Let R_1, R_2, $\cdots$, R_n be rings. Prove that the Cartesian product

$$R\_1 \times R\_2 \times \cdots \times R\_n$$

is a ring under component-wise addition and multiplication. Show that if each R_i is a ring with identity, then so also is the product.

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

$$(a_1, a_2, -, a_n)(b_1, b_2, -, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

Verify the ring axioms — easy

Let R = Z × Z, and r, s constant integers. Define the maps on R as

Additive Identity : $(0,0)$

(a,b) + (c,d) = (a+b,c+d), and

(a,b)(c,d) = (ad + bc + rac, bd + sac).

$-(a,b) = (-a,-b)$

Multiplicative identity : $(0,1)$

(a) Prove that R is a ring under these operations.

commutative : ✓

$$((a,b)(c,d))(e,f) = (ad+bc+rac,\ bd+sac)(e,f)$$

$$= ((ad+bc+rac)f + (bd+sac)e + r(ad+bc+rac)e,\ (bd+sac)f + s(ad+bc+rac)e)$$

$$(a,b)((c,d)(e,f)) = (a,b)(cf+de+rce,\ df+sce)$$

$$= (a(df+sce) + b(cf+de+rce) + ra(cf+de+rce),\ b(df+sce) + sa(cf+de+rce)$$

(b) Prove that R is an integral domain if and only if r^2 + 4s is not a perfect square.

To show: R has non-zero zero divisors

$\Leftrightarrow$ r^2+4s is a perfect square

" $\Rightarrow$ "

$a \neq 0, \ c \neq 0$

$$(a, b)(c, d) = (0, 0)$$

$$ad + bc + rac = 0 \qquad r = \frac{ad+bc}{ac}$$

$$bd + sac = 0$$

$$s = -\frac{bd}{ac}$$

$a = 0 \Rightarrow (a,b)(c,d)$

$= (bc, bd)$

$= (0, 0)$

$\Rightarrow b = 0$ or $c = d = 0$.

$$r^2 + 4s = \left(\frac{ad-bc}{ac}\right)^2$$

" $\Leftarrow$ " r^2+4s is a perfect square.

$$x^2 - rx - s = (x-\alpha)(x-\beta)$$

$\alpha, \beta \to$ integers

$$\alpha + \beta = r, \quad \alpha\beta = -s$$

$$(1, -\alpha)(1, -\beta) = (0,0)$$

$\neq 0$ $\neq 0$ zero

Prove that $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ is an integral domain. Argue that $\mathbb{Z}[\sqrt{5}]$ contains infinitely many units. Prove that $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ is a field.

Domain:

$\mathbb{Z}[\sqrt{5}] \subseteq \mathbb{R}$ closure under $-$, $\cdot$

$(a+b\sqrt{5}) - (c+d\sqrt{5}) = (a-c) + (b-d)\sqrt{5}$

$(a+b\sqrt{5})(c+d\sqrt{5}) = (ac+5bd) + (ad+bc)\sqrt{5}$

commutative ✓ identity $\rightarrow$ 1

non-zero zero divisors $\rightarrow$ X

Units in $\mathbb{Z}[\sqrt{5}]$:

$(a+b\sqrt{5})(c+d\sqrt{5}) = 1$

$u(a+b\sqrt{5})(a-b\sqrt{5}) = 1$

$u(a^2-5b^2) = 1 \Rightarrow u = \pm 1$

$a^2 - 5b^2 = 1$

$a^2 - 5b^2 = -1$

$$a^2 - 5b^2 = 1$$

$$9^2 - 5 \times 4^2 = 1$$

$a = \pm 1, \quad b = 0$

units: $1, -1$

$$(9 + 4\sqrt{5})(9 - 4\sqrt{5}) = 1$$

$$(9 + 4\sqrt{5})^r (9 - 4\sqrt{5})^r = 1$$

for all $r \geqslant 1$

$$a^2 - 5b^2 = -1$$

$$(2 + \sqrt{5})(2 - \sqrt{5}) = -1$$

$$(2 + \sqrt{5})(-2 + \sqrt{5}) = 1$$

$r = 2$

$$(2 + \sqrt{5})^r (-2 + \sqrt{5})^r = 1 \quad \forall\, r \geqslant 1$$

$2+\sqrt{5} \longrightarrow$ "fundamental unit"

