§1 Euclidean rings

Motivation: Provides a criterion for being a PID.

Def Ring A euclidean $\underset{def}{=}$ A domain and

$\exists\ \deg : A \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ s.th.

$\forall\ a, b \in A \setminus \{0\}$ $\exists\ q, r \in A$ with $a = qb + r$ and

$$r = 0 \quad \text{or} \quad \deg(r) < \deg(b).$$

Prop 1 Every euclidean ring is a PID.

Proof (Euclidean Algorithm): Assume A euclidean w.r.t. deg, let $\mathfrak{a} \subseteq A$ any ideal. If $\mathfrak{a} = (0)$, we are done. Otherwise, let $0 \neq b \in \mathfrak{a}$ be s.th. $\deg(b) = \min \{ \deg(a) \mid 0 \neq a \in \mathfrak{a} \}$.

Claim: $\mathfrak{a} = (b)$.

Indeed, for $0 \neq a \in \mathfrak{a}$, let q, r be s.th.

$$a = q \cdot b + r, \quad r = 0 \quad \text{or} \quad \deg(r) < \deg(b).$$

Then $r = a - qb \in \mathfrak{a}$ and hence $r = 0$ by minimality of $\deg(b)$.

Thus $a = qb \in (b)$ as claimed. $\square$

Let A be one of the rings $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$

(The minimal polynomial of $\frac{1+\sqrt{-3}}{2}$ is $T^2 - T + 1$, hence $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \cong \mathbb{Z}[T]/(T^2-T+1)$.)

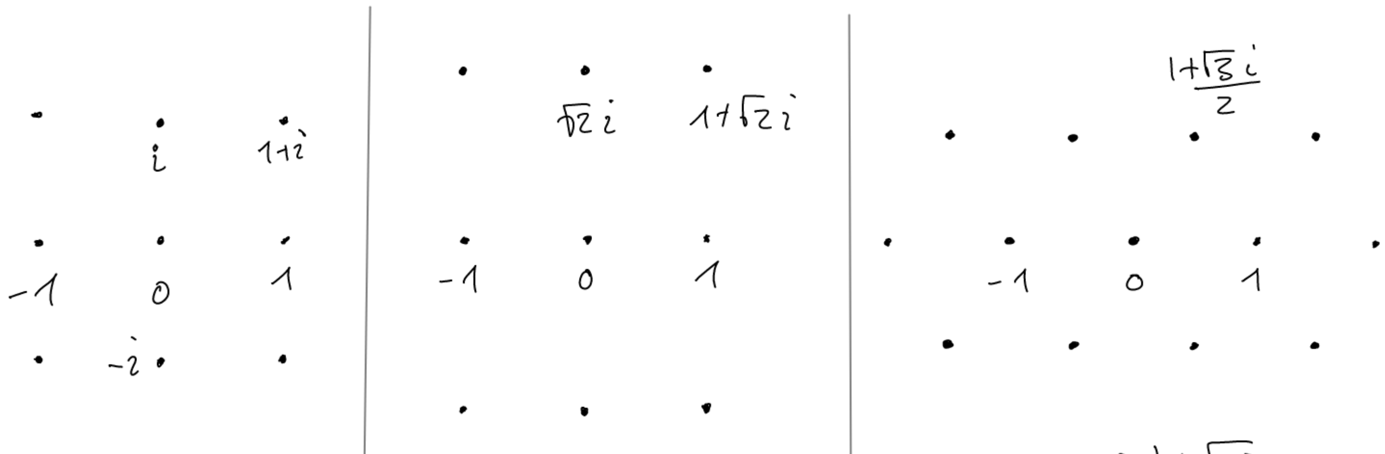
Then A is a subring of $K = \mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-3})$, in ptic. a domain.

The norm $N: K \longrightarrow \mathbb{Q}$, $a + b\sqrt{-n} \longmapsto a^2 + n \cdot b^2$ restricts to a function

$$N : A \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}.$$

<u>Prop 2</u> A is euclidean w.r.t. N. In ptic, A is a PID.

