- if $\mathbb{F}$, $\mathbb{K}$ two fields

$\mathbb{F}$ $\qquad$ $\mathbb{K}$

$\{ \rightarrow \cdot_{\mathbb{F}}, +_{\mathbb{F}} \qquad \cdot_{\mathbb{K}}, +_{\mathbb{K}}$

$\rightarrow 1_{\mathbb{F}}, 0_{\mathbb{F}} \qquad 1_{\mathbb{K}} \quad 0_{\mathbb{K}}$

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

→ a field homomorphism (field map)

is a function

$$f: \mathbb{F} \rightarrow \mathbb{K} \quad \text{s.t.}$$

$$f(0_{\mathbb{F}}) = 0_{\mathbb{K}}$$

$$f(1_{\mathbb{F}}) = 1_{\mathbb{K}}$$

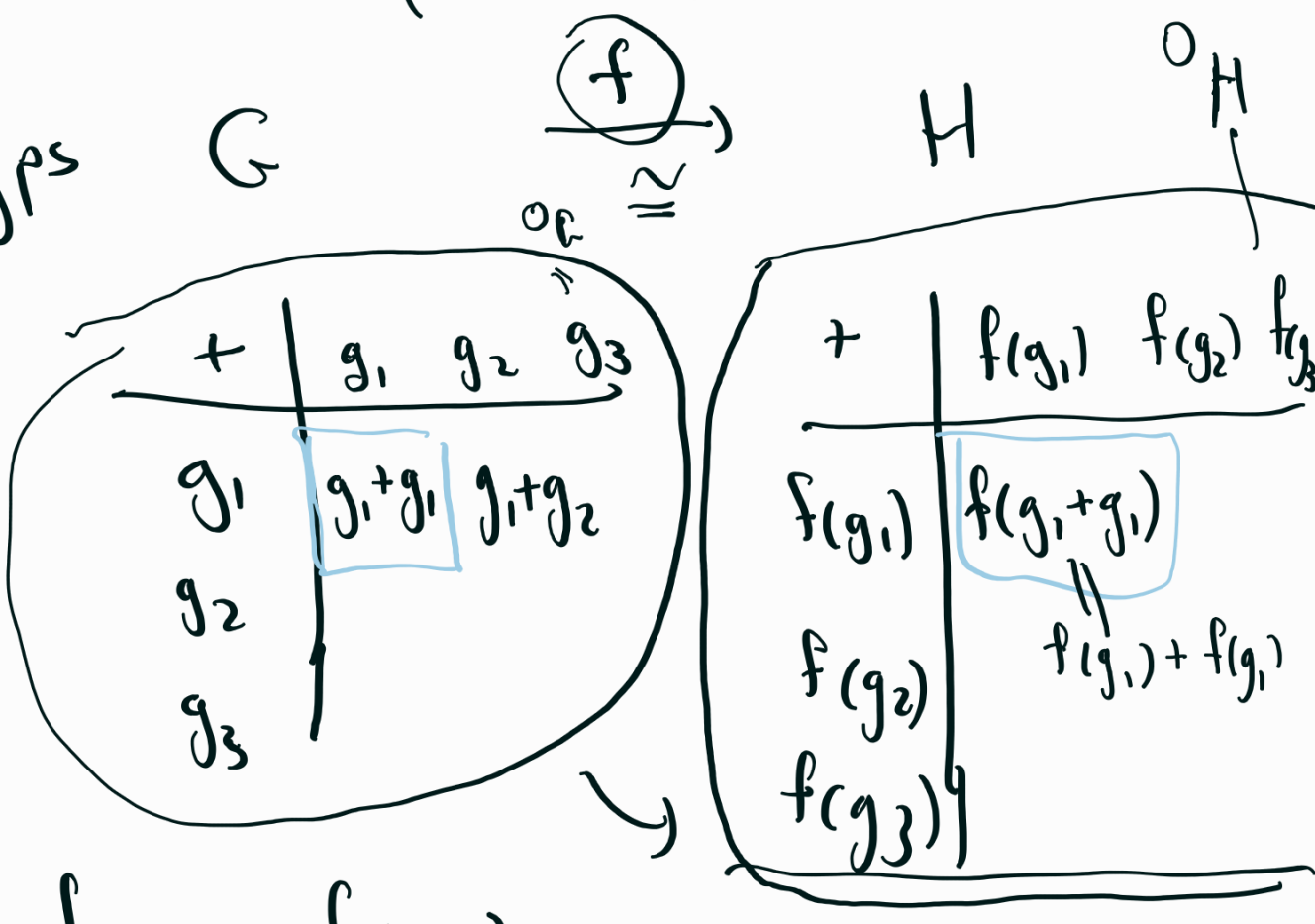
$\forall a, b \in \mathbb{F} \quad f(a+b) = f(a) + f(b)$