Algebraic number theory

$\mathbb{Z}[\sqrt{5}] \longrightarrow$ number "rings"

$1, \sqrt{5}, 5$

$1, \sqrt[3]{2}, \sqrt[3]{4}, 2$

$\{a+b\sqrt{5} \mid a,b \in \mathbb{Q}\}$ is a field.

$a+b\sqrt{5} \neq 0$ $\quad \dfrac{1}{a+b\sqrt{5}} = \dfrac{a-b\sqrt{5}}{a^2-5b^2}$

denom $\neq 0$ since $\sqrt{5}$ is irrational.

Prove that $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a,b \in \mathbb{Z}\}$ is an integral domain. Find all the units in this ring. Prove that $\mathbb{Q}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a,b \in \mathbb{Q}\}$ is a field.

Only units : $\{1, -1\}$

Prove that the set Z_n of integers modulo n is a commutative ring with identity. What are the units of Z_n? How many units?
Prove that for gcd(a,n)=1, we have a^φ(n) ≡ 1 (mod n).
What if n is prime?

See initial part of video

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ ← c.r.i

$\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n \mid \gcd(a,n) = 1 \}$

$|\mathbb{Z}_n^*| = \phi(n)$

$a \in \mathbb{Z}_n^*$ $\quad a^{\phi(n)} \equiv 1 \pmod{n}$ [Euler's theorem]

$n = p, \ \phi(n) = p-1 \Rightarrow a^{p-1} \equiv 1 \pmod{n}$ [Fermat's little theorem]

Let R be a commutative ring with identity. Prove that the set R[x] of all univariate polynomials with coefficients from R is again a commutative ring with identity (under polynomial addition and multiplication).

Verify the ring axioms

Let R be a commutative ring. An element $a \in R$ is said to be *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$.

(a) Given an example of a non-zero nilpotent element in a ring.

(b) Prove that if a and b are nilpotent, then so also is $a + b$.

(c) Let R be with identity. Prove that if a is nilpotent and u is a unit, then $a + u$ is a unit.

(a) Take $R = \mathbb{Z}_4$, $a = 2$

(b) $a^m = 0$, $b^n = 0$

$(a+b)^{m+n} \rightarrow$ binomial expansion

(a) Prove that there cannot be any non-zero homomorphism $\mathbb{Z}_n \to \mathbb{Z}$ for any $n \in \mathbb{N}$.

(b) Prove that there exists a non-zero homomorphism $\mathbb{Z}_m \to \mathbb{Z}_n$ taking $[1]_m \mapsto [1]_n$ if and only if $n|m$.

(c) Prove that the only non-zero homomorphism of $\mathbb{Z} \to \mathbb{Z}$ is the identity map.

(b) $\quad f : \mathbb{Z}_m \to \mathbb{Z}_n$

$$f(1) = 1 \qquad \Rightarrow \quad n \mid m$$

$$f(1+1) = f(1) + f(1) = 1 + 1 = 2$$

$$f(\underbrace{1+1+\cdots+1}_{m \text{ times}}) = 1+1+\cdots+1 = m$$

$0 \pmod{m}$ $\qquad f(0) = 0 \qquad m \equiv 0 \pmod{n}$

Define an operation $\circ$ on $G = \mathbb{R}^* \times \mathbb{R}$ as $(a,b) \circ (c,d) = (ac, bc+d)$. Prove that $(G, \circ)$ is a non-abelian group.

Identity $(1, 0)$

$$(a, b)^{-1} = \left(\frac{1}{a}, -\frac{b}{a}\right)$$

<u>not Abelian</u>

Give an example

Let G be the set of all points on the hyperbola $xy = 1$ along with the point $(0,\infty)$ at infinity. Define $(a,1/a) + (b,1/b) = (a+b, 1/(a+b))$. Prove that G is an Abelian group under this operation.

