Structure	Verdict	Reason
$(\mathbb{Z}, \times)$	not a group	0 has no inverse, and $2^{-1} \notin \mathbb{Z}$.
$(\mathbb{Z} \setminus \{0\}, \times)$	not a group	$2^{-1} = 1/2$ leaves the set.
$(\mathbb{Q}, \times)$	not a group	0 has no multiplicative inverse.
$(\mathbb{Q} \setminus \{0\}, \times)$	group	every nonzero a/b has inverse b/a.

Diagnostic strategy

First identify the proposed identity. Then ask whether every element can be undone without leaving the set.

Multiplication modulo n: nonzero does not mean invertible

Why all nonzero residues may fail

For composite n, multiplying two nonzero residues can produce 0 modulo n. For example,

$$2 \cdot 3 \equiv 0 \pmod{6}.$$

Thus $\{1, 2, 3, 4, 5\}$ is not closed under multiplication modulo 6.

A residue $[a] \in \mathbb{Z}_n$ is called a **unit** if it has a multiplicative inverse modulo n. The set of all units is

$$\mathbb{Z}_n^\times := \{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}.$$

It is a group under multiplication modulo n.

When p is prime, every nonzero residue is a unit, so $\mathbb{Z}_p^\times = \{1, \ldots, p-1\}$.

Groups need not be commutative

Consider the group of invertible 2×2 rational matrices under matrix multiplication. Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \qquad BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \qquad AB \neq BA.$$

Lesson

Associativity is required; commutativity is optional. In a noncommutative group, the order of factors and inverses matters.

Powers: repeated use of one element

For $g \in G$, repeated application of the group operation is written as a power:

$$g^0 = e, \qquad g^k = \underbrace{g \circ \cdots \circ g}_{k \text{ copies}} \quad (k > 0), \qquad g^{-k} = (g^{-1})^k.$$

Associativity gives the familiar exponent laws

$$g^a \circ g^b = g^{a+b}, \qquad (g^a)^b = g^{ab}.$$

In additive notation, g^k is written kg; thus $0g = 0$ and $(-k)g = -(kg)$.

Powers in groups: [HPS14, §2.5]

Generators: can one element reach the whole group?

For $g \in G$, consider all integer powers of g:

$$\{g^k : k \in \mathbb{Z}\}.$$

Definition

If every element of G is equal to g^k for some integer k, then g is a **generator** of G. A group having a generator is called **cyclic**.

In additive notation, the same condition reads

$$G = \{kg : k \in \mathbb{Z}\}.$$

Important

A group may have several generators, and many of its elements may fail to generate the whole group.

Example: 2 generates $(\mathbb{Z}_5, +)$

k	0	1	2	3	4	5
$k \cdot 2 \pmod 5$	0	2	4	1	3	0

What happened?

Before returning to 0, the sequence visited every element of $\mathbb{Z}_5$. Hence 2 is a generator of $(\mathbb{Z}_5, +)$.

The same calculation shows that $1, 2, 3$, and 4 all generate $(\mathbb{Z}_5, +)$.

Example: generators of $\mathbb{Z}_7^\times$

The unit group $\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\}$ uses multiplication modulo 7.

a	powers until the first return to 1
2	$1, 2, 4, 1$
3	$1, 3, 2, 6, 4, 5, 1$
4	$1, 4, 2, 1$
5	$1, 5, 4, 6, 2, 3, 1$
6	$1, 6, 1$

Conclusion

The elements

$$3 \quad \text{and} \quad 5$$

visit all six units, so they generate $\mathbb{Z}_7^\times$.

Powers and generators modulo a prime: [HPS14, §1.5]

Repeated squaring: read the exponent in binary

Write the exponent i in binary:

$$i = b_0 + 2b_1 + 4b_2 + \cdots + 2^k b_k, \qquad b_j \in \{0, 1\}.$$

First compute

$$g,\ g^2,\ g^4,\ g^8, \ldots,\ g^{2^k}$$

using one squaring at each step. Then combine exactly those powers for which $b_j = 1$:

$$g^i = \prod_{j : b_j = 1} g^{2^j}.$$

Important clarification

The element g need not generate the entire group. Repeated squaring computes g^i for every element g in every group.

Square-and-multiply: maintain one invariant

Right-to-left binary method

Input: group element g and integer $i \geq 0$

1. $r \leftarrow e$, $b \leftarrow g$, $n \leftarrow i$
2. while $n > 0$ do
   - if n is odd, set $r \leftarrow r \circ b$
   - set $b \leftarrow b \circ b$
   - set $n \leftarrow \lfloor n/2 \rfloor$
3. return r

A **loop invariant** is a statement that remains true after every iteration. Here the invariant is

$$r \circ b^n = g^i.$$

When the loop ends, $n = 0$, so the invariant gives $r = g^i$.