<u>Proof</u> Pick a field embedding $\varphi : K \hookrightarrow \mathbb{C}$. Then $\varphi(A)$ is the lattice $\mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \alpha$, $\alpha = i, \sqrt{2}i$ or $\frac{1+\sqrt{3}i}{2}$



$\mathbb{Z}[i]$ $\qquad$ $\mathbb{Z}[\sqrt{-2}]$ $\qquad$ $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

Moreover, $N(a) = \|\varphi(a)\|^2$ ← complex abs value

Observation $z \in \mathbb{C}$ any. Then there exists $z_0 \in \varphi(A)$ s.th. $\|z - z_0\|^2 < 1$. (This is specific to these rings!)

Proof of euclidean property: $a, b \in A \setminus \{0\}$ any.

$z := \varphi(a)/\varphi(b)$, $z_0 = \varphi(q) \in \varphi(A)$ s.th. $\|z - z_0\|^2 < 1$.

$q = \varphi^{-1}(z_0)$, $r = a - qb$.

Then
$$
\begin{aligned}
N(a-qb) &= \|\varphi(a-qb)\|^2 \\
&= \|\varphi(a) - \varphi(q)\varphi(b)\|^2 \\
&= \|\varphi(b)\|^2 \cdot \|z - z_0\| \\
&< \|\varphi(b)\|^2 = N(b). \qquad \square
\end{aligned}
$$

Rmk Being euclidean is a strong property that is only satisfied by some PIDs.

Cor 3 $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ have unique prime factorization.

Question addressed next: How to determine prime elements in these rings?

§2 Computing primes

<u>Setting</u> $A = \mathbb{Z}[T]/(f)$ with $f \in \mathbb{Z}[T]$ monic.

<u>Aim</u> Determine $\operatorname{MaxSpec}(A) := \{ m \subset A \text{ max ideal} \}$.

<u>Lem 4</u> $m \subset A$ any max ideal. Then $m \cap \mathbb{Z} = (p)$ for some prime numbes $p \in \mathbb{Z}$.

<u>Proof</u> 1st lecture: $A \cong \bigoplus_{i=0}^{\deg(f)-1} \mathbb{Z}$ as ab. grp.

2nd lecture: A/m is a field.

Existence of projection $A \to A/m$ then implies that A/m is a fin. gen. ab grp.

<u>Recall</u> k field. Then the unique ring map $\mathbb{Z} \to k$ is either injective or has image $\mathbb{F}_p$ for some prime p.

In first case, k contains $\mathbb{Q}$ because it contains $\frac{1}{n}$ $\forall n \in \mathbb{Z}_{>0}$.

<u>Terminology</u> k called of characteristic 0 or p correspondingly.

Back to A/m: Since $\mathbb{Q}$ does not embed in any fin. gen. abelian group, A/m has to be of characteristic p for some prime p, meaning $m \cap \mathbb{Z} = (p)$. $\square$

Refined aim: Given prime $p \in \mathbb{Z}$. What are the max ideals $m \subset A$ s.th. $m \cap \mathbb{Z} = (p)$?

Observations (1) A any ring, $\mathfrak{a} \subseteq A$ ideal. Then

$$\mathrm{MaxSpec}(A/\mathfrak{a}) = \{\text{max ideals } m \subset A \text{ s.th. } \mathfrak{a} \subseteq m\}.$$

$$\bar{m} \longmapsto \pi^{-1}(\bar{m})$$

$$m/\mathfrak{a} \longleftarrow\!\shortmid\, m.$$

(2) $\mathfrak{a}, \mathfrak{b} \subseteq A$ ideals. Have $\mathfrak{a}+\mathfrak{b} := (\mathfrak{a} \cup \mathfrak{b})$ ideal generated by $\mathfrak{a}$ and $\mathfrak{b}$.

Example $(f_1, \dots, f_n) + (g_1, \dots, g_m) = (f_1, \dots, f_n, g_1, \dots, g_m)$

Put $\bar{\mathfrak{a}} := \mathfrak{a}+\mathfrak{b}/\mathfrak{b} \subseteq A/\mathfrak{b}$

$\bar{\mathfrak{b}} := \mathfrak{a}+\mathfrak{b}/\mathfrak{a} \subseteq A/\mathfrak{a}$.

