A.2 · Abstract algebra and number theory

Original classroom teaching; not an official form or score predictor

Abstract algebra and number theory

- Check the group axioms and use Lagrange's theorem.
- Work with cyclic groups and the orders of elements.
- Use a **homomorphism** 同态 and its kernel.

Abstract algebra and number theory (2)

- Tell rings from **fields** 域, and find the units of $\mathbb{Z}/n\mathbb{Z}$.
- Use the Euclidean algorithm and Fermat's little theorem.

Groups

- Closure, associativity, an identity element, and an inverse for every element.
- Commutativity is extra: groups that have it are abelian.
- The integers form a group under addition, but not under multiplication: 2 has no integer inverse.

Subgroups and order

- Lagrange's theorem: in a finite group, the order of every subgroup divides the order of the group. So does the order of every element.
- The converse is false: a group of order 12 (the alternating group A_4) has no subgroup of order 6.
- A cyclic group of order n is generated by one element; in $\mathbb{Z}/n\mathbb{Z}$ the element k has order $n/\gcd(k, n)$.
- Every group of prime order is cyclic.

Homomorphisms

- Its kernel, the elements sent to the identity, is a normal subgroup.
- ϕ is one-to-one exactly when its kernel is only the identity.
- First isomorphism theorem: $G/\ker\phi \cong \operatorname{im}\phi$, so $|G| = |\ker\phi|\,|\operatorname{im}\phi|$ for finite G.

Rings and fields

- A ring has addition and multiplication; a field is a commutative ring in which every nonzero element has a multiplicative inverse.
- In $\mathbb{Z}/n\mathbb{Z}$, a is a unit exactly when $\gcd(a, n) = 1$. There are $\varphi(n)$ units, where φ is Euler's function.
- $\mathbb{Z}/n\mathbb{Z}$ is a field exactly when n is prime.

Figure: Rings and fields

Same addition rule; different invertibility

Ring	Multiplicative units	Check
mod 5	1, 2, 3, 4	every nonzero residue
mod 6	1, 5	2 times 3 is zero

- Mod 5 every nonzero residue is invertible; mod 6 the zero divisors 2 and 3 are not
- Match each part of the diagram to the text.

Number theory

- The Euclidean algorithm finds $\gcd(a, b)$ by repeated division, and gives integers x, y with $ax + by = \gcd(a, b)$.
- Fermat's little theorem: if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.
- Euler's theorem: if $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Worked example: two rings

- Both are groups under addition.
- Units mod 5: 1, 2, 3, 4, so $\mathbb{Z}/5\mathbb{Z}$ is a field. Units mod 6: only 1 and 5.
- Mod 6, $2 \times 3 = 0$ though neither factor is 0, so the nonzero elements are not even closed under multiplication.

Worked example: a large power

- 7 is prime and does not divide 3, so $3^{6} \equiv 1 \pmod 7$.
- $100 = 6 \times 16 + 4$, so $3^{100} \equiv 3^{4} = 81 \pmod 7$.
- $81 = 77 + 4$, so $3^{100} \equiv 4 \pmod 7$.

Common errors

- Assuming every group is abelian.
- Using the converse of Lagrange's theorem.
- Thinking every nonzero element of $\mathbb{Z}/n\mathbb{Z}$ is a unit.

Common errors (2)

- Applying Fermat's little theorem when the modulus is not prime.
- Forgetting that a **homomorphism**'s kernel must be checked before calling it one-to-one.

Key terms

- **homomorphism**: A map between algebraic structures that preserves the operation.
- **fields**: Commutative rings in which every nonzero element has a multiplicative inverse.

Check yourself

- What is the order of 3 in the additive group $\mathbb{Z}/12\mathbb{Z}$?
- How many units does $\mathbb{Z}/12\mathbb{Z}$ have?
- Can a group of order 15 have an element of order 4?