Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

All rings in this note are commutative.

1. Euclidean Domains

Definition: *Integral Domain* is a ring with no zero divisors (except 0).

Definition: Any function $N : R \to \mathbb{Z}^+ \cup 0$ with $N(0) = 0$ is called a *norm* on the integral domain R. If $N(a) > 0$ for $a \neq 0$ define N to be a *positive norm*.

Definition: *Euclidean Domain* is an integral domain with a division algorithm that is $\forall a, b \in R$ such that $b \neq 0$ there is a *norm* on R $N : R \to \mathbb{Z}^+$ with

$$a = qb + r \qquad \text{and } r = 0 \text{ or } N(r) < N(b).$$

The element q is called the *quotient* and the element r the *remainder* of the division.

Examples

(1) Fields are Euclidean Domains where any norm will satisfy the condition, e.g., $N(a) = 0$ for all a.

(2) The integers $\mathbb{Z}$ are a Euclidean Domain with norm given by $N(a) = |a|$.

(3) the ring $\mathbb{Z}$ of polynomials with integer coefficients is not a Euclidean Domain (for any choice of norm).

Examples *on Sage*

(1) $\mathbb{Z}_2[x]/(1 + x + x^2)$

```
sage: IntegerModRing(2)
Ring of integers modulo 2
sage: R1 = IntegerModRing(2)
sage: R1['x']
Univariate Polynomial Ring in x over Ring of integers modulo 2 (using NTL)
sage: R1['x,y,z']
Multivariate Polynomial Ring in x, y, z over Ring of integers modulo 2
sage: R2 = R1['x']
sage: R2.gens()
(x,)
sage: R2.gen()
x
sage: x = R2.gen()
sage: R2.ideal(1+x+x^2)
Principal ideal (x^2 + x + 1) of Univariate Polynomial Ring in x over Ring
of integers modulo 2 (using NTL)
sage: I1 = R2.ideal(1+x+x^2)
sage: R2.quotient(I1)
Univariate Quotient Polynomial Ring in xbar over Ring of integers modulo 2
with modulus x^2 + x + 1
sage: R3 = R2.quotient(I1)
sage: R3.gens()
(xbar,)
```

```
sage: one = R3.one()
sage: one
1
sage: 1
1
sage: one == 1
True
sage: 1.parent()
Integer Ring
sage: one.parent()
Univariate Quotient Polynomial Ring in xbar over Ring of integers modulo 2
with modulus x^2 + x + 1
sage: R3.gens()
(xbar,)
sage: xbar = R3.gen()
sage: [[y*z for y in [0,one,xbar,one+xbar]] for z in [0,one,xbar,
....: one+xbar]]

[[0, 0, 0, 0],
 [0, 1, xbar, xbar + 1],
 [0, xbar, xbar + 1, 1],
 [0, xbar + 1, 1, xbar]]
sage: [[y+z for y in [0,one,xbar,one+xbar]] for z in [0,one,xbar,
....: one+xbar]]

[[0, 1, xbar, xbar + 1],
 [1, 0, xbar + 1, xbar],
 [xbar, xbar + 1, 0, 1],
 [xbar + 1, xbar, 1, 0]]
sage: I1.is_maximal()
True
sage: R3.is_field()
True
```

(2) $\mathbb{R}[x]/(1+x^2) \cong \mathbb{C}$

```
sage: R4 = RR['x']
sage: R4
Univariate Polynomial Ring in x over Real Field with 53 bits of precision
sage: R4 = QQ['x']
sage: R4
Univariate Polynomial Ring in x over Rational Field
sage: R4 = RR['x']
sage: CC
Complex Field with 53 bits of precision
sage: R4
Univariate Polynomial Ring in x over Real Field with 53 bits of precision
sage: x = R4.gen()
sage: R4.quotient(R4.ideal(1+x^2))
Univariate Quotient Polynomial Ring in xbar over Real Field with 53 bits of
precision with modulus x^2 + 1.00000000000000
sage: R5 = R4.quotient(R4.ideal(1+x^2))
sage: R5.is_field()
True
sage: xbar = R5.gen()
sage: (3+2*xbar)*(3/13-2/13*xbar)
1.00000000000000
```

```
sage: _.parent()
Univariate Quotient Polynomial Ring in xbar over Real Field with 53 bits of
precision with modulus x^2 + 1.00000000000000
sage: (3+2*xbar)*(3/13-2/13*xbar)==R5.one()
True\\
```

Example (*Euclidean Algorithm*)

gcd(18, 30)

$$\begin{aligned} 30 &= 1 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 \end{aligned}$$

so 6 is the gcd(18, 30)

$$\left.\begin{aligned} 6 \quad &= 18 - 1 \cdot 12 \\ 12 \quad &= 30 - 18 \end{aligned}\right\} \Longrightarrow 6 = -1 \cdot 30 + 2 \cdot 18$$

so $6 \in (18, 30) = (6)$

Now generalize this to Euclidean Domain, this shows that every *Euclidean Domain* is a *Principal Ideal Domain.*

2. Principal Ideal Domains

Definition: A *Principal Ideal Domain* (P.I.D.) is an integral domain in which every ideal is principal.