Then, by Noether isomorphism Thm,

$$(A/\mathfrak{a})/\bar{\mathfrak{b}} \cong A/\mathfrak{a}+\mathfrak{b} \cong (A/\mathfrak{b})/\bar{\mathfrak{a}}$$

(3) $\mathfrak{a} \subseteq A$ ideal, $\pi : A \longrightarrow A/\mathfrak{a}$ projection and

$\overline{\mathfrak{b}} = (g_1, \dots, g_m) \subseteq A/\mathfrak{a}$ any ideal.

Pick any $\tilde{g}_i \in A$ s.th. $\pi(\tilde{g}_i) = g_i$. Then

$$\pi^{-1}(\overline{\mathfrak{b}}) = \mathfrak{a} + (\tilde{g}_1, \dots, \tilde{g}_m)$$

<u>Application to $A = \mathbb{Z}[T]/(f)$</u>

$\{ \mathfrak{m} \subset A$ s.th. $\mathfrak{m} \cap \mathbb{Z} = (p) \}$

$\overset{\text{Lem 4}}{=} \{ \mathfrak{m} \subset A$ s.th. $p \cdot A \subseteq \mathfrak{m} \}$

$\overset{(1)}{=} \operatorname{Max\,Spec}(A/pA)$

$\overset{(1)+(3)}{=} \operatorname{Max\,Spec}\left(\mathbb{Z}[T]/(p,f) \right)$

$$\overset{(2)}{=} \operatorname{Max\,Spec}\Big(\underbrace{\left(\mathbb{Z}[T]/p\mathbb{Z}[T] \right) / (\overline{f})}_{= \mathbb{F}_p[T]/(\overline{f})} \Big) \qquad \overline{f} := f \bmod (p)$$

$\overset{(1)}{=} \{ (\overline{h}_i) \mid \overline{h}_i \in \mathbb{F}_p[T]$ irreducible, $\overline{h}_i \mid \overline{f} \}$

$$(1)+(3) \;\Longrightarrow\; \{ (p, h_i) \subset A, \quad h_i \text{ image in } A \text{ of } \tilde{h}_i \in \mathbb{Z}[T] \text{ lifting } \bar{h}_i \text{ from before.} \}.$$

Summary

$$\begin{tikzcd}
\left\{ \begin{array}{c} \mathfrak{m} \subset A \text{ max ideals} \\ \text{s.th. } \mathfrak{m} \cap \mathbb{Z} = (p) \end{array} \right\} \arrow[d, leftrightarrow, "1:1"] & (p, h_i) \\
\left\{ \begin{array}{c} \text{irred. monic factors} \\ \bar{h}_i \mid \bar{f} \text{ in } \mathbb{F}_p[T] \end{array} \right\} & \bar{h}_i \arrow[u, mapsto]
\end{tikzcd}$$

$$\begin{tikzcd}
 & & \mathbb{Z}[T] \arrow[dll] \arrow[drr] & & \\
 & & \tilde{h}_i \arrow[dl, mapsto] \arrow[dr, mapsto] & & \\
A & h_i & & \bar{h}_i & \mathbb{F}_p[T]
\end{tikzcd}$$

§3 Sums of squares

<u>Thm 5</u> (Fermat, Euler 1758) Let p be a prime. Then

$$p = x^2 + y^2 \text{ for some } x, y \in \mathbb{Z} \iff p \equiv 1, 2 \mod (4)$$

<u>Proof</u> $\Rightarrow$ $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 0$, $3^2 \equiv 1 \mod 4$,

so a sum $x^2 + y^2$, $x, y \in \mathbb{Z}$, is $\equiv 0, 1, 2 \mod 4$.

$\Leftarrow$ This is the difficult statement. Our proof will use crucially that $\mathbb{Z}[i]$ is a PID.

