Thm. A PID is a UFD.

Proof: Let D be a PID, then each irreducible of D is a prime.

We only need to prove that each non-invertible elt of D is a product of finitely many irreducibles. (factor chain's uniqueness is guarenteed by 'prime')

Suppose a non-inv. elt. a is not a prod. of finitely many irr.

Then $a = a_1 b_1$ s.t. a_1 is not irr. (a_1, b_1 both non-inv.)

$a_1 = a_2 b_2$ a_2 is not irr.

$a_2 = a_3 b_3$ a_3 is not irr.

$\vdots$ $\vdots$

$a_i = a_{i+1} b_{i+1}$ a_{i+1} is not irr.

$\vdots$

Hence $(a) < (a_1) < (a_2) < \cdots < (a_i) < (a_{i+1}) < \cdots$

Let $I = (a) \cup (a_1) \cup \cdots \cup (a_i) \cup \cdots\cdots$

Then I is an ideal of D. Since D is a PID, $I = (b)$ and $b \in (a_i)$ for some i.

Thus $I = (b) \leq (a_i) < (a_{i+1}) < I$. a contradiction.

So each non-inv. elt of D is a prod. of finiteely many irr.

Then D is a UFD. $\square$

Upshot: UFD: ① irreducible $\equiv$ prime.

② each elt is a prod of finitely many irr.

Euclidean Domain

Recall: $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. as $6 = 2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$.

How about $\mathbb{Z}[\sqrt{-1}]$?

Def: Let D be an integral domain. A map

$$v: D \setminus \{0\} \longrightarrow \mathbb{Z}^+$$

is called a valuation if for any elts $x, y \in D$ with $y \neq 0$,

there exist $q, r \in D$ s.t. $x = qy + r$, with $r = 0$ or $v(r) < v(y)$.

(Can apply Euclidean algorithm in D).

Def. (ED). An ID is called a <u>Euclidean domain</u> if it has a valuation

Ex. ① $\mathbb{Q}[x]$ is a ED, with the degree being the valuation.

② $\mathbb{Z}$ is a ED.

Thm. A ED is a PID and a UFD.

Proof: Let D be a ED and let I be an ideal. ($I=\{0\}$ trivial. Let $I\neq\{0\}$).

Take non-zero $b\in I$ s.t $v(b)$ is the smallest. Then $I=(b)$.

In fact, let $a\in I$. Then $a,b\in I$. and there exist $q,r\in D$ s.t $a=qb+r$.

where $r=0$ or $v(r)<v(b)$. So $r=0$ and $a=qb$. i.e. $a\in(b)$. So $(b)=I$.

And D is a PID, and a UFD. $\square$.

Let $J=\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$, $i=\sqrt{-1}$.

Claim: J is a ED.

Proof of claim: Let $v(a+bi)=a^2+b^2$. We need to prove v is a valuation.

Let $x,y\in D$. with $y\neq 0$. Write $\frac{x}{y}=t+si$ with $t,s\in\mathbb{Q}$.

Let $q_1,q_2\in\mathbb{Z}$. s.t $|t-q_1|\leq\frac{1}{2}$, $|s-q_2|\leq\frac{1}{2}$.

Then, letting $q=q_1+q_2 i$, we have

$$v\left(\frac{x}{y}-q\right)=v\left((t-q_1)+(s-q_2)i\right)=(t-q_1)^2+(s-q_2)^2\leq\frac{1}{2}.$$

So $r:=x-qy$ is s.t.

$$v(r)=v(x-qy)=v\left(y\left(\frac{x}{y}-q\right)\right)\leq v(y)\,v\left(\frac{x}{y}-q\right)\leq\frac{1}{2}v(y)<v(y).$$

i.e. $x=qy+r$ with $v(r)<v(y)$. and v is indeed a valuation.

So J is a ED, a PID and a UFD. $\square$.

Upshot: ED $\to$ PID $\to$ UFD.

Polynomial rings over UFD

Let R be a UFD, and $f(x)\in R[x]$.

Def. ① the greatest common divisor of the coefficients of $f(x)$ is called the <u>capacity</u> of $f(x)$, denoted by $c(f)$.

e.g. $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. $c(f) = \gcd(a_0, \cdots, a_n)$.

