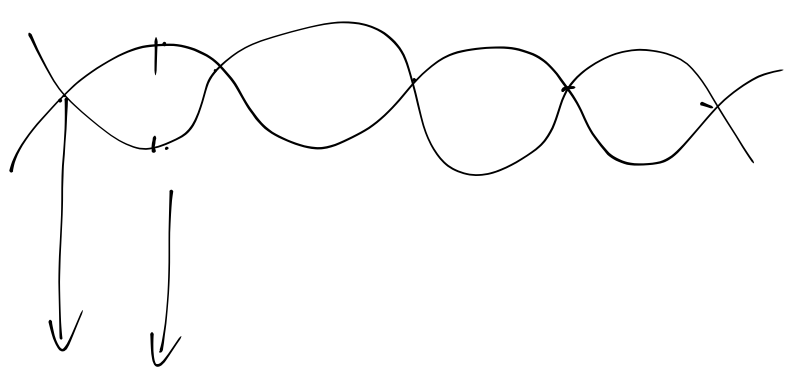
Conclusion: $p = m^2 + n^2$ has solutions $m, n \in \mathbb{Z}$ iff

$$p \equiv 1 \pmod 4.$$

Prime elements in $\mathbb{Z}[i]$.




$p \equiv 1 \pmod 4$

$p' \equiv 3 \pmod 4$

$p' \in \mathbb{Z}$. $p' \equiv 3 \pmod 4$. then $p'$ is still prime in $\mathbb{Z}[i]$

$p \in \mathbb{Z}$. $p \equiv 1 \pmod 4$. then $p = a^2 + b^2$

$= (a+bi)(a-bi)$

Such $a+bi$ are prime elements.

$(a+bi) = (c+di)(e+fi)$

$\Rightarrow \quad a^2+b^2 = (c^2+d^2)(e^2+f^2)$

$\Rightarrow \quad c^2+d^2$, or $e^2+f^2 = 1$

((aim:

If $a+bi$ is a prim element.

then $a^2+b^2$ must be a prime number.

$a^2+b^2 = p_1 p_2 \cdots p_m$

$(a+bi)(a-bi) = p_1 p_2 \cdots p_m$.

$a+bi$ prime $\Rightarrow$ $a-bi$ prime in $\mathbb{Z}[i]$.

So $m = 1$ or $2$.

$m=1$, then $(a+bi)(a-bi) = p_1 \Rightarrow a^2+b^2 = p_1$.

$m=2$. then $(a+bi)(a-bi) = p_1 p_2$.

$a+bi$ associate with $p_1$.

so $a+bi = \pm p_1 \cdot \pm p_1 i$.

or $a+bi = \pm p$

$\pm pi$.

$p \equiv 3 \pmod 4$

Field extension.

$\varphi: F \to F'$. $F$, $F'$ fields.

$\varphi$ hom. $\varphi$ is inj or 0. (why?!)

So the only interesting ring homs between fields are injective.

In which we can view $F$ as a subring of $F'$.

Field extension. $F \subset F'$ subfield. $F'/F$.

$F'/F$

$F'$ is an extension of $F$.

Ex: $\mathbb{Q} \hookrightarrow \mathbb{Q}(i)/(x^2+1)$.

Ex: $\mathbb{Q} \hookrightarrow \mathbb{C}$.

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

Ex: $G \hookrightarrow G(\bar{f}) = \left\{ \frac{f(\bar{f})}{g(\bar{f})} \mid f, g \in F(\bar{f}), g \neq 0 \right\}$

Two different extensions.

Transcedental.

Algebraic element.

Algebraic element $\alpha$ over $F$.

$\exists f(x) \neq 0 \in F(x)$. s.t. $f(\alpha) = 0$.

then $\alpha$ is algebraic. otherwise transcedental

relation to: $\varphi: F(\bar{x}) \to K$.

$x \mapsto \alpha$.

Two possibility. $\ker \varphi = (0)$.

or $\ker \varphi = (f(x))$

$F(\bar{x})/(f(x)) \hookrightarrow k$ is a subring in $k$.

So it has no zero divisor

So $F(\bar{x})/(f(x))$ is an integral domain

$f(x)$ is prime element, irreducible polynomial

Such monic $f(x)$ is called the irreducible polynomial of $\alpha$ in $F$.

① $f(\alpha) = 0$

② If $g(\alpha) = 0$, $g(x) \in F(\bar{x})$, then $f(x) | g(x)$

Corollary:

$F(\alpha) = \{ g(\alpha) \mid g \in F(\bar{x}) \} \hookrightarrow k$

is a <u>subfield</u>

Defn. $k/F$ is algebraic iff $\forall \alpha \in k$, $\alpha$ is algebraic over $F$.

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

If $\alpha$ is algebraic, then

$$F(\alpha) = F[\alpha].$$

Prop: $f(x)$ is irreducible polynomial of $\alpha$ in $F$, then $F[\alpha] = F(\alpha)$ and has a basis $(1, \alpha, \ldots \alpha^{n-1})$ as a vector space over $F$.

pf: $F[\alpha]$ is already a field, so $g(\alpha) \neq 0$.

$$(g(\alpha))^{-1} \in F[\alpha].$$

$$F[\alpha] = F(\alpha).$$

basis from the statement about adjoining elements in a ring.

Defn deg of extension. $K/F$

$$[K:F] = \dim_F K$$

Prop: If $[K:F]$ is finite, then $K$ is algebraic extension over $F$.

Pf: $\forall \alpha \in K$,

$$1, \alpha, \alpha^2, \cdots \alpha^{n-1}, \alpha^n$$

must be linear dependent for large $n$.

So $a_0 + a_1\alpha + \cdots a_n\alpha^n = 0$.

for some $(a_0, \cdots a_n) \in F^n$

$\neq (0, \cdots 0)$

$f(x) = a_0 + a_1 x \cdots a_n x^n$ has a root $x = \alpha$.