u_n is an LRS of order 2.

$$u_{n+2} = c_1 u_{n+1} + c_2 u_n$$

$c_1, c_2 \in \mathbb{Q}$

$u_0, u_1 \in \mathbb{Q}$

$$x^2 - c_1 x - c_2 = 0$$

$\lambda_1, \lambda_2 \in \overline{\mathbb{Q}}$ roots.

$\lambda_1 \neq \lambda_2$

$$u_n = a_1 \lambda_1^n + a_2 \lambda_2^n$$

where $a_1, a_2 \in \overline{\mathbb{Q}}$

$\lambda_1 = \lambda_2$

$$u_n = a_1 n \lambda_1^n + a_2 \lambda_2^n .$$

$\langle u_n \rangle$

$\exists n.\ u_n = 0$?

$u_n = a n \lambda^n + b \lambda^n$

$u_n = 0 \iff$

$a n \lambda^n + b \lambda^n = 0$

$a n + b = 0$

$a, b \in \overline{\mathbb{Q}} \cap \mathbb{Q}$

Just solve ...

$u_n = a_1 \lambda_1^n + a_2 \lambda_2^n$

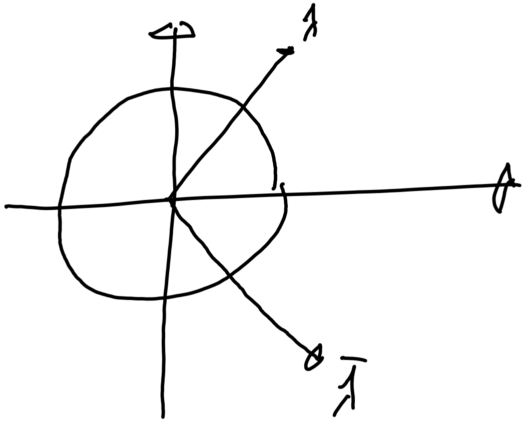
$\lambda_1, \lambda_2 \in \mathbb{R}$

$|\lambda_1| > |\lambda_2|$

$a_1 \lambda_1^n = -a_2 \lambda_2^n$

$-\frac{a_1}{a_2} = \left(\frac{\lambda_2}{\lambda_1}\right)^n$ so place bound on n.

$$u_n = a\lambda^n + \bar{a}\bar{\lambda}^n .$$



$$u_n = 0$$

$$a\lambda^n + \bar{a}\bar{\lambda}^n = 0$$

$$\iff$$

$a\lambda^n$ lies on the imaginary axis.

Let $\gamma = \dfrac{\lambda}{|\lambda|}$ $\quad |\gamma| = 1$

$$\frac{u_n}{|\lambda|^n} = 0 \iff u_n = 0$$

$$\frac{w_n}{|\lambda|^n} = a\gamma^n + \bar{a}\,\bar{\gamma}^n$$

$a\gamma^n$ lies on the imaginary axis $\iff w_n = 0$

$\iff a\gamma^n = ic \qquad c \in \mathbb{R}$

$\iff \gamma^n = \frac{ic}{a} \qquad \left|\frac{c}{a}\right| = 1$

$\gamma^n = \beta$ where β is some algebraic number

$\beta \in \overline{\mathbb{Q}} \qquad |\beta| = 1.$

Need to solve:

Given $\alpha, \beta \in \overline{\mathbb{Q}}$,
determine if $n \in \mathbb{N}$ s.t.
$\alpha^n = \beta$.

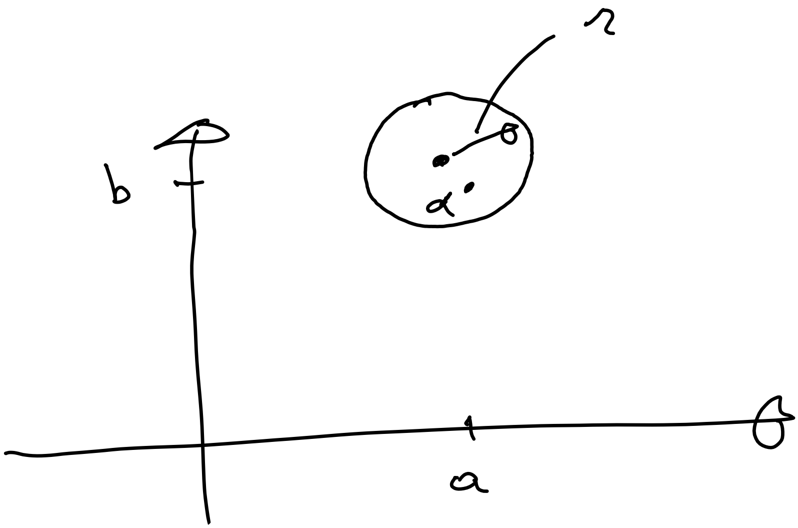
Computing with Algebraic Numbers

Represent algebraic numbers α as follows

(p, a, b, r), where
$p \in \mathbb{Q}[x]$ is the minimal polynomial of α

$a, b, r \in \mathbb{Q}$ s.t.