② If $c(f) = 1$, then $f(x)$ is called <u>primitive</u>.

Lemma (Gauss Lemma). Let $f, g \in R[x]$, then $c(fg) = c(f)\, c(g)$.

If f, g primitive, so is fg.

Proof of lemma: Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. $g(x) = b_0 + b_1 x + \cdots + b_m x^m$.

Let $h(x) = f(x) g(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$.

Then $c_{i+j} = a_i b_j + a_{i-1} b_{j+1} + \cdots + a_0 b_{i+j} + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0$.

Let p be a prime s.t. $c(f)_p = p^k$, $c(g)_p = p^l$

Then $p^{k+l} \mid c(h)$. So $c(fg) \geq c(f)\, c(g)$.

The following arguement shows $c(fg) = c(f)\, c(g)$.

Assume f, g are prime. Suppose $p \mid c(fg)$, then there exist $i\,(0 \leq i \leq n)$ and $j\,(0 \leq j \leq m)$ s.t.

- p divides $a_0, a_1, \cdots, a_{i-1}$ but $p \nmid a_i$.
- p divides $b_0, b_1, \cdots, b_{j-1}$ but $p \nmid b_j$.

Then $c_{i+j} = a_i b_j + \underline{a_{i-1} b_{j+1} + \cdots + a_0 b_{i+j} + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0}$ (for this i and j).

is such that $p \nmid a_i b_j$ but $p \nmid (a_{i-1} b_{j+1} + \cdots)$. So $p \nmid c_{i+j}$.

which contradicts the assumption that $p \mid c(fg)$. So fg is primitive. □.

Lemma. R: UFD.

Let K be the fraction field of R, $f(x) \in R[x]$, $\deg f(x) \geq 1$.

Then $f(x) \in R[x]$ is irreducible iff $f(x)$ is irreducible in $K[x]$.

Proof of lemma: Let $f(x)$ be irr. in $R[x]$.

Suppose $f(x)$ is reducible in $K[x]$. i.e. $f(x) = g(x) h(x)$ with $g, h \in K[x]$.

Then, there exist $r, s \in R$ such that $r g(x), s h(x) \in R[x]$.

($g(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1} x + \cdots + \frac{a_n}{b_n} x^n$, $a_i, b_i \in R$. Let $r = b_0 b_1 \cdots b_n$. then $rg \in R[x]$).

So $rs f(x) = r g(x) \cdot s h(x)$ in $R[x]$.

Let $a = c(r g(x))$, $b = c(s h(x))$. Then $r g(x) = a\, g_1(x)$, $s h(x) = b\, h_1(x)$.

where $g_1(x)$, $h_1(x)$ primitive. Thus

$$rs f(x) = r g(x) \cdot s h(x) = a \cdot g_1(x) \cdot b \cdot h_1(x) = ab\; g_1(x) \cdot h_1(x).$$

Since $f(x)$ is irreducible in $R[x]$, we have

$$c(rs \cdot f(x)) = c(ab \cdot g_1(x) h_1(x)) = ab.$$

Thus, $rs = abu$ with u invertible. $\boxed{(f \text{ primitive?})}$

So $f(x) = (u g_1(x))(h_1(x))$ in $R[x]$. a contradiction.

So $f(x)$ is irreducible in $K[x]$. $\square$.

<u>eg.</u> $\mathbb{Z}[x] \to \mathbb{Q}[x] \to \mathbb{R}[x]$.

$x^2 - 2 \to x^2 - 2 \to (x - \sqrt{2})(x + \sqrt{2})$.

<u>Thm.</u> If R is a UFD, then so is $R[x]$.

<u>Proof</u>: Let $f \in R[x]$ of deg n. Then

- f is a prod. of finitely many polys of deg ≥ 1.

Thus, we only need to prove irr. $\equiv$ prime.

Suppose f is irr. and $f \mid gh$. Then $f(x) q(x) = g(x) h(x)$.

If $\deg f = 0$, then $f(x) = a \mid c(g) c(h)$.

As R is a UFD, $a \mid g(x)$ or $a \mid h(x)$. i.e. $f(x)$ is a prime. T.B.C.