(b) $\Leftrightarrow$ (c): Check that the rings $\mathbb{Z}[i]/(p)$, $\mathbb{F}_p[x]/(x^2+1)$ are isomorphic, as both are isomorphic to $\mathbb{Z}[x]/(p, x^2+1)$:

one can check $\mathbb{Z}[x] \xrightarrow{\varphi_1} \mathbb{Z}[i]/(p)$

$x \longmapsto i + (p) =: \bar{i}$

and $\mathbb{Z}[x] \xrightarrow{\varphi_2} \mathbb{F}_p[x]/(x^2+1)$

$x \longmapsto \bar{x}$

both are surjective and have $\ker(\varphi_1) = \ker(\varphi_2) = (p, x^2+1) \subset \mathbb{Z}[x]$

[This is an instance of using Noether's 3rd isomorphism theorem: For ideals $I, J \subset R$

$R/I+J \cong (R/I)/\bar{J}$

and $R/I+J \cong (R/J)/\bar{I}$ ← so these two rings must be isomorphic

Above $R = \mathbb{Z}[x]$, $I = (p)$, $J = (x^2+1)$, $I+J = (p, x^2+1)$]

3/1 ~~2/21~~/2019

(c) $\Leftrightarrow$ (d): $\mathbb{F}_p[x]/(x^2+1)$ is a field

$\Leftrightarrow (x^2+1)$ is maximal in $\mathbb{F}_p[x]$

$\Leftrightarrow x^2+1$ is irreducible in $\mathbb{F}_p[x]$

$\Leftrightarrow x^2+1 = 0$ has no roots $x \in \mathbb{F}_p$

$\Leftrightarrow x^2 = -1$ has no solution $x \in \mathbb{F}_p$

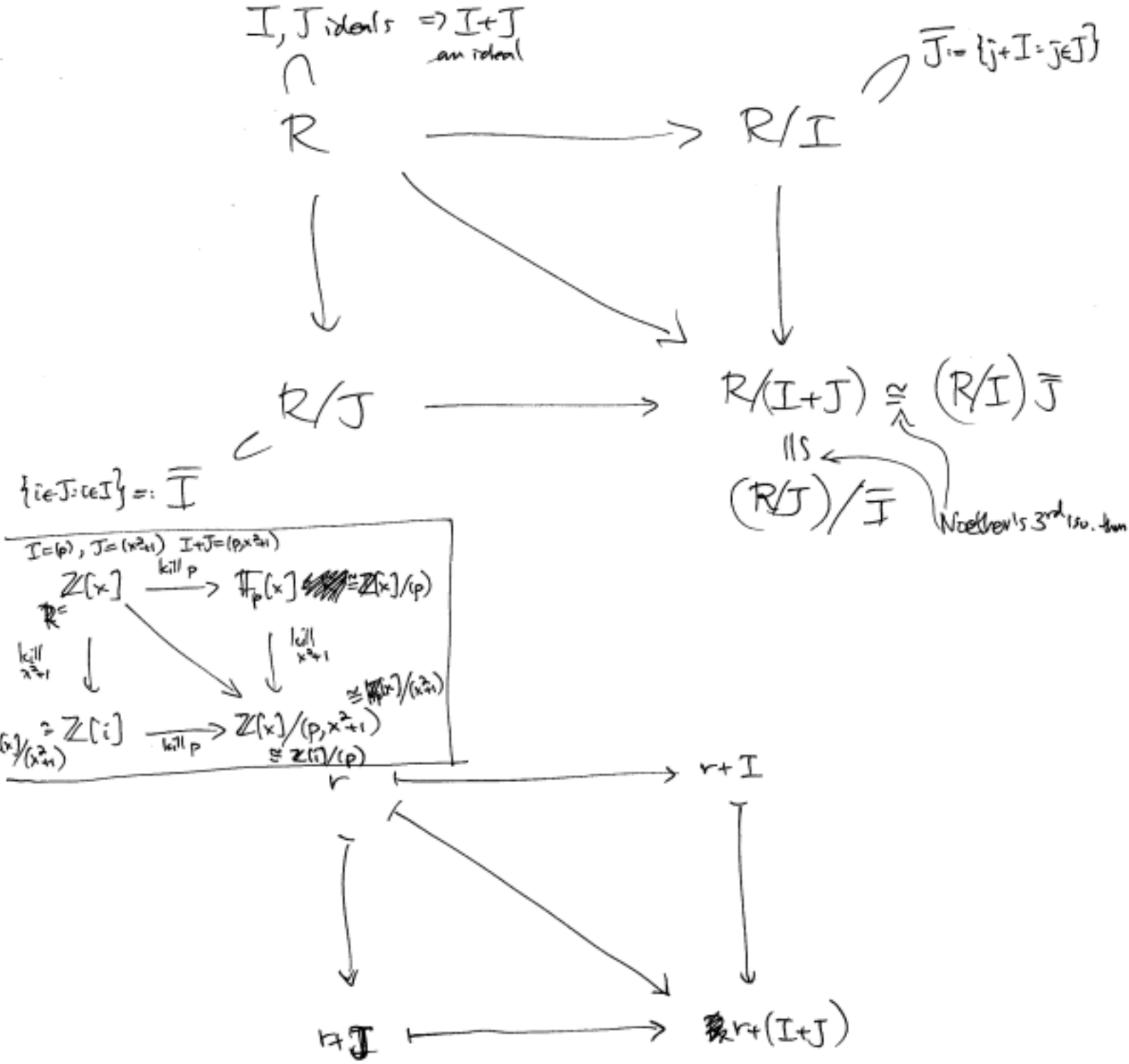
(d) $\Leftrightarrow$ (e): $x^2 = -1$ has a solution in $\mathbb{F}_2$, namely $x = \bar{1}$ ($\{\bar{0}, \bar{1}\}$)

For odd primes p, where $-\bar{1} \neq +\bar{1}$ in $\mathbb{F}_p$, then $\bar{x}^2 = -\bar{1} \Rightarrow \bar{x}^4 = +\bar{1}$

so $\bar{x}$ is an element of $\mathbb{F}_p^\times$ of order exactly 4. Since $\mathbb{F}_p^\times$ is cyclic, such an $\bar{x}$ exists $\Leftrightarrow$ 4 divides $|\mathbb{F}_p^\times| = p-1 \Leftrightarrow p \equiv 1 \bmod 4$ ∎

(49½)

How were we using Noether's 3rd isomorphism theorem again?



