III.H. Principal ideal domains

Let R be a commutative domain.

III.H.1. DEFINITION. R is a **principal ideal domain (PID)** if every ideal $I \subseteq R$ is principal.

Regardless of whether R is a PID, note that we have

$$\text{(III.H.2)} \qquad \begin{cases} r \mid s & \iff \quad (r) \supseteq (s) \\ r \sim s & \iff \quad (r) = (s) \end{cases}$$

for $r, s \in R$.

III.H.3. EXAMPLES (of PIDs).
(A) $R = \mathbb{Z}$ (consider the additive subgroups).
(B) Euclidean domains (which of course includes (A)).
(C) $\mathbb{F}[x]$ ($\mathbb{F}$ any field), $\mathbb{Z}[\mathbf{i}]$, and $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$ (HW) are Euclidean, hence PIDs by (B).
(D) $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, while non-Euclidean (HW), is a PID.

PROOF OF (B). Given $I \subseteq R$ an ideal in a Euclidean domain R, let $\beta \in I\backslash\{0\}$ be of minimal $\delta(\beta)$ ($\in \mathbb{N}$), and take $\alpha \in I$ to be arbitrary. Then

$$\alpha = \beta q + r \quad (q, r \in R)$$

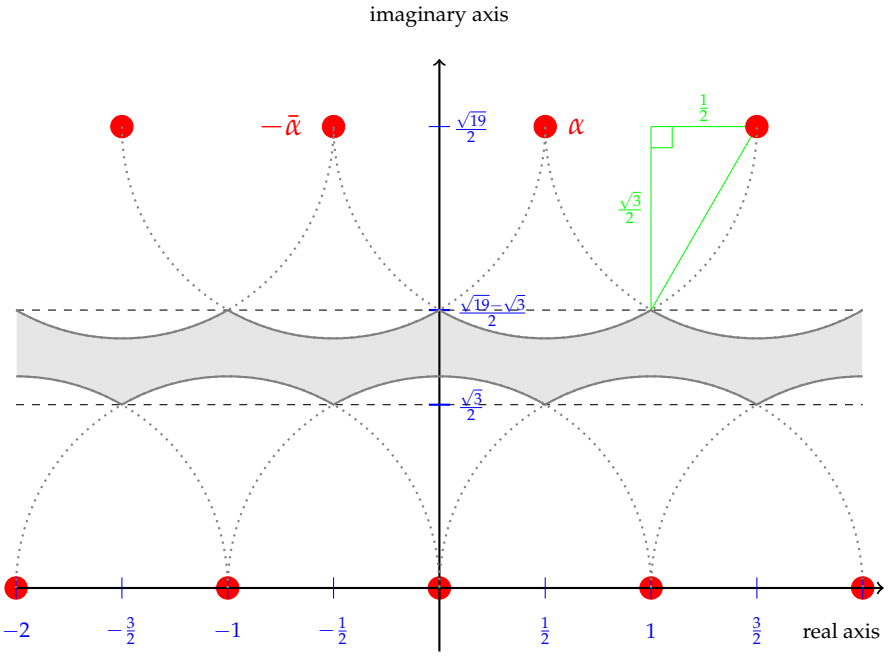
with (i) $\delta(r) < \delta(\beta)$ and $r = \alpha - \beta q \in I\backslash\{0\}$, or (ii) $r = 0$. Since (i) contradicts minimality of $\delta(\beta)$, we have (ii) and $\alpha = \beta q \in (\beta) \implies I \subseteq (\beta)$. Since $\beta \in I$, we have $(\beta) \subseteq I$; thus $I = (\beta)$ is principal. □

PROOF OF (D). Write $\alpha := \frac{1+\sqrt{-19}}{2}$ and $R := \mathbb{Z}[\alpha]$. Let I be any nonzero ideal of R, and take $x \in I\backslash\{0\}$ of minimal norm $x\tilde{x} = |x|^2$ (i.e. minimal $|x|$). We will show that $I = xR\,(= (x))$. Equivalently, working in the field of fractions $K = \mathbb{Q}[\alpha]$, we can try to show that the fractional ideal $J := x^{-1}I$ is R. (Clearly, from $I \supset xR$ we have $J \supset R$.)

Step 1 *Any element $\gamma \in J\backslash R$ has imaginary part $\Im(\gamma)$ differing from any integral multiple of $\frac{\sqrt{19}}{2}$ by at least $\frac{\sqrt{3}}{2}$, i.e. $\Im(\gamma) \in [\frac{\sqrt{3}}{2}, \frac{\sqrt{19}-\sqrt{3}}{2}] + \frac{\sqrt{19}}{2}\mathbb{Z}$.*

Given $\gamma \in J$, suppose $|\gamma - r| < 1$ for some $r \in R$. Since $\gamma = x^{-1}r_0$ for some $r_0 \in I$, we have $1 > |x^{-1}r_0 - r| \implies |x| > |r_0 - rx|$. Since $|x|$ is minimal, $r_0 - rx \notin I\backslash\{0\}$. But $r_0 - rx \in I$ as $r_0, x \in I$. So the only possibility is for $r_0 - rx$ to be 0, i.e. $\gamma = x^{-1}r_0 = r \in R$.