Let G be a (multiplicative) group, and H, K subgroups of G. Prove that:

(a) $H \cap K$ is a subgroup of G.
(b) $H \cup K$ need not be a subgroup of G.
(c) $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.
(d) Define $HK = \{hk \mid h \in H,\ k \in K\}$. Define KH analogously. Prove that HK is a subgroup of G if and only if $HK = KH$.

(a) Closure under mul and inverse.

(b) $H \cup K$ need not be a subgp.

$$G = (\mathbb{Z}, +) \qquad H = (2\mathbb{Z}, +)$$
$$K = (3\mathbb{Z}, +)$$

$$2 \in H \cup K, \quad 3 \in H \cup K$$
$$2 + 3 = 5 \notin H \cup K$$

(c) "$\Rightarrow$" $H \cup K$ is a subgp of G.

Assume $H \not\subseteq K$

To show that $K \subseteq H$.

$\exists\ h \in H,\ h \notin K$.

Take any $k \in K$.

$hk \in H \cup K$

$hk \in H$ or $hk \in K$

$(h^{-1}h)k = k \in H$

$h(kk^{-1}) \in K$

$h \in K$ $\lightning$

Let G be a group. Let $\operatorname{Aut} G$ denote the set of all automorphisms of G. Prove that $\operatorname{Aut} G$ is a group under function composition.

Prove that $\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^*$.

Let p be a prime. Prove that $\operatorname{Aut} \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}^*$.

Let G be a non-abelian group, and $a, b \in G$. Prove that $\operatorname{ord}(ab) = \operatorname{ord}(ba)$.

$G \to$ finite (not nec. abelian)

$\operatorname{ord}(ab) = m$

$\operatorname{ord}(ba) = n$

$(ab)^m = e$ $\qquad a(ba)^{m-1} b = e$

$(ba)^m \cdot b = b \Rightarrow (ba)^m = e$

$\Rightarrow n \mid m$

Likewise, $m \mid n$ $\qquad \Rightarrow m = n$

Let G be a finite group, and $h = \operatorname{ord}(a)$ for some $a \in G$. Prove that $\operatorname{ord}(a^k) = \dfrac{h}{\gcd(h,k)}$ for all $k \in \mathbb{Z}$.

$$h = \operatorname{ord}(a) \Rightarrow \operatorname{ord}(a^k) = \frac{h}{\gcd(h,k)}$$

$$\operatorname{ord}(a^k) = l.$$

$$(a^k)^{\frac{h}{\gcd(h,k)}} = (a^h)^{\frac{k}{\gcd(h,k)}} = e$$

$$\Rightarrow l \,\Big|\, \frac{h}{\gcd(h,k)}$$

$$(a^k)^l = e \Rightarrow h \mid kl \Rightarrow \frac{h}{\gcd(h,k)} \,\Big|\, \frac{k}{\gcd(h,k)} l$$

$$\Rightarrow \frac{h}{\gcd(h,k)} \,\Big|\, l$$

Let $G_1, G_2, \ldots, G_n$ be groups and $G = G_1 \times G_2 \times \cdots \times G_n$. Let each G_i be finite of order m_i. Establish that G is cyclic if and only if each G_i is cyclic and $\gcd(m_i, m_j) = 1$ for $i \neq j$.

Let G be a finite group. The smallest positive integer n such that $a^n = e$ for all $a \in G$ is called the *exponent* of G, denoted $\exp(G)$. Prove that:

(a) $\exp(G) = \operatorname{lcm}(\operatorname{ord}(a) \mid a \in G)$.

(b) $\exp(G) | \operatorname{ord}(G)$.

(c) If G is abelian, then there exists an element of G of order equal to $\exp(G)$.

(d) If G is abelian, and $\exp(G) = \operatorname{ord}(G)$, then G is cyclic.

(e) Parts (c) and (d) do not necessarily hold if G is not abelian.