<u>Step 1</u> Compute $\operatorname{MaxSpec}(\mathbb{Z}[i])$: By previous §,

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[T]/(p, T^2+1) \cong \mathbb{F}_p[T]/(T^2+1).$$

<u>Lem</u>

$$T^2+1 \equiv \begin{cases} (T+1)^2 & \mod (2) \\ (T-\alpha)(T+\alpha) & \mod (p) \text{ if } p \equiv 1 \ (4) \\ \quad \text{here } \alpha \in \mathbb{F}_p^\times \text{ is s.th. } \alpha^2 = -1 & \\ \text{irreducible} & \mod (p) \text{ if } p \equiv 3 \ (4). \end{cases}$$

<u>Proof</u> $p = 2$ case ok. Assume $p \neq 2$. Then $\mathbb{F}_p^\times$ cyclic

of order $p-1$. Let ξ be generator, i.e. of exact order $p-1$. Then $\xi^{(p-1)/2} \neq 1$ and $\left(\xi^{(p-1)/2}\right)^2 = 1$. Thus $\xi^{(p-1)/2} = -1$ since the solutions of T^2-1 are exactly $\{\pm 1\}$. Then

T^2+1 has zero α in $\mathbb{F}_p$ $\iff$ can write $\xi^{(p-1)/2} = (\xi^k)^2$

$\iff$ $(p-1)/2$ is even

$\iff$ $p \equiv 1 \mod (4)$. $\square$ Lemma

Hence $\operatorname{MaxSpec}(\mathbb{Z}[i]) =$

$$\coprod_{\substack{p \in \mathbb{Z}_{>0} \\ \text{prime}}} \begin{cases} (2, i+1) & p = 2 \\ (p, i-\alpha),\ (p, i+\alpha) \\ \text{where } \alpha \in \mathbb{Z},\ \alpha^2 \equiv -1\ (4) & p \equiv 1\ (4) \\ (p) & p \equiv 3\ (4). \end{cases}$$

<u>Step 2</u> Since $\mathbb{Z}[i]$ is a PID (!), every $\mathfrak{m}$ has form (π) for prime element $\pi \in \mathbb{Z}[i]$.

Assume $(\pi) \cap \mathbb{Z} = (p)$ with $p \equiv 1$ or $2 \mod (4)$.

Then $(p) \subsetneq (\pi)$ because $\pi \neq 0$ in $\mathbb{F}_p[T]/(T^2+1)$. (It generates an ideal $(T-a)$ for $(T-a) \mid (T^2+1)$.)

$\Rightarrow$ $\pi \mid p$ <u>properly</u> in $\mathbb{Z}[i]$, meaning $p/\pi \notin \mathbb{Z}[i]^\times$.

Write $\pi = x+iy$. Then $N(\pi) = x^2+y^2$.

<u>Claim</u> $N(\pi) = p$.

<u>Proof</u> $N(\pi) \in \{1, p, p^2\}$ because $N(\pi) \mid N(p) = p^2$.

Observe that $u \in \mathbb{Z}[i]^\times \iff N(u) = 1$.

Since π, p/π are no units, $N(\pi) = p$. ∎

<u>Claim + Thm</u>

<u>Exercise</u> Use that $\mathbb{Z}[i]$ is a PID to prove:

$$n = x^2+y^2 \iff \left\{ \begin{array}{l} \text{Let } n = p_1^{e_1} \cdots p_r^{e_r} \quad p_i \neq p_j \text{ for } i \neq j \\ \text{be prime factorization of } n. \\ \text{Then } p_i \equiv 3 \ (4) \Rightarrow e_i \text{ even.} \end{array} \right.$$

<u>Rmks</u> 1) Thm 5 has analog for $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

For $\mathbb{Z}[\sqrt{-2}]$:

$$p = x^2 + 2y^2 \iff p \equiv 1, 2, 3 \mod (8).$$

2) Historically, this example + attempts of generalization were an important driver in the development of commutative algebra.

3) Solving $p = x^2 + ny^2$ or $m = x^2 + ny^2$ for larger n requires class field theory and is much more difficult. See the nice book "Primes of the form $x^2 + ny^2$" by Cox.

Finally some example factorizations:

Prime $p \in \mathbb{Z}_{>0}$	in $\mathbb{Z}[i]$	in $\mathbb{Z}[\sqrt{-2}]$
2	$-i(1+i)^2$	$-\sqrt{-2}^{\,2}$
3	prime	$(1+\sqrt{-2})(1-\sqrt{-2})$
5	$(1+2i)(1-2i)$	prime
7	prime	prime