Conclude that any $\gamma \in J\backslash R$ has $|\gamma - r| \geq 1$ ($\forall r \in R$). Representing elements of R in the complex plane by red dots, the following picture explains why the above claim holds:



since being outside the circles forces γ inside the union of translates of the grey strip by $\frac{\sqrt{19}}{2}\mathbf{i}\mathbb{Z}$. In fact, since we can translate (in $J\backslash R$) by elements of R, this shows: *if $J\backslash R \neq \emptyset$, then there exists $\gamma \in J\backslash R$ with $\Im(\gamma) \in [\frac{\sqrt{3}}{2}, \frac{\sqrt{19}-\sqrt{3}}{2}]$ and $\Re(\gamma) \in (-\frac{1}{2}, \frac{1}{2}]$.*

Step 2 *For such a γ, we have $\gamma = \frac{\alpha}{2}$ or $-\frac{\bar{\alpha}}{2}$.*

We have $\Im(2\gamma) \in [\sqrt{3}, \sqrt{19} - \sqrt{3}]$ and $\Re(2\gamma) \in (-1, 1]$. In particular, $\Re(2\gamma)$ is within $\frac{1}{2}$ of either $\frac{1}{2}$ or $-\frac{1}{2}$. Accordingly, either $|2\gamma - \alpha|^2$ or $|2\gamma + \bar{\alpha}|^2$ is

$$\leq (\tfrac{\sqrt{19}}{2} - \sqrt{3})^2 + (\tfrac{1}{2})^2 = 8 - \sqrt{57} < 8 - 7 = 1,$$

i.e. 2γ is within 1 of α or $-\bar{\alpha}$ — hence *cannot* be in $J \backslash R$ by Step 1.

Conclude that $2\gamma \in R$. But the only elements of R in the rectangle to which 2γ is confined are $\alpha, -\bar{\alpha}$. Hence $\gamma = \frac{\alpha}{2}$ or $-\frac{\bar{\alpha}}{2}$.

Step 3 *J does not contain either of these elements.*

Since J is closed under multiplication by elements of R, if $\gamma = \frac{\alpha}{2}$ or $-\frac{\bar{\alpha}}{2}$, then $\frac{\alpha\bar{\alpha}}{2} \in J$. But

$$\frac{\alpha\bar{\alpha}}{2} = \frac{\frac{1+\sqrt{-19}}{2} \cdot \frac{1-\sqrt{-19}}{2}}{2} = \frac{1+19}{8} = \frac{5}{2},$$

which is within 1 of an element (say, 3) of R *so cannot be in* $J \backslash R$. On the other hand, $\frac{5}{2} \notin R$. So $\frac{5}{2} \notin J$, a contradiction.

Thus there exists no $\gamma \in J \backslash R$; that is, $J = R$. Hence $I = (x)$ is principal as desired. □

III.H.4. EXAMPLES (of non-PIDs).

(A) $\mathbb{Z}[\sqrt{10}]$ is not a PID.

PROOF. Writing $I := (3, 1 + \sqrt{10})$, Hurwitz gives

$$I\tilde{I} = (3, 1 + \sqrt{10})(3, 1 - \sqrt{10}) = (\gcd(9, -9, 6)) = (3).$$

Suppose $I = (\beta)$ for some $\beta = a + b\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$. Then $(3) = I\tilde{I} = (\beta\tilde{\beta}) = (a^2 - 10b^2) \implies a^2 - 10b^2 \sim 3$. Since $\mathbb{Z}^* = \{\pm 1\}$, we get $a^2 - 10b^2 = \pm 3$, which by a recent HW problem is impossible. □

(B) $R[x]$, where R is a PID, need not be a PID. In particular, $\mathbb{F}[x, y]$ (for $\mathbb{F}$ a field) is not.

PROOF. Consider the proper ideal $I := \{\sum_{i,j} a_{ij} x^i y^j \mid a_{00} = 0\} = (x, y)$ in $\mathbb{F}[x, y]$. If $I = (f)$ then $f \mid x, y$.

