Abstract Algebra. Math 6310. Bertram/Utah 2022-23.

PIDs, UFDs and Noetherian Rings

Let R be a commutative ring with 1.

Definition. $u \in R$ is a *unit* if $uv = 1$ for some $v \in R$.

Remark. The subset $R^* \subset R$ of units is an abelian group (with multiplication).

Examples. (i) $\mathbb{Z}^* = \{\pm 1\}$

(ii) $(\mathbb{Z}/n\mathbb{Z})^*$ consists of the cosets $m + n\mathbb{Z}$ for which $\gcd(m, n) = 1$.

(iii) $R[x]^* = R^*$ (unit constants) but $R[[x]]^* =$ (unit constants) + anything.

Let D be an integral domain.

Definition. (a) An ideal $I \subset D$ is *principal* if $I = \langle a \rangle$ for some $a \in D$.

(b) D is a *principal ideal domain* (PID) if every ideal in D is principal.

Note. We will allow for $\langle u \rangle = D$ to be an ideal in this discussion.

Observation. We say nonzero elements $a, b \in D$ are *associated* if $\langle a \rangle = \langle b \rangle$, which is the case if and only $a = bu$ and $b = av$ for $u, v \in D$, in which case $a = avu$ and $1 = vu$ by cancellation. Thus the set of nonzero principal ideals is in bijection with:

$$\{aD^* |\ a \in D - \{0\}\} = (D - \{0\})/D^*$$

which has a commutative multiplicative structure, but isn't an abelian group since each $a \in D - \{0\}$ that is not a unit has **no** multiplicative inverse, by definition.

Examples. (i) Fields k are the simplest PIDs. They have only the zero ideal.

(ii) The power series rings $k[[x]]$ have only the zero ideal and $\langle x^n \rangle$ for each $n \geq 1$. In particular, they have only one maximal ideal.

(iii) $\mathbb{Z}$ has only the zero ideal and the ideals $\langle n \rangle = \langle -n \rangle$ for $n \geq 1$.

(iv) Polynomial rings $k[x]$ (coefficients in a field!) are PID's, as we see below:

Definition. A *Euclidean domain* is a domain D that supports a function:

$$f : D - \{0\} \to \mathbb{Z}^{\geq 0}$$

with the property that for all $a, b \in D - \{0\}$, there exist $q, r \in D$ such that:

$$a = bq + r$$

with $r = 0$ or $r \neq 0$ and $\deg(r) < \deg(b)$.

Examples. $k[x]$ with polynomial degree, and $\mathbb{Z}$ with $f(n) = |n|$.

Proposition 1. Every Euclidean domain D is a PID.

Proof. Let $I \subset D$ be a nonzero ideal, and let $d \in I - \{0\}$ minimize $f(s) \in \mathbb{Z}^{\geq 0}$ over all $s \in I - \{0\}$. Then for all $s \in I - \{0\}$, we have $s = dq$ for some $q \in D$ by the definition of a Euclidean domain. Thus $\langle d \rangle \subset I \subset \langle d \rangle$ and $I = \langle d \rangle$ is principal. $\square$

Remark. The element $d \in I$ is called a *greatest common divisor* of I.

The notion of a divisor is important in commutative ring theory in general.

Definition. (i) $a \in R$ *divides* $s \in R$ if $s = ab$ for some $b \in R$. This is written $a|s$, and we say a (and b) is a divisor of s.

(ii) a is a *common divisor* of a subset $S \subset R$ if $a|s$ for all $s \in S$, i.e. if $\langle S \rangle \subset \langle a \rangle$.

Recall that a prime (natural) number p is defined by the property that 1 and p are its only divisors, and $p \neq 1$. This is, unfortunately, **not** what algebraists mean by a prime element of a general commutative ring.

Definition. (a) A nonzero element $a \in D$ is *irreducible* if the only divisors of a are units and associates of a, and a is not itself a unit.

(b) $a \in D$ is *prime* if a is not a unit, not zero, and $\langle a \rangle$ is a prime ideal, i.e.

$$a|bc \text{ implies that } a|b \text{ or } a|c$$

Proposition 2. All prime elements of a domain D are irreducible.