Worked example: $3^{13} \bmod 17$

Since $13 = (1101)_2 = 8 + 4 + 1$, compute successive squares:

power	value modulo 17
3^1	3
3^2	9
3^4	$9^2 = 81 \equiv 13$
3^8	$13^2 = 169 \equiv 16$

Therefore

$$3^{13} = 3^8 \cdot 3^4 \cdot 3 \equiv 16 \cdot 13 \cdot 3 \equiv 12 \pmod{17}.$$

Independent check: $3^{13} = 1{,}594{,}323$, and division by 17 leaves remainder 12.

Why repeated squaring is efficient

Let

$$\ell = \lfloor \log_2 i \rfloor + 1$$

be the number of bits needed to write i.

Naive repetition

Computing g^i directly uses about i group operations. Since i may be close to 2^ℓ, this is exponential in the input length ℓ.

Repeated squaring

At most about 2ℓ group operations suffice. Thus the number of group operations is linear in the bit length of the exponent.

This distinction—time measured against the number itself versus the number of bits describing it—is fundamental in cryptography.

Definition

A **field** $(F, +, \cdot)$ is a set with two operations such that:

1. $(F, +)$ is an abelian group with identity 0;
2. $(F \setminus \{0\}, \cdot)$ is an abelian group with identity 1;
3. multiplication distributes over addition:

$$a(b + c) = ab + ac.$$

What this guarantees

One may add, subtract, multiply, and divide by every nonzero element without leaving the set.

This is the seven-property checklist in the core lecture rewritten in group language.

Fields and nonfields

Fields

- $\mathbb{Q}$ with ordinary addition and multiplication.
- $\mathbb{R}$ with ordinary addition and multiplication.
- $\mathbb{Z}_p$ with modular operations when p is prime.

Not fields

- $\mathbb{Z}$: the nonzero element 2 has no inverse in $\mathbb{Z}$.
- $\mathbb{Z}_6$: the nonzero elements 2 and 3 satisfy

$$2 \cdot 3 = 0.$$

Hence neither can have an inverse.

A field with finitely many elements is called a **finite field**.

The prime field $\mathbb{F}_p$

When p is prime, we write

$$\mathbb{F}_p := \mathbb{Z}_p$$

when emphasizing that addition and multiplication modulo p form a field. Every nonzero $a \in \mathbb{F}_p$ has an inverse because $\gcd(a, p) = 1$.

Example in $\mathbb{F}_{17}$

$$5^{-1} = 7,$$

because

$$5 \cdot 7 = 35 \equiv 1 \pmod{17}.$$

Connection to the earlier group

The nonzero elements form the multiplicative group

$$\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\} = \mathbb{Z}_p^\times.$$

Finite fields have prime-power size

Finite-field size theorem

Every finite field has

$$p^m$$

elements for some prime p and some integer $m \geq 1$. A number of the form p^m is called a **prime power**.

The case $m = 1$ is the prime field $\mathbb{F}_p$. Fields with $p^2, p^3, \ldots$ elements also exist, but their construction requires polynomial arithmetic.

Signpost

The construction of these larger finite fields is not part of the minimum core deck. It appears in Part II as optional additional reading.

Core takeaways

1. **Group:** a set together with one associative operation, an identity, and inverses.
2. **Notation:** always specify both the set and the operation; the same set can support different structures.
3. **Powers and generators:** powers record repeated use of one element; a generator reaches the whole group.
4. **Repeated squaring:** binary expansion computes g^i using $O(\log i)$ group operations.
5. **Field:** addition and nonzero multiplication are compatible abelian group operations.
6. **Finite fields:** their sizes are prime powers; $\mathbb{F}_p$ is the first example.

The central algebraic habit

State the set and operation first; then identify the identity, compute inverses, and only afterward ask about powers, generators, or algorithms.

From the core material to additional reading

New algebraic vocabulary

- privacy of the group one-time pad;
- subgroups and element order;
- Lagrange's theorem and primitive roots;
- finite fields beyond prime size.

Broader cryptographic context

- additive sharing, RSA, and Diffie–Hellman;
- elliptic-curve groups;
- AES, GCM, and Shamir sharing;
- permutation and direct-product groups.