$$f(a \cdot_F b) = f(a) \cdot_{ik} f(b)$$

$$\xrightarrow{\text{mod } n} \underset{=}{\mathbb{Z}} \longrightarrow \underset{=}{\mathbb{Z}_n}$$

$$(a \bmod n) + (b \bmod n)$$

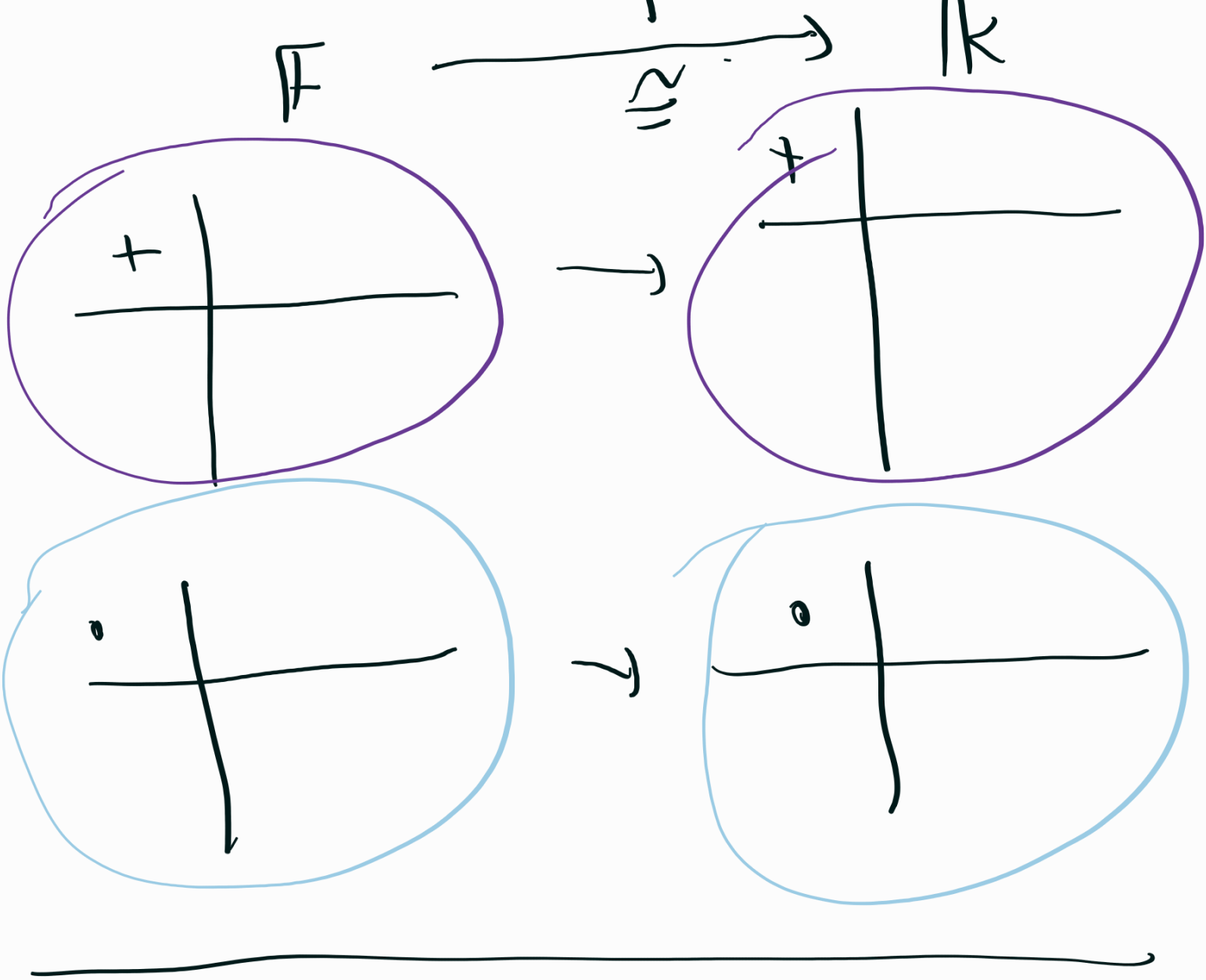
$$= (a+b) \bmod n$$

ab gps $G \xrightarrow{f} H$, $H \cong$ 

$$f(g_1) + f(g_1)$$

$$= f(g_1+g_1)$$

$$f$$



F field, $\phi(x) \in F[x]$ prime

ϕ has no roots in F

($\phi(x) = (x-a) \cdot \phi'(x)$)

Want: field k s.th

1) $F \subseteq \mathbb{K}$

2) for $\phi(x) \in \mathbb{K}[x]$

we have

$$\phi(x) = \alpha \cdot \prod_{i=1}^{n} (x - \alpha_i)$$

$\alpha, \alpha_1, \ldots, \alpha_n \in \mathbb{K}$.

3) if $\mathbb{L}$ is a field s.t h

(a) $F \subseteq \mathbb{L} \subseteq \mathbb{K}$

(b) ϕ splits over $\mathbb{L}$

then $\mathbb{L} = \mathbb{K}$

