A REVIEW OF P.I.D.'S

Throughout the review we assume that $R$ is an integral domain. This means that $R$ is a commutative ring with identity $1$, $1 \neq 0$, and

$$a, b \in R, \ ab = 0 \implies a = 0 \text{ or } b = 0.$$ 

The two most important examples to keep in mind are the ring of integers $\mathbb{Z}$ and the ring of polynomials $F[\lambda]$ over a field $F$ in the indeterminate $\lambda$.

§1 DIVISIBILITY

Definition 1.

(i) If $a, b \in R$, we say that $b$ divides $a$, written $b \mid a$, if there exists $r \in R$ so that $a = rb$.

(ii) A unit in $R$ is an element $u \in R$ that divides 1. Equivalently, a unit in $R$ is an element $u \in R$ that has a multiplicative inverse in $R$ (that is, there is an element $v \in R$ so that $uv = 1$).

(iii) If $a, b \in R$, we say that $a$ is an associate of $b$, written $a \sim b$, if $a = ub$ for some unit $u$ of $R$. $\sim$ is an equivalence relation on $R$. Note that

$$a \sim b \iff a \mid b \text{ and } b \mid a.$$

(This uses the fact that $R$ is an integral domain.)

Example 2.

(i) Suppose that $R = \mathbb{Z}$. The units of $R$ are $\pm 1$. Thus, given $a \in \mathbb{Z}$, the associates of $a$ are $\pm a$.

(ii) Suppose that $R = F[\lambda]$. The units of $F[\lambda]$ are the nonzero constant polynomials. Thus, if $a(\lambda) \in F[\lambda]$, the associates of $a(\lambda)$ are the polynomials of the form $ka(\lambda)$, where $0 \neq k \in F$. Hence, any nonzero polynomial $a(\lambda)$ in $F[\lambda]$ is an associate of a unique monic polynomial in $F[\lambda]$ (multiply $a(\lambda)$ by the inverse of its leading coefficient). (Recall that a monic polynomial is a nonzero polynomial with leading coefficient 1.) For example in $\mathbb{Q}[\lambda]$, the polynomial $2\lambda^2 - 3\lambda + 5$ is an associate of the monic polynomial $\lambda^2 - \frac{3}{2} \lambda + \frac{5}{2}$.
§2 Principal ideals in $R