Everything from this point onward is supplementary to the minimum Lecture 03 deck.

Definition in this setting

Privacy means that every message induces the same ciphertext distribution; equivalently, the ciphertext reveals no additional information about the message.

Fix $m, c \in G$. There is exactly one key mapping m to c:

$$m \circ \mathsf{sk} = c \quad \Longleftrightarrow \quad \mathsf{sk} = m^{-1} \circ c.$$

Because the key is uniform,

$$\Pr[C = c \mid M = m] = \frac{1}{|G|},$$

which does not depend on m.

Conclusion. The scheme is private; together with correctness, it is secure in this course terminology.

Perfect-secrecy viewpoint: [Sha49]

Should the identity key be excluded?

The key value $\mathsf{sk} = e$ produces $c = m \circ e = m$. This is not a privacy defect when the key is sampled from all of G.

With every key allowed

For all $m, c \in G$,

$$\Pr[C = c \mid M = m] = \frac{1}{|G|}.$$

If e is removed

For the ciphertext $c = m$,

$$\Pr[C = m \mid M = m] = 0,$$

but for $m' \neq m$,

$$\Pr[C = m \mid M = m'] = \frac{1}{|G| - 1}.$$

Removing e makes the ciphertext probabilities depend on the message and therefore destroys privacy.

Why the key must be one-time

Suppose the same key is used twice:

$$c_1 = m_1 \circ \mathsf{sk}, \qquad c_2 = m_2 \circ \mathsf{sk}.$$

An observer can eliminate the key:

$$\begin{aligned} c_1 \circ c_2^{-1} &= m_1 \circ \mathsf{sk} \circ (m_2 \circ \mathsf{sk})^{-1} \\ &= m_1 \circ \mathsf{sk} \circ \mathsf{sk}^{-1} \circ m_2^{-1} \\ &= m_1 \circ m_2^{-1}. \end{aligned}$$

Additive notation

For XOR or modular addition, this relation becomes

$$c_1 - c_2 = m_1 - m_2.$$

Thus key reuse reveals a relation between the messages.

Subgroup

A subset $H \subseteq G$ is a **subgroup** if it is itself a group under the same operation. We write $H \leq G$.

Element order

For finite G, the **order of** g, written $\mathrm{ord}(g)$, is the least positive r such that

$$g^r = e.$$

The powers of g form the **cyclic subgroup generated by** g:

$$\langle g \rangle := \{g^k : k \in \mathbb{Z}\}.$$

It has exactly $\mathrm{ord}(g)$ elements.

A generator of all of G is precisely an element g for which $\langle g \rangle = G$.

Lagrange's theorem: subgroup size divides group size

Lagrange's theorem

If H is a subgroup of a finite group G, then the number of elements in H divides the number of elements in G.

For $H = \langle g \rangle$, the subgroup has $\operatorname{ord}(g)$ elements. Therefore:

$$\text{the order of } g \text{ divides the size of } G, \qquad g^{|G|} = e.$$

For a prime field

The group $\mathbb{F}_p^\times$ has $p - 1$ elements. Hence every nonzero $a \in \mathbb{F}_p$ satisfies

$$a^{p-1} = 1.$$

[HPS14, §2.5]

Definition

A **primitive root modulo a prime** p is a generator of the multiplicative group $\mathbb{F}_p^\times$. Equivalently, it is an element whose powers visit all $p-1$ nonzero residues.

For $p = 7$, the earlier computation showed that 3 and 5 are primitive roots:

$$\langle 3 \rangle = \mathbb{F}_7^\times, \qquad \langle 5 \rangle = \mathbb{F}_7^\times.$$

Structural fact

The multiplicative group of every finite field is cyclic. In particular, primitive roots exist modulo every prime.

Powers and primitive roots: [HPS14, §1.5]

Finite fields beyond prime size

Let $f(x)$ be a polynomial of degree m with coefficients in $\mathbb{F}_p$. It is **irreducible** if it cannot be factored into two positive-degree polynomials over $\mathbb{F}_p$.

Construction

Using an irreducible f, one obtains a field with p^m elements, written

$$\mathbb{F}_p[x]/(f(x)).$$

The notation means that polynomial expressions are reduced using the rule $f(x) = 0$.

Every element has a representative

$$a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}, \qquad a_i \in \mathbb{F}_p.$$

Addition is coefficientwise; multiplication is followed by reduction using $f(x) = 0$.