Example 5.57 : $F = \mathbb{Q} \subseteq \mathbb{C}$

$f(x) = x^4 - 2$ is prime

over $\mathbb{Q}$ $\pm\sqrt[4]{2}$, $\pm i\cdot\sqrt[4]{2}$

"$\mathbb{Z}/n\mathbb{Z}$" "$\mathbb{Z}_n$"

- $\mathbb{K}_1 = \mathbb{Q}[x] / (f) \simeq \mathbb{Q}[x]_f$

$$= \left\{ r(x) = a_k x^k + \dots + a_1 x + a_0 \;\middle|\; a_i \in \mathbb{Q},\ k < \deg f = 4 \right\}$$

$\mathbb{F} = \mathbb{Q}$

$r_1, r_2 \in \mathbb{K}_1$

$$\begin{cases} r_1 + r_2 \pmod f \\ r_1 \cdot r_2 \pmod f \end{cases}$$

$\mathbb{K}_1$ is a field.

$\mathbb{Q} \subseteq \mathbb{K}_1$

- Consider $f(X) \in \mathbb{K}_1[X]$

$g(X) = \mathbb{K}_1[X]$

$X^k \quad X^{k-1}$

$$\cdot \begin{cases} g(X) = r_k(x) X^k + r_{k-1}(x) \cdot X^{k-1} \cdots \\ g'(X) = r'_k(x) X^k + r'_{k-1}(x) X^{k-1} \cdots \end{cases}$$