α is the unique root of p within r of $a+bi$.



If $p(x) = a_0 + a_1 x + \dots + a_t x^t$

$\deg(p) = t$

$\text{Height}(p) = H(p) =$

$\max\{|a_0|, \dots, |a_t|\}$

Theorem (Mignotte)

If $\alpha, \beta \in \overline{\mathbb{Q}}$ roots of p, then ($\alpha \neq \beta$)

$$|\alpha - \beta| > \frac{\sqrt{6}}{d^{\frac{d+1}{2}} \cdot H^{d-1}}$$

Claim:
Given canonical representations of $\alpha, \beta \in \overline{\mathbb{Q}}$, one can compute canonical representations of $\alpha + \beta$, $\alpha \cdot \beta$, $1/\alpha$, $\sqrt[k]{\alpha}$, α^k, ...

$\alpha^n = \beta$ for some $n \in \mathbb{N}$?

$\exists n \quad \alpha^n = 1$?

If α is r.o.u. then

α is a root of

$x^r - 1$.

$$\deg(\alpha) > \frac{r}{283 \log \log r}$$

so can check....

Place ~~bound~~ bound on

maximum value of

r, then check

$\alpha^n = 1$ for $n = 1, 2, \ldots$

bound.

$\exists n \ \alpha^n = \beta$?

Algebraic integer:
Algebraic number
root of a polynomial
$p \in \mathbb{Z}[x]$ s.t. leading
coeff. is 1.

$$p(x) = x^d + a_1 x^{d-1} + \dots + a_d$$

where $a_1, \dots, a_d \in \mathbb{Z}$.

$\mathcal{O}$ = ring of alg.
integers.

Want unique factorization
via theory of ideals.

An ideal I is a set of algebraic integers closed under addition and multiplication by alg. integers.

$I \subseteq \mathcal{O}$ is an ideal $\iff$

$I \neq \emptyset$

$\alpha, \beta \in I \Rightarrow \alpha + \beta \in I$

$\alpha \in I \quad r \in \mathcal{O} \Rightarrow$

$r \cdot \alpha \in I.$

A, B are ideals

$A \cdot B = [\alpha \cdot \beta \mid \alpha \in A, \beta \in B]$

For any $\alpha \in \mathcal{O}$

$$[\alpha] = P_1 \cdot \ldots \cdot P_k$$

where $P_1, \ldots, P_k$ are prime ideals, and this is unique up to order.

P is a prime ideal

$\iff$

$P = A \cdot B$, $P = A$ or $P = B$.

$$v_p : \mathcal{O} \setminus \{0\} \longrightarrow \mathbb{N}$$

$$[\alpha] = p_1^{k_1} \dots p_r^{k_r}$$

$$v_p(\alpha) = \begin{cases} k_i & \text{if } p = p_i \\ 0 & \text{if } p \notin \{p_1, \dots, p_r\} \end{cases}$$

$\alpha \neq 0$

$$v_p(0) = \infty$$

$$v_p : \overline{\mathbb{Q}} \longrightarrow \mathbb{Z}$$

$\alpha \in \overline{\mathbb{Q}}$ $\quad \exists\ \beta \in \mathcal{O}$ s.t.

$\alpha = \dfrac{\beta}{m}$ for some $m \in \mathbb{Z}$.

$$v_p(\alpha) = v_p(\beta) - v_p(m)$$

$\exists n \ \alpha^n = \beta$.

Let $\alpha \in \mathcal{O}$

Let $p \in \mathbb{Q}[x]$ be the minimal polynomial of α.

Let $\alpha_1, \ldots, \alpha_d$ be the roots of p.

Let $\alpha = \alpha_1$. Then $\alpha_2, \ldots, \alpha_d$ are the Galois conjugates of α.

For each $i \in \{2, \ldots, d\}$ there is a field isomorphism $\sigma_i : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ s.t.

$\sigma_i(\alpha) = \alpha_i$.

Sp. that

$|\alpha_1|, \ldots, |\alpha_d| \leq 1$.

Then α is a r.o.u.

(In other words,

if α is <u>not</u> a r.o.u.

then some Galois

conjugate of α

has modulus > 1.)

[Kronecker]

$\exists\, n \quad \alpha^n = \beta \quad (\alpha, \beta \in \overline{\mathbb{Q}})$

$|\alpha| \neq 1. \quad \boxed{\alpha \in \sigma}$

Place ~~bound~~ on n
and check manually.....

$|\alpha| = 1$, first check if
α is a r.o.u.

$|\alpha| = 1$, α is <u>not</u> a r.o.u.

Then $\exists\, \alpha'$ Galois conj.
of α s.t. $|\alpha'| > 1$.