Finite-field constructions: see [HPS14, Ch. 2]

Worked example: $\mathbb{F}_{2^3}$

Use $f(x) = x^3 + x + 1$ over $\mathbb{F}_2$ and impose $f(x) = 0$. Let α be the element represented by x. Then

$$\alpha^3 = \alpha + 1.$$

Every field element is

$$a_0 + a_1\alpha + a_2\alpha^2, \qquad a_i \in \mathbb{F}_2.$$

Addition

$$(\alpha^2 + 1) + (\alpha + 1) = \alpha^2 + \alpha.$$

Coefficients add by XOR.

Multiplication

$$(\alpha^2 + 1)\alpha = \alpha^3 + \alpha = 1.$$

Thus $\alpha = (\alpha^2 + 1)^{-1}$.

Additive secret sharing

Let $(G, +)$ be a finite abelian group and let the secret be $s \in G$. To form a k-out-of-k additive sharing—one in which all k shares are required—do the following:

1. sample $s_1, \ldots, s_{k-1}$ independently and uniformly from G;
2. set

$$s_k = s - (s_1 + \cdots + s_{k-1}).$$

Correctness

Adding all shares gives

$$s_1 + \cdots + s_k = s.$$

Privacy

Any fixed collection of $k - 1$ shares is uniformly distributed independently of s; the missing share absorbs the dependence on the secret.

RSA: exponentiation in the unit group

The Rivest–Shamir–Adleman (RSA) system uses exponentiation modulo $N = pq$, where p and q are distinct primes. Its clean group-theoretic core is

$$\mathbb{Z}_N^\times = \{[a] \in \mathbb{Z}_N : \gcd(a, N) = 1\}.$$

Example: $N = 15$

$$\mathbb{Z}_{15}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Every listed residue has a multiplicative inverse modulo 15.

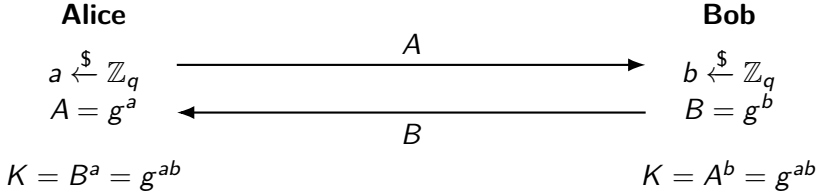
Why today's material matters

RSA encryption and decryption are exponentiation maps. Inverses and repeated squaring explain the algebra and efficient computation; full RSA correctness appears later.

RSA: [RSA78]; textbook treatment: [HPS14, Ch. 3]

Diffie–Hellman: powers are easy, exponents are hidden

Let $G = \langle g \rangle$ be a cyclic group having a large prime number q of elements.



The inverse problem

The **discrete logarithm problem** asks: given g and g^a, recover a. Diffie–Hellman uses groups in which powers are easy to compute but this recovery problem is believed to be hard.

[DH76]; see also [HPS14, Ch. 2]

Elliptic-curve points: a different group law

Let $p > 3$ be prime. For $a, b \in \mathbb{F}_p$ with $4a^3 + 27b^2 \neq 0$, an **elliptic curve over** $\mathbb{F}_p$ is built from solutions of

$$y^2 = x^3 + ax + b$$

and an extra identity element $\mathcal{O}$ called the point at infinity. A rule called **point addition** makes these points an abelian group.

Scalar multiplication

$$[k]P = \underbrace{P + \cdots + P}_{k \text{ copies}}.$$

The double-and-add algorithm computes it efficiently.

Cryptographic role

Given P and $[k]P$, recovering k is the elliptic-curve discrete logarithm problem. It underlies elliptic-curve Diffie–Hellman (ECDH) and elliptic-curve signatures.

Background: [HPS14, Ch. 5]; practical curves: [LHT16]

Elliptic-curve example I: the calculation rules

Consider the following curve over the prime field $\mathbb{F}_{17}$:

$$E: \; y^2 = x^3 + 1, \qquad 4(0)^3 + 27(1)^2 \equiv 10 \not\equiv 0 \pmod{17}.$$

Identity and inverse

The identity is $\mathcal{O}$. For $P = (x, y)$,

$$-P = (x, -y \bmod 17).$$

Therefore $P + (-P) = \mathcal{O}$. In particular, if $P = (x, 0)$, then $P = -P$ and $2P = \mathcal{O}$.

Addition formula

For $P = (x_1, y_1)$ and $Q = (x_2, y_2) \neq -P$, set

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & P \neq Q, \\ (3x_1^2)(2y_1)^{-1}, & P = Q. \end{cases}$$

Then

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1,$$

and $P + Q = (x_3, y_3)$.