Now I claim that x is irreducible. To show this, suppose $x = gh$. Since $\mathbb{F}[y]$ is a domain, the degrees (as polynomials in x over $\mathbb{F}[y]$) satisfy $\deg_x g + \deg_x h = 1$. Swapping g and h if needed, we have $\deg_x g = 0$ and $\deg_x h = 1$ hence $g \in \mathbb{F}^* = (\mathbb{F}[x, y])^*$ is a unit. Likewise, y is irreducible.

So $f = ax$ or a, for $a \in (\mathbb{F}[x,y])^* = \mathbb{F}^*$; *and* $f = by$ or b, with $b \in (\mathbb{F}[x,y])^* = \mathbb{F}^*$. Obviously then $f \in \mathbb{F}^*$, which gives $I = R[x,y]$, a contradiction. We conclude that I is not principal. □

(C) $\mathbb{Z}[x]$ is not a PID: consider $I = (3, x^3 - x^2 + 2x - 1)$ (HW) or, more simply, $I = (3, x)$.

(D) Two more non-examples are (i) $\mathbb{Z}[\sqrt{-17}]$ and (ii) $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$. I won't prove this, but rather just say where the argument in the proof of III.H.3(D) goes wrong: for (i), the bounding argument in Step 2 — i.e. getting $|2\gamma - \alpha|$ or $|2\gamma + \bar{\alpha}| < 1$ — fails because (viewed as a lattice) R is now too "spread out" vertically. For (ii), Step 2 still works, but $\frac{\alpha\bar{\alpha}}{2} = \frac{23+1}{8} = 3$ belongs to R hence fails to yield a contradiction.

We now turn to some remarks on principal ideals generated by irreducible elements. To begin, let R be a *commutative domain*, and $\alpha \in R\backslash\{0\}$. Notice that in general

$$\begin{aligned} \alpha \text{ irreducible} &\implies \alpha \notin R^* \implies \alpha \nmid 1 \\ &\implies (\alpha) \not\supseteq 1 \implies (\alpha) \in \mathcal{PP}, \end{aligned} \tag{III.H.5}$$

where "$\mathcal{PP}$" denotes the set of proper principal ideals of R.

III.H.6. THEOREM. *α is irreducible $\iff$ (α) is maximal in*[25] *$\mathcal{PP}$.*

PROOF. ($\implies$): Suppose $(\beta) \in \mathcal{PP}$ and $(\beta) \supseteq (\alpha)$. Then $\beta \notin R^*$ and $\alpha = \beta r$ (for some $r \in R$). Since α is irreducible, r must belong to R^*. So $(\alpha) = (\beta)$.

($\impliedby$): Let (α) be maximal in $\mathcal{PP}$, and write $\alpha = \beta\gamma$, with $\beta \notin R^*$. Then $(\beta) \in \mathcal{PP}$ and $(\beta) \supseteq (\alpha)$. By maximality of (α) in $\mathcal{PP}$, $(\beta) = (\alpha)$ hence we can write $\beta = \alpha\delta$. This gives $\alpha = \alpha\delta\gamma \implies \delta\gamma = 1 \implies \gamma \in R^*$. Thus α is irreducible. □

In general, for a principal ideal (α), "maximality in $\mathcal{PP}$" is quite a bit weaker than "maximality". Of course, when R is a PID these are equivalent, and we get the

[25] The RHS contains two assertions: $(\alpha) \in \mathcal{PP}$, and (α) is maximal there.

III.H.7. COROLLARY. *Let R be a PID, $\alpha \in R\backslash\{0\}$. Then*[26]

$$\alpha \text{ is irreducible} \iff (\alpha) \text{ is maximal amongst proper ideals.}$$

III.H.8. COROLLARY. *Let R be a PID, $\alpha \in R\backslash(R^* \cup \{0\})$. Then:*
(i) *$R/(\alpha)$ is a field $\iff$ α is irreducible; and*
(ii) *otherwise, $R/(\alpha)$ isn't a domain.*

PROOF. (i) Follows at once from III.H.7 and III.F.3.
(ii) If α is not irreducible, then there exist $\beta, \gamma \in R\backslash(R^* \cup \{0\})$ such that $\alpha = \beta\gamma$. Suppose $\beta \in (\alpha)$; then $\beta = \alpha r$ $(r \in R) \implies \alpha = \alpha r\gamma \implies r\gamma = 1 \implies \gamma \in R^*$, a contradiction.
So $\beta, \gamma \notin (\alpha) \implies \bar{\beta}, \bar{\gamma} \neq \bar{0}$ in $R/(\alpha)$ but $\bar{\beta}\bar{\gamma} = \bar{\alpha} = \bar{0}$. □

Now let $\mathbb{F}$ be a field and $S \supset \mathbb{F}$ a ring, with $u \in S$. Recall from III.G.3 the evaluation map $\mathrm{ev}_u : \mathbb{F}[x] \to S$ sending $x \mapsto u$, with image $=: \mathbb{F}[u]$, and kernel $=: I_u$. Since $\mathbb{F}[x]$ is a PID, $I_u = (g)$ for some $g \in \mathbb{F}[x]$, and $I_u \cap \mathbb{F} = \{0\} \implies g \notin \mathbb{F}^*\,(= \mathbb{F}[x]^*)$. If $g = 0$, then u is transcendental over $\mathbb{F}$; otherwise, $\deg(g) > 0$ and u is algebraic over $\mathbb{F}$.