σ field isomorphism

$\sigma(\alpha) = \alpha'$

$$\alpha^n = \beta \iff \sigma(\alpha^n) = \sigma(\beta)$$
$$\iff (\sigma(\alpha))^n = \sigma(\beta)$$
$$\iff (\alpha')^n = \sigma(\beta) \ldots\ldots$$

$|\alpha| = 1, \quad \alpha \notin \mathcal{O}$

$\alpha = \dfrac{\gamma}{m} \qquad m > 1$

there is some ideal P

$v_P(\alpha) \neq 0$

$v_P(\alpha) = v_P(\gamma) - v_P(m).$

$\alpha^n = \beta$

$v_P(\alpha^n) = v_P(\beta)$

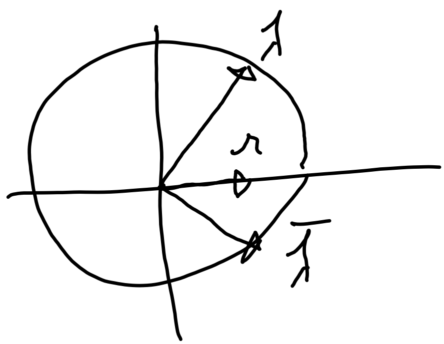
$n \cdot v_P(\alpha) = v_P(\beta)$

Places a bound on n $\checkmark$

.....

$\blacksquare$

SKOLEM at ORDER $\underline{3}$



$\lambda \in \overline{\mathbb{Q}}$

$r \in \mathbb{R} \cap \overline{\mathbb{Q}}$

$|\lambda| = |\bar{\lambda}| = 1$, $r < 1$

$\lambda, \bar{\lambda}, r$ are the char. roots.

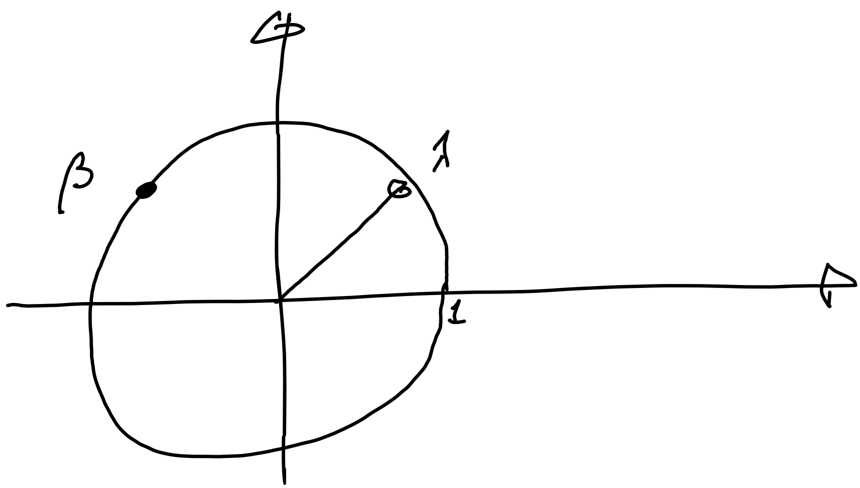
$$u_n = a\lambda^n + \bar{a}\bar{\lambda}^n + b r^n.$$

$\exists n .\ u_n = 0$?

Let $\beta \in \overline{\mathbb{Q}}$ s.t.

$$a\beta + \bar{a}\bar{\beta} = 0.$$

If $u_n = 0$ and n is "large", then $|r^n|$ is "small" so $|\lambda^n - \beta|$ must be "small".



Baker's Theorem says that if $\lambda^n \neq \beta$, then

$$|\lambda^n - \beta| > \frac{C}{P(n)}$$

where $C > 0$ and $P \in \mathbb{Z}[x]$

Because λ is not a r.o.u., $\lambda^n = \beta$ can happen at most <u>once</u>.

You can check, for that value of n, whether $u_n = 0$. Sp. not.

$\lambda^n \neq \beta$

$$|\lambda^n - \beta| > \frac{c}{p(n)}$$

Because $b \cdot r^n \to 0$ exp. fast, eventually $|b r^n| << \frac{c}{p(n)}$ for all suff. large n.

So for n larger than this bound

$$|u_n| = |a \lambda^n + \bar{a} \bar{\lambda}^n + b r^n| > 0.$$

$A \in \mathbb{Q}^{d \times d}$

~~states~~ $1, \ldots, d$

$(\underline{1}, 0, \ldots, 0)$

$$(1, 0 \ldots 0) A^n \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \underline{1} \end{pmatrix} = u_n$$

$\langle u_n \rangle$ is an LRS.

Halt if $u_n = 0$

```
x := a
WHILE u·x ≠ 0 DO

      x := Ax
```

Does this loop halt?

$\exists n \quad u \cdot A^n a = 0$?