$$r_k(x) \cdot r'_k(x) \cdot X^{2k} + \cdots$$

$\mod f$

$\deg r < \deg f$

$$r_1 \cdot r_2 = f \cdot q + r$$

$r_0(x) = 2$

$$r_1 \cdot r_2 = r \pmod f$$

$$X^4 - 2 = f(X) \in \mathbb{k}_1[X]$$

Claim: f has a root in $\mathbb{k}_1$

Proof: consider $r_1(x) := \underbrace{x}_{\alpha} \in \mathbb{k}_1$

$$\mathbb{k}_1 \ni f(X)| = f(X)|$$

$r_1(x)$ $\quad$ x

$\Rightarrow$

$\exists\ f(x) = 0 \pmod{f}$

$\Rightarrow$

$\Rightarrow \quad f(X) = (X - x) f'(X)$

$\mathbb{Q}$, $f(x) = x^4 - 2$

Say α is a root of f

in some $\mathbb{Q} \subseteq \mathbb{K}$ $\quad \mathbb{K}_1$

Consider $\rightarrow \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$

$\Downarrow$

$\alpha = x$

Suppose $\boxed{\phi(x) = x^2 + 1}$

$\in \mathbb{Q}[x]$

$\boxed{\alpha^2 + 1 = 0}$

---

before 552 | α $\quad \mathbb{Q}(\alpha)$

$$\mathbb{Q}(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f, g \in \mathbb{Q}[x],\ g \neq 0 \right\}$$

$$\frac{f(\alpha)}{g(\alpha)} + \frac{f'(\alpha)}{g'(\alpha)} := \qquad f(x) = x,\ f(\alpha) = \alpha$$

$$\frac{f(\alpha)g'(\alpha) + f'(\alpha)g(\alpha)}{g(\alpha)g'(\alpha)} \in \mathbb{Q}(\alpha)$$

$$\frac{f(\alpha)}{g(\alpha)} \cdot \frac{f'(\alpha)}{g'(\alpha)} = \frac{(f \cdot f')(\alpha)}{(g \cdot g')(\alpha)}$$

$$\mathbb{Q}(\alpha) \ni \alpha$$

$$\mathbb{Q}(\alpha) \ni \alpha^2, \alpha^3 \cdots$$

$$\Rightarrow \text{if } a \in \mathbb{Q}$$

$$a \cdot \alpha \in \mathbb{Q}(\alpha)$$

$$a \cdot \alpha^2 \in \mathbb{Q}(\alpha)$$

$$\forall\ f(x) \in \mathbb{Q}[x]$$

$$f(\alpha) \in \mathbb{Q}(\alpha)$$

$$\mathbb{Q}(\alpha) \ni \alpha^{-1}, \alpha^{-2}, \cdots$$

$$a \in \mathbb{Q} \qquad a \cdot \alpha^{-1} \in \mathbb{Q}(\alpha)$$

$$\forall\ g(x) \neq 0 \in \mathbb{Q}[x]$$

$$\underline{\mathbb{Q}(\alpha)} \ni \frac{1}{g(\alpha)}$$

$$\Rightarrow \frac{f(\alpha)}{g(\alpha)} \in \mathbb{Q}(\alpha)$$

$$-\frac{f(\alpha)}{g(\alpha)} := \frac{-f(\alpha)}{g(\alpha)}$$

$$\frac{f(\alpha)}{g(\alpha)} + \left(-\frac{f(\alpha)}{g(\alpha)}\right) = 0$$

$$0 = \frac{0}{g(\alpha)}$$

$$\left(\frac{f(\alpha)}{g(\alpha)}\right)^{-1} = \frac{g(\alpha)}{f(\alpha)}$$

In our case $\phi(x) = x^2 + 1$

$\Rightarrow \alpha^2 + 1 = 0$

So $\left\{ \dfrac{f(\alpha)}{g(\alpha)} = \dfrac{f(x)|_\alpha}{g(x)|_\alpha} = \dfrac{r_1(\alpha)}{r_2(\alpha)} \right.$

$$f = q_1 \phi + r_1$$

$$g = q_2 \phi + r_2$$

$$f(\alpha) = q_1(\alpha)\,\phi(\alpha) + r_1(\alpha) = r_1(\alpha)$$

$$g(\alpha) = r_2(\alpha)$$

$r(x)$ — r_1, r_2 — k_1, k_2

$\phi(x) = x^2 + 1$

$\mathbb{Q}[x]/\phi$

$$\mathbb{Q}(\alpha) = \left\{ \frac{r_1(\alpha)}{r_2(\alpha)} \;\middle|\; r_1, r_2 \in \mathbb{Q}[x],\ r_2 \neq 0 \right\}$$