Henceforth assume that u is algebraic; then as $\mathbb{F}$ is a field, we may also assume that g is monic. In fact, since any two generators of I_u are associate, this uniquely determines g.

III.H.9. DEFINITION. The (unique) monic generator m_u of I_u is called the **minimal polynomial** of u over $\mathbb{F}$.

III.H.10. LEMMA. *This m_u is the lowest-degree polynomial in $\mathbb{F}[x]\backslash\{0\}$ having u as a root.*

PROOF. $f(u) = 0 \implies f \in I_u = (m_u) \implies f = m_u q \implies \deg(f) \geq \deg(m_u)$ or $f = 0$. □

III.H.11. COROLLARY. *$\mathbb{F}[u]$ is a field $\iff$ m_u is irreducible in $\mathbb{F}[x]$. Otherwise, $\mathbb{F}[u]$ is not a domain.*

PROOF. Immediate from $\mathbb{F}[u] \cong \mathbb{F}[x]/I_u$ and III.H.8. □

[26] The RHS here means that (α) is a maximal ideal (in the standard sense).

III.H.12. REMARK. The following construction of $\mathbb{F}[u]$ appears tautological but is actually the most useful one. Let $g(x) \in \mathbb{F}[x]$ be a monic polynomial of positive degree; we put $S := \mathbb{F}[x]/(g(x))$ and $u := x + (g(x)) \in S$. Then the evaluation map $\mathrm{ev}_u \colon \mathbb{F}[x] \twoheadrightarrow \mathbb{F}[x]/(g(x))$ is just the natural map, with kernel $I_u = (g(x))$. Hence $\mathbb{F}[u] = \mathbb{F}[x]/(g(x))$, and $g(x) = m_u(x)$. The construction yields a field if and only if $g(x)$ is irreducible. Regardless of that, every element of $\mathbb{F}[u]$ can be written in exactly one way as a sum $\sum_{k=0}^{d-1} a_k u^k$ with $a_k \in \mathbb{F}$ and $d := \deg(g)$. This makes it a vector space over $\mathbb{F}$ of dimension d with basis $1, u, \ldots, u^{d-1}$.

This construction is important, for instance, when studying number fields. Let $\mathbb{F} = \mathbb{Q}$. Rather than starting with $u \in S = \mathbb{C}$ and sending x to that, we start with an irreducible polynomial and need never make any reference to $\mathbb{C}$. So to take one example, we can *define* $\mathbb{Q}[\sqrt{-3}] := \mathbb{Q}[x]/(x^2+3)$. This is both practically superior (when studying polynomials for which we don't know an "explicit" root) and theoretically superior (as we don't have to invoke the fundamental theorem of algebra). In $\mathbb{Q}[u] := \mathbb{Q}[x]/(g(x))$ one still thinks of u as an abstract root of g. If desired, we can map $\mathbb{Q}[u]$ into $\mathbb{C}$ in multiple ways by sending u to *any* root of g in $\mathbb{C}$.

III.H.13. EXAMPLE. I claim that $F = \mathbb{Q}[\theta] := \mathbb{Q}[x]/(x^3 - x + 2)$ is a field. Suppose otherwise; then $g := x^3 - x + 2$ is reducible, which means it has a linear and quadratic factor. The linear factor obviously would have a root $\frac{P}{Q} \in \mathbb{Q}$ (written in lowest terms). But

$$\tfrac{P^3}{Q^3} - \tfrac{P}{Q} + 2 = 0 \quad\Longrightarrow\quad Q = 1 \quad\Longrightarrow\quad P^3 - P + 2 = 0,\ P \in \mathbb{Z};$$

and reducing mod 5, multiplying by $\bar{P}$ and using $\bar{P}^4 = \bar{1}$ gives $\bar{1} - \bar{P}^2 + \bar{2}\bar{P} = \bar{0} \implies \bar{P}(\bar{P} - \bar{2}) = \bar{1}$. Since $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{3}$, $\bar{3}^{-1} = \bar{2}$, and $\bar{4}^{-1} = \bar{4}$, this is impossible.

As the polynomial has degree 3, F is a vector space over $\mathbb{Q}$ of dimension 3, with basis $1, \theta, \theta^2$. The field F is called a *cubic field*.