How many ways to write $n \in \mathbb{Z}$ as $n = a^2 + b^2$ with $a, b \in \mathbb{Z}$?
i.e. as ordered pairs $(a,b) \in \mathbb{Z}^2$

EXAMPLES:

① $n = 25 = 5^2$
$= 0^2 + (\pm 5)^2$
$= (\pm 5)^2 + 0^2$
$= (\pm 3)^2 + (\pm 4)^2$
$= (\pm 4)^2 + (\pm 3)^2$
$= 4(2+1)$ ways

② $n = 125 = 5^3$
$= (\pm 5)^2 + (\pm 10)^2$
$= (\pm 10)^2 + (\pm 5)^2$
$= (\pm 2)^2 + (\pm 11)^2$
$= (\pm 11)^2 + (\pm 2)^2$
$= 4(3+1)$ ways

③ $n = 50 = 2 \cdot 5^2$
$= (\pm 1)^2 + (\pm 7)^2$
$= (\pm 7)^2 + (\pm 1)^2$
$= (\pm 5)^2 + (\pm 5)^2$
$= 4(2+1)$ ways

④ $n = 103$ has zero ways

THEOREM: If $n = 2^c p_1^{e_1} \cdots p_k^{e_k} q_1^{d_1} \cdots q_l^{d_l}$ where p_i, q_j are odd primes

$p_i \equiv 1 \bmod 4$
$q_j \equiv 3 \bmod 4$

then #ways to write $n = a^2 + b^2$ with $(a,b) \in \mathbb{Z}^2$

$$= \begin{cases} 0 & \text{if any } d_i \text{ are odd,} \\ 4(e_1+1)\cdots(e_k+1) & \text{if all } d_i \text{ are even.} \end{cases}$$

proof: If $n = a^2 + b^2 = (a+ib)(a-ib)$ then factor $a+ib = \pi_1 \cdots \pi_k \sigma_1 \cdots \sigma_l$ in $\mathbb{Z}[i]$

primes π_i with $\pi_i \bar{\pi}_i = p_i \equiv 1 \bmod 4$ or $p_i = 2$

primes σ_j with σ_j assoc. to $q_j \equiv 3 \bmod 4$

and $n = (\pi_1 \cdots \pi_k \sigma_1 \cdots \sigma_l)(\bar{\pi}_1 \cdots \bar{\pi}_k \bar{\sigma}_1 \cdots \bar{\sigma}_l)$
$= (\pi_1 \bar{\pi}_1) \cdots (\pi_k \bar{\pi}_k)(\sigma_1 \bar{\sigma}_1) \cdots (\sigma_l \bar{\sigma}_l)$
$= p_1 \cdots p_k q_1^2 \cdots q_l^2 \Rightarrow$ all d_i even.

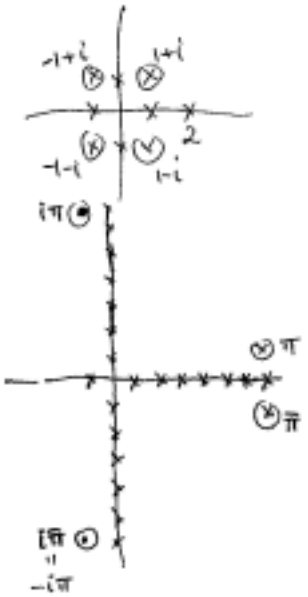
On the other hand to obtain

$2^c \underbrace{p_1^{e_1} \cdots p_k^{e_k}}_{\pi_1^{e_1}\bar{\pi}_1^{e_1}\cdots\pi_k^{e_k}\bar{\pi}_k^{e_k}} q_1^{d_1} \cdots q_\ell^{d_\ell} = n = (a+bi)(a-bi)$, if $p_i = \pi_i \bar{\pi}_i$ for $i=1,\dots,k$

then the prime factorization in $\mathbb{Z}[i]$ of $a+bi$ must look, up to units,

like $a+bi = (1+i)^c \left(\pi_1^{i_1}\bar{\pi}_1^{e_1-i_1}\right)\cdots\left(\pi_k^{i_k}\bar{\pi}_k^{e_k-i_k}\right) q_1^{d_1/2}\cdots q_\ell^{d_\ell/2}$

$0\le i_1\le e_1$ $\quad\cdots\quad$ $0\le i_k\le e_k$



---

e.g. $50 = 2^1\cdot 5^2$ with $5=(2+i)(2-i)$

$= a^2+b^2 = (a+bi)(a-bi)$ where $a+bi = (1+i)^1(2+i)^2(2-i)^0 = -1+7i$

$= (1+i)^1(2+i)^1(2-i)^1 = 5+5i$

$= (1+i)^3(2+i)^0(2-i)^1 = 7-i$

There are e_j+1 choices for $i_j \in \{0,1,2,\dots,e_j\}$,

and then 4 choices for a unit to multiply $a+bi$, giving $4\prod_{j=1}^{k}(e_j+1)$ total ∎