

• every finite domain is a division ring

↳ nonzero elements can be cancelled, so the nonzero elts form a group

↳ $|R|=n$, the set $\{x, x^2, x^3, \dots, x^n\}$ contains a duplicate

$x^i = x^j$, $i < j$. Then $x^i(1 - x^{j-i}) = 0$, $x^i \neq 0 \Rightarrow x^{j-i} = 1$,
so x^{j-i-1} is inverse for x .

idempotent: $e^2 = e$

nilpotent: $\exists n$ s.t. $x^n = 0$.

Jordan-Hölder Theorem:

If $1 = H_k \triangleleft H_{k-1} \triangleleft \dots \triangleleft H_1 = G$ and $1 = G_\ell \triangleleft G_{\ell-1} \triangleleft \dots \triangleleft G_1 = G$

are two comp. series for G , then $\ell = k$ and

$$\exists \sigma \in S_{k-1} \text{ s.t. } G_i / G_{i+1} \cong H_{\sigma(i)} / H_{\sigma(i)+1}.$$

We can use this to prove $\overset{\text{arithmetic.}}{\text{FTA}}$:

Idea $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell.$

→ → → →

$$\mathbb{Z}_n \triangleright \mathbb{Z}_{\frac{n}{p_1}} \triangleright \mathbb{Z}_{\frac{n}{p_1 p_2}} \triangleright \dots \triangleright \mathbb{Z}_{p_k} \triangleright 1$$

$$\mathbb{Z}_n \triangleright \mathbb{Z}_{\frac{n}{q_1}} \triangleright \mathbb{Z}_{\frac{n}{q_1 q_2}} \triangleright \dots \triangleright \mathbb{Z}_{q_\ell} \triangleright 1$$

Prime Ideal

R/P is an integral domain

$$IJ \subset P \Rightarrow I \subset P \text{ or } J \subset P.$$

$$(I : J) = \{ r \in R \mid rJ \subset I \}$$

$$\text{ann}(x) = \{ r \mid rx = 0 \} = \{ r \mid r(x) \subset (0) \} = (0 : x)$$

$$\mathcal{Z}(R) = \bigcup_{x \in R} \text{ann}(x)$$

$a \in R$ is irreducible if (TFAE)

$$\textcircled{1} \quad a = bc \Rightarrow b \text{ or } c \text{ is a unit}$$

$$\textcircled{2} \quad a = bc \Rightarrow (a) = (b) \text{ or } (a) = (c)$$

$\textcircled{3}$ (a) is maximal in the set of proper principal ideals.

$$\mathbb{Z}_4, \quad 0, 2 \quad 0\text{-divisors}$$

$$\mathbb{Z}_6, \quad 3^2 = 3, \quad 3^3 = 3, \quad \text{et cetera}$$

$$\mathbb{Z}_6[X] \quad (2x+3)(3x+2) = x$$

$\uparrow \quad \quad \uparrow$
 both irreducible

Central Series

$$G = G_0 \geq G_1 \geq \dots \geq G_n = 1$$

$$(1) \quad G_{i+1} \triangleleft G_i$$

$$(2) \quad G_i/G_{i+1} \leq \mathbb{Z}(G/G_{i+1})$$

G is nilpotent iff it has a central series.