Examples

(1) The polynomial ring $\mathbb{R}[x]$ is a Euclidean Domain (or a Principal Ideal Domain).

(2) There are integral domains that are not Euclidean Domain, e.g., $\mathbb{Z}[x]$.

(3) If $\mathbb{F}$ is a field, $\mathbb{F}[x]$ is a Euclidean Domain.

(4) For $x^3 + 1$ and $x^2 + 2x + 1$ in $\mathbb{Q}[x]$, show $(x^3 + 1, x^2 + 2x + 1) = x + 1$

$$\begin{aligned} x^3 + 1 &= x(x^2 + 2x + 1) - 2x^2 - x + 1 \\ x^2 + 2x + 1 &= -\frac{1}{2}(-2x^2 - x + 1) + \frac{3}{2}x + \frac{3}{2} \\ -2x^2 - x + 1 &= -\frac{4}{3}x\left(\frac{3}{2}x + \frac{3}{2}\right) + x + 1 \end{aligned}$$

Exercise: Compute gcd(2, x).

Definition:

(1) An ideal $P \subseteq R$ is a *prime ideal* if $1 \notin P$ (i.e., $P \neq R$) and if $ab \in P$ then either $a \in P$ or $b \in P$.

(2) An ideal M in an arbitrary ring R is called a *maximal ideal* if $M \neq R$ and the only ideals containing I are I and R

Theorem: Assume R is commutative with identity 1.

(1) The ideal I is a maximal ideal if and only if the quotient ring R/I is a field.

(2) The ideal I is a prime ideal in R if and only if the quotient ring R/I is an integral domain.

(3) Every maximal ideal of R is a prime ideal.

Sketch of a proof:

(1) There are two things to be shown here.
$\Rightarrow$ If I is a maximal ideal of R, then every non-zero element of R/I is a unit. A strategy for doing this is as follows: if $a \in R$ does not belong to I (so $a + I$ is not the zero element in R/I), then the fact that I is maximal as an ideal of R means that the only ideal of R that contains both I and the element a is R itself. In particular the only ideal of R that contains both I and the element a contains the identity element of R.
$\Leftarrow$ If R/I is a field (i.e. if every non-zero element of R/I is a unit), then I is a maximal ideal of R. A useful strategy for doing this is to suppose that J is an ideal of R properly containing I, and try to show that J must be equal to R.

(2) As mentioned in class, this follows by translating notion of prime ideal into the language of quotients.
$rs \in I \iff (r + I)(s + I) = I \implies r \in I$ or $s \in I \implies r + I = I$ or $s + I = I$

(3) I is maximal ideal $\implies R/I$ is a field $\implies R/I$ is an Ideal Domain $\implies I$ is prime if we follwed (2).

Proposition: If R is a Principal Ideal Domain then I is prime ideal $\iff I$ is maximal ideal.

Sketch of a proof: Just need to show "$\implies$".
Assume $I = (p) \subseteq (m)$ maximal $\subsetneq R$ then $p = rm \implies m \in (p)$ or $r \in (p)$.
If $m \in (p)$ then $(m) = (p)$.
If $r \in (p)$ then $(m) = R$ (not possible).

Corollary: R is a field $\iff R[x]$ is a Principal Ideal Domain.

Sketch of a proof: We discussed "$\implies$" as an example since R field $\implies R[x]$ is a Euclidean Domain $\implies R[x]$ is a Principal Ideal Domain.
"$\impliedby$" because (x) is prime $\implies (x)$ is max $\implies R[x]/(x) \cong R$ is field.

3. Unique Factorization Domains

Definition: Let R be an integral domain.

(1) Suppose $r \in R$ is nonzero and is not a unit. The r is called *irreducible* in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R. Otherwise, r is said to be *reducible.*

(2) The nonzero element $p \in R$ is called *prime* in R if the ideal (p) generated by p is a prime ideal.

Note: irreducible and prime are not the same.

Examples

$R = \mathbb{Z}[i\sqrt{5}]$ is not a Principal Ideal Domain.

$\gamma = 2 + i\sqrt{5}$ is an irreducible element.
$\gamma(2 - i\sqrt{5}) = 9$ so $9 \in (\gamma)$ but $9 = 3 \cdot 3$ and $3 \notin (\gamma)$

Proposition: In an integral domain a prime element, p, is always irreducible.

Sketch of a proof: $p = ab \underset{\text{(since either } a \in (p) \text{ or } b \in (p))}{\implies} a \in (p), a = rp \implies p = prb \implies b$ unit.

Proposition: In a Principal Ideal Domain a nonzero element, p, is prime if and only if it is irreducible.

Sketch of a proof: $\Longleftarrow$ if r is irreducible (want to show (r) is a prime ideal).
(r) is contained in some maximal ideal $(m) \Longleftarrow r = ma$ with m not a unit therefore a is a unit and $(r) = (m)$.
(r) is maximal ideals we know maximal are prime ideals.