All arithmetic is modulo 17; u^{-1} means the inverse of a nonzero u. Formulas: [HPS14, Ch. 5].

Elliptic-curve example II: find the points

A pair $(x, y) \in \mathbb{F}_{17}^2$ lies on E precisely when $x^3 + 1$ is a square modulo 17. The possible square values are

$$\{y^2 : y \in \mathbb{F}_{17}\} = \{0, 1, 2, 4, 8, 9, 13, 15, 16\}.$$

The x-coordinates that work

x	0	1	2	6	7	9	10	14	16
$x^3 + 1$	1	2	9	13	4	16	15	8	0
y values	1, 16	6, 11	3, 14	8, 9	2, 15	4, 13	7, 10	5, 12	0

For $x \in \{3, 4, 5, 8, 11, 12, 13, 15\}$, the value $x^3 + 1$ is not a square modulo 17. Hence the table is exhaustive.

Elliptic-curve example III: list all points

The table on the previous slide gives the following complete point set:

$E(\mathbb{F}_{17})$

$$E(\mathbb{F}_{17}) = \{\, \mathcal{O},\ (0,1), (0,16), (1,6), (1,11), (2,3), (2,14), (6,8), (6,9), (7,2), (7,15), (9,4), (9,13), (10,7), (10,10), (14,5), (14,12), (16,0) \,\}.$$

Inverse pairs

Every point with $y \neq 0$ occurs together with

$$(x, -y \bmod 17).$$

There are eight such pairs.

The point $(16, 0)$ is its own inverse. Including $\mathcal{O}$,

$$|E(\mathbb{F}_{17})| = 16 + 1 + 1 = 18.$$

Elliptic-curve example IV: first multiples of P

Choose

$$P = (2, 3) \in E(\mathbb{F}_{17}), \qquad 3^2 \equiv 2^3 + 1 \equiv 9 \pmod{17}.$$

First compute $2P$

Since $6^{-1} \equiv 3 \pmod{17}$,

$$\lambda = \frac{3(2)^2}{2(3)} = \frac{12}{6} \equiv 12 \cdot 3 \equiv 2,$$
$$x_{2P} \equiv 2^2 - 2 - 2 \equiv 0,$$
$$y_{2P} \equiv 2(2 - 0) - 3 \equiv 1.$$

Therefore

$$2P = (0, 1).$$

Then compute $3P = 2P + P$

$$\lambda = \frac{3 - 1}{2 - 0} \equiv 1,$$
$$x_{3P} \equiv 1^2 - 0 - 2 \equiv 16,$$
$$y_{3P} \equiv 1(0 - 16) - 1 \equiv 0.$$

Therefore

$$3P = (16, 0).$$

Elliptic-curve example V: a proper subgroup

Since $(16, 0)$ is its own inverse, $6P = 2(3P) = \mathcal{O}$. Consequently, $4P = -2P = (0, 16)$ and $5P = -P = (2, 14)$.

All multiples before the first return to the identity

k	0	1	2	3	4	5	6
$[k]P$	$\mathcal{O}$	$(2, 3)$	$(0, 1)$	$(16, 0)$	$(0, 16)$	$(2, 14)$	$\mathcal{O}$

Thus

$$\langle P \rangle = \{\mathcal{O}, (2, 3), (0, 1), (16, 0), (0, 16), (2, 14)\}.$$

It has 6 elements, whereas $E(\mathbb{F}_{17})$ has 18. Therefore

$$\langle P \rangle \subsetneq E(\mathbb{F}_{17}),$$

so P is not a generator of the whole curve group.

Check: 6 divides 18, as Lagrange's theorem predicts. Practical protocols specify both the public point and the intended subgroup.

AES and GCM: fields in symmetric cryptography

Advanced Encryption Standard (AES)

A byte is represented by a degree-at-most-7 polynomial over $\mathbb{F}_2$, reduced using

$$x^8 + x^4 + x^3 + x + 1 = 0.$$

The AES substitution box (S-box), a nonlinear byte transformation, uses field inversion followed by a fixed linear-plus-constant map.

Galois/Counter Mode (GCM)

A 128-bit block is represented in a field defined using

$$x^{128} + x^7 + x^2 + x + 1 = 0.$$

GCM multiplies field elements to authenticate data.

A bitstring does not determine the field arithmetic by itself; the reduction polynomial is part of the representation.