$\deg r_1, \deg r_2 < \deg \phi = 2$

min field $\supseteq \mathbb{Q}$

$+ \alpha$

$\mathbb{C}$

$\mathbb{Q}(\alpha) \simeq \mathbb{Q}(i)$

$\mathbb{Q}(\alpha)$

$$= \{ a + bi \mid a, b \in \mathbb{Q} \}$$

$$\cong \{ a + b \cdot (-i) \mid a, b \in \mathbb{Q} \}$$

$$\mathbb{Q}(-i)$$

$+ \bmod \phi$

$\cdot \bmod \phi$

$$\mathbb{K}_1 = \mathbb{Q}[x]/(\phi) = \{ r(x) \mid \deg r < \deg \phi \}$$

claim $\mathbb{K}_1 \cong \mathbb{Q}(\alpha)$

$$\mathbb{Q}(\alpha) = \left\{ \frac{r_1(\alpha)}{r_2(\alpha)} \;\middle|\; \begin{array}{l} \deg r_1 \\ \deg r_2 \end{array} < \deg \phi \right\}$$

$r_1(x), r_2(x) \in \mathbb{K}_1$, $\boxed{\phi(x) = x^4 - 2}$

$2 = x$ is a root of ϕ

$(\phi(X) \in \mathbb{K}_1[X])$

$\phi(x)$ in K_1 α satisfies

$x^4 - 2 = \alpha^4 - 2 = 0$

$K_1 = \mathbb{Q}[x]/(\phi) \cong \mathbb{Q}(\alpha)$

for α s.th $\alpha^4 - 2 = 0$

$\left(\alpha \in \{ \pm \sqrt[4]{2}, \pm i\sqrt[4]{2} \}\right)$

$K_1[X] \ni \phi(X) = (X - \alpha)\phi'(X)$

$\deg \phi' < \deg \phi$

Let

$\phi(X) = p_1(X) \cdots p_s$

where $p_1, \ldots, p_s$ are prime in $k_1[X]$

Wlog suppose

$\forall i \geq j$ $p_i(X)$ is not linear

$k_2 = k_1[X] / p_{j+1}(X) \cong k_1(\alpha_2)$

$\exists \alpha_2$ a root of $p_{j+1}(X)$ in k_2

$\phi(x) = x^4 - 2$

$$\mathbb{Q}[x]/(\phi) = \mathbb{Q}(\alpha)$$

$$\mathbb{Q}(\sqrt[4]{2}) = \left\{ a + b\cdot\sqrt[4]{2} \;\middle|\; a, b \in \mathbb{Q} \right\}$$

obs $\quad \sqrt{2} = \sqrt[4]{2}\cdot\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$

$\mathbb{Q}(\sqrt[4]{2})$: $\quad \phi(x) = x^4 - 2$

$$= (x - \sqrt[4]{2})\cdot(x + \sqrt[4]{2})\cdot(x^2 + \sqrt{2})$$

$\pm i\sqrt[4]{2}$ — $(x^2+\sqrt{2})$

$\phi'(x)$

$$\mathbb{Q}(\sqrt[4]{2})[x]/(\phi')$$

$$\mathbb{Q}(\sqrt[4]{2}, i\cdot\sqrt[4]{2})$$

a, b, c

$$= \left\{ a + b\sqrt[4]{2} + c \cdot i\sqrt[4]{2} \;\middle|\; \in \mathbb{Q} \right\}$$

Splits $\not\emptyset$

$$\cong \mathbb{Q}\left(\sqrt[4]{2}, i\right)$$

$$= \left\{ a + b\sqrt[4]{2} + c \cdot i \;\middle|\; \begin{matrix} a,b,c \\ \in \mathbb{Q} \end{matrix} \right\}$$

$\mathbb{F}_p$ $\quad \phi(x) = x^q - x$ $\quad$ $\not\mid$ $\quad q = p^n$

$\mathbb{F}_p \subseteq \mathbb{F}_q$