Proof. Suppose a is prime and $a = bc$. Then either $a|b$, in which case:

$$b = ad \text{ and } a = bc = bad, \text{ so } bd = 1$$

in which case b is a unit, or else $a|c$ and c is a unit by the same argument. □

Prime elements are even more striking in a PID.

Proposition 3. In a PID, all prime elements generate *maximal* ideals.

Proof. Every prime ideal $\langle a \rangle \subset D$ is contained in a maximal ideal $\mathfrak{m} = \langle b \rangle$ (Zorn's Lemma) which is also principal since D is a PID. Thus $a = bc$ for some c. Because a is prime, either $a|b$, in which case $b \in \langle a \rangle$ and so $\langle a \rangle = \langle b \rangle$ is maximal, or else $a|c$, in which case $c = ad$ and $a = bad$ so $1 = bd$ and b is a unit. This latter option is a contradiction, since by assumption, $\langle b \rangle \neq D$. □

In a Euclidean domain, even more is true.

Proposition 4. Every irreducible element of a Euclidean Domain is prime.

Proof. Suppose $a \in D$ is irreducible and a divides bc but does not divide b. Then the greatest common divisor of a and b is 1 (or any unit) since it divides a and is not associated to a (because then a would divide b). So $1 = ad + be$ has a solution for $d, e \in D$ and then a divides $c = adc + bce$. □

Corollary. If $f(x) \in k[x]$ is irreducible and non-constant, then $k[x]/\langle f(x) \rangle$ is a field.

It behooves us to exhibit an irreducible element of a domain D that isn't prime. It is probably about time for us to consider some new examples.

Subrings of Polynomials. Let $k[t]$ be the polynomial ring, and consider:

$$D = k[t^2, t^3] \subset k[t]$$

(polynomials without a linear term). Then D is a domain and t^2, t^3 are irreducible. However, neither of them is prime, since

$$t^2 \cdot t^4 = t^3 \cdot t^3 \text{ but } t^2 \text{ does not divide } t^3 \text{ and } t^3 \text{ does not divide } t^4$$

This ring is also not a PID, since the ideal $\langle t^2, t^3 \rangle$ (the kernel of evaluation at 0) is clearly not principal. Notice that there is a surjective ring homomorphism:

$$f : k[x, y] \to D;\ f(x) = t^2,\ f(y) = t^3$$

whose kernel is the ideal $\langle x^3 - y^2 \rangle$. This shows that D is isomorphic to:

$$k[x, y]/\langle y^2 - x^3 \rangle$$

which is interpreted as the ring of polynomial functions (in two variables) on the cuspidal plane curve $C = \{(a, b) \in k^2 \mid b^2 = a^3\} \subset k^2$ since the quotient is by the ideal consisting of polynomials that vanish identically on C.

Integer-Like Rings. Let $\alpha \in \mathbb{C}$ be a complex root of a polynomial:

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0 \subset \mathbb{Q}[x]$$

that is irreducible in $\mathbb{Q}[x]$. Without loss of generality, we may assume that

$$f(x) \in \mathbb{Z}[x] \text{ and } \gcd(a_d, ..., a_0) = 1$$

and let $\mathbb{Q}[\alpha] \subset \mathbb{C}$ be the image of the evaluation homomorphism $\text{ev}_\alpha : \mathbb{Q}[x] \to \mathbb{C}$. This is a subfield of $\mathbb{C}$ that is isomorphic to $\mathbb{Q}[x]/\langle f(x) \rangle$ with basis:

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

as a vector space over $\mathbb{Q}$. These are the **number fields** (with complex embeddings).

The polynomial $f(x)$ is *monic* when $a_d = 1$ and in that case the domain:

$$\mathbb{Z}[\alpha] \subset \mathbb{C}$$

is a ring whose additive group $(\mathbb{Z}[\alpha], +)$ is isomorphic to $\mathbb{Z}^d$ (with the same basis).