AES: [Nat23]; GCM: [Dwo07]

Shamir secret sharing

A t-**out-of-**n **sharing** allows any t parties to recover a secret while fewer than t parties learn nothing about it. Let $s \in \mathbb{F}_q$ and choose distinct nonzero evaluation points.

1. Choose random $a_1, \ldots, a_{t-1} \in \mathbb{F}_q$.
2. Define
$$f(x) = s + a_1 x + \cdots + a_{t-1} x^{t-1}.$$
3. Give party i the point $(i, f(i))$.

Why a field is needed

Polynomial interpolation means reconstructing a polynomial from sufficiently many of its values. Its formulas divide by nonzero differences between evaluation points, so multiplicative inverses are essential.

[Sha79]

Permutation groups

A **permutation** of a set X is a bijection $X \to X$. All permutations of X form a group under composition. For each fixed key, a block cipher acts as one permutation of the block space.

Direct-product groups

Given a group G, the set

$$G^t = \{(g_1, \ldots, g_t) : g_i \in G\}$$

is a group under coordinatewise operations. This models vectors of masks, shares, or group elements.

A family of block-cipher permutations need not be closed under composition; the full permutation group is the surrounding algebraic structure.

Where today's algebra appears

Cryptographic setting	**Algebraic structure**	**Main operation**
One-time pad and masks	$(\{0,1\}^n, \oplus)$	XOR
Additive secret sharing	finite abelian group $(G, +)$	addition
RSA	$\mathbb{Z}_N^\times$	exponentiation modulo N
Diffie–Hellman	cyclic group $\langle g \rangle$	exponentiation
Elliptic-curve crypto	group of curve points	scalar multiplication
AES and GCM	$\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^{128}}$	finite-field arithmetic
Shamir sharing	finite field $\mathbb{F}_q$	evaluation and interpolation
Block ciphers	permutation group	function composition

Takeaways

1. **Groups:** one composable operation together with identities and inverses.
2. **Generated subgroups:** the elements reachable by repeatedly using one element.
3. **Repeated squaring:** large exponents computed using only $O(\log i)$ group operations.
4. **Fields:** addition, subtraction, multiplication, and nonzero division in one closed system.
5. **Cryptographic context:** different systems choose the group or field matching their required operation.
6. **Security:** algebra must be paired with a privacy proof or a stated hardness assumption.

The central design pattern

Make the honest operations well defined and efficient; then separately justify why the adversary learns nothing or faces a hard problem.

Reading guide

Required baseline

First read the distributed **Lecture 03: Groups and Fields** deck. Its 14 slides contain the minimum course material.

Requested textbook reading

Hoffstein–Pipher–Silverman, *An Introduction to Mathematical Cryptography*, 2nd ed.:

- **Section 2.5**: group vocabulary and structure;
- **Section 1.5**: powers, orders, generators, and primitive roots in finite fields.

Read Section 2.5 first, so its group terminology is available before Section 1.5.

References I

[DH76] Whitfield Diffie and Martin E. Hellman.
New directions in cryptography.
IEEE Transactions on Information Theory, 22(6):644–654, 1976.
doi:10.1109/TIT.1976.1055638.

[Dwo07] Morris Dworkin.
Recommendation for block cipher modes of operation: Galois/counter mode (gcm) and gmac.
NIST Special Publication 800-38D, National Institute of Standards and Technology, 2007.
doi:10.6028/NIST.SP.800-38D.

[HPS14] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman.
An Introduction to Mathematical Cryptography.
Undergraduate Texts in Mathematics. Springer, New York, 2 edition, 2014.
doi:10.1007/978-1-4939-1711-2.

[LHT16] Adam Langley, Mike Hamburg, and Sean Turner.
Elliptic curves for security.
RFC 7748, Internet Engineering Task Force, 2016.
doi:10.17487/RFC7748.

References II

[Nat23] National Institute of Standards and Technology.
Advanced encryption standard (aes).
Federal Information Processing Standards Publication 197-upd1, National Institute of Standards and Technology, 2023.
doi:10.6028/NIST.FIPS.197-upd1.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard Adleman.
A method for obtaining digital signatures and public-key cryptosystems.
Communications of the ACM, 21(2):120–126, 1978.
doi:10.1145/359340.359342.

[Sha49] Claude E. Shannon.
Communication theory of secrecy systems.
Bell System Technical Journal, 28(4):656–715, 1949.
doi:10.1002/j.1538-7305.1949.tb00928.x.

[Sha79] Adi Shamir.
How to share a secret.
Communications of the ACM, 22(11):612–613, 1979.
doi:10.1145/359168.359176.