Consider the quadratic case $f(x) = x^2 + bx + c$ and let $Dd^2 = \Delta = b^2 - 4c$, i.e. D is the discriminant Δ with all square factors squeezed out of it, Then:

$$\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{D}]$$

admits a multiplicative *norm* map $N : \mathbb{Q}[\sqrt{D}] \to \mathbb{Q}$ defined by:

$$N(r + s\sqrt{D}) = (r + s\sqrt{D})(r - \sqrt{D}) = r^2 - s^2 D$$

which has the following properties:

(i) The norm $N(\alpha)$ is the product of α with the other root, i.e. $N(\alpha) = c \in \mathbb{Z}$. Moreover, $N(\beta) \in \mathbb{Z}$ for every $\beta \in \mathbb{Z}[\alpha]$.

(ii) An element $\beta \in \mathbb{Z}[\alpha]$ is a unit if and only if $N(\beta) = \pm 1$.

Examples. (a) The Gaussian integers $\mathbb{Z}[i]$ with N are a Euclidean domain and the units in this ring are $\{1, i, -1, -i\}$.

(b) $\mathbb{Z}[\sqrt{-5}]$ with N is not a Euclidean domain. In fact, it isn't even a PID by Proposition 4 since the elements $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible and:

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

without any of them dividing another. The units in this ring are ± 1.

(c) The ring $\mathbb{Z}[\sqrt{2}]$ has infinitely many units; the solutions to *Pell's equation*:

$$a^2 - 2b^2 = \pm 1 \text{ (in integers)}$$

which include $1 + \sqrt{2}, (1 + \sqrt{2})^2, ...$ This is a Euclidean domain, with $|N|$.

We return to nestled ideas to define:

Definition. A commutative ring R is *Noetherian* if every ascending chain of ideals:

$$I = I_0 \subset I_1 \subset \cdots \subset R$$

reaches its maximal element, i.e. there is an n such that:

$$I_n = I_\infty := \bigcup_{i=0}^{\infty} I_i$$

Remark. Descending chains in reasonable rings may never reach their minimum:

$$\bigcap_{m=0}^{\infty} (p^m)\mathbb{Z} = 0 \text{ but } (p^n)\mathbb{Z} \neq 0 \text{ for any } n \text{ (and prime } p)$$

However, descending chains of *prime* ideals are a different matter, as we will see.

Proposition 5. R is Noetherian if and only if every ideal $I \subset R$ is generated by finitely many elements $s_1, ..., s_m \in I$, i.e.

$$I = \langle s_1, ..., s_m \rangle = \{\sum_{j=1}^{m} r_j s_j \text{ ranging over all choices of } r_j \in R\}$$

Proof. Consider a chain of ideals $I_0 \subset I_1 \subset \cdots$. If the union ideal I_∞ is finitely generated by elements $s_1, ..., s_m$, then there is an $n \in \mathbb{Z}$ for which each $s_i \in I_n$, and then $I_n = \langle s_1, ..., s_m \rangle = I_\infty$. Conversely, given an ideal I, consider the chain $I_0 = 0 \subset \langle s_1 \rangle \subset \langle s_1, s_2 \rangle \subset \cdots \subset I$, where either $I_n = I$, or else s_{n+1} is chosen to be in I but not in I_n. Then eventually $\langle s_1, ..., s_n \rangle = I_n = I$, because otherwise the chain of ideals would not reach I_∞. □

Note. This proof also shows that any finite set of elements $s_1, ..., s_m \in I$ of an ideal in a Noetherian ring can be expanded to a finite generating set of the ideal.

Corollary. PID's are Noetherian.

The Noetherian property (all ideals are finitely generated) holds for far more rings than the PID property (all ideals are generated by one element). We will see that the Noetherian property also spills over to submodules of finitely generated modules over a Noetherian ring. This generalizes the fact that every ascending chain of abelian subgroups of a finitely generated abelian group reaches its maximum.

Hilbert Basis Theorem. If R is Noetherian then $R[x]$ is Noetherian.

Proof. Suppose $J \subset R[x]$ is an arbitrary ideal and for each $d \geq 0$, let:

$$I_d = \{\text{leading coefficients } a_d \in R \text{ of polynomials } f(x) = a_d x^d + \cdots + a_0 \in J\}$$

Then each $I_d \subset R$ is a (finitely generated!) ideal and the ideals form a chain:

$$I_1 \subset I_2 \subset \cdots \subset I_n = I_\infty$$

reaching its maximum at $d = n$ because R is Noetherian. For each $d \leq n$, choose generators $I_d = \langle a_{d,i} \rangle$ for I_d and also choose representative polynomials:

$$f_{d,i}(x) = a_{d,i} x^d + ...$$

Then for each $d \leq n$ and $f(x) \in J$ of degree d, there are constants $b_{d,i}$ so that

$$f(x) = a_d x^d + ... \text{ and } g(x) = \sum b_{d,i} f_{d,i}(x) = a_d x^d + ...$$

while if $d \leq n$, then there are constants $b_{n,i}$ so that

$$f(x) = a_d x^d + ... \text{ and } g(x) = \sum b_{n,i} x^{d-n} f_{n,i}(x) = a_d x^d + ...$$

In each case, we conclude that within the ideal generated by all the $f_{d,i}$

$$\langle f_{d,i}(x) \mid 0 \leq d \leq n \rangle \subset J$$

there is a polynomial $g(x)$ whose leading term matches the leading term of $f(x)$. Subtracting this element and proceeding by induction on the degree, we conclude that $f(x) \in \langle f_{d,i}(x) \mid 0 \leq d \leq n \rangle$, i.e. that J is generated by the $f_{d,i}$. □

Corollary. Every quotient ring of $\mathbb{Z}[x_1, ..., x_n]$ or $k[x_1, ..., x_n]$ is Noetherian.

Remark. The same idea shows that if R is Noetherian, then $R[[x]]$ is Noetherian.

One application of Noetherianness is the following.

Proposition 6. Suppose R is a commutative ring with 1, in which every chain:

$$I_1 = \langle a_1 \rangle \subset I_2 = \langle a_2 \rangle \subset \cdots$$

of *principal* ideals reaches its maximum (which is then also principal). Then every non-zero non-unit $b \in R$ has an *irreducible factorization*

$$b = c_1 c_2 \cdots c_n;\ c_i \in R$$

as a finite product of irreducible elements of R.

Proof. Suppose on the contrary b is not a product of finitely many irreducibles. Then b is not irreducible, so

$$b = a_1 c_1 \text{ and neither } a_1 \text{ nor } c_1 \text{ is a unit, and } \langle b \rangle \subset \langle a_1 \rangle$$

is a proper ideal. We may assume a_1 is not a product of finitely many irreducibles, and proceed by induction, generating a sequence of proper inclusions of ideals $\langle b \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots$ violating the assumption on R. □

Corollary. Noetherian rings have irreducible factorization.

Note. The rings $\mathbb{Z}[\sqrt{-5}]$ or $k[t^2, t^3]$ are quotients of polynomial rings, hence they are Noetherian, but in these rings irreducible factorizations are not unique!

Definition. A domain D is a *unique factorization domain* (UFD) if every non-zero non-unit $a \in D$ factors as a finite product of *prime* elements of D, in which case the factorization is unique (up to reordering and associated elements).

Examples. $\mathbb{Z}$ and $k[x]$ (and any Euclidean domain) are UFDs.

Proposition 7. A domain D with irreducible factorization is a UFD if and only if every irreducible element of D is prime.

Proof. (Fill in the details) Prime factorizations are unique, when they exist, and if an irreducible element has a prime factorization, then it is prime.

Analogous to the Hilbert Basis Theorem, in the next section we will prove:

Gauss' Lemma. If R is a UFD, then $R[x]$ is a UFD.

But please keep in mind that quotients of UFD's are not, in general, UFD's. We've seen two examples above, but the most fundamental example is:

$$R = k[x, y, z, w]/I \text{ with } I = \langle xw - yz \rangle$$

in which $\overline{x} := x + I, \overline{y}, \overline{z}, \overline{w}$ are irreducible, but R is constructed on purpose so that:

$$\overline{x} \cdot \overline{w} = \overline{y} \cdot \overline{z}$$

is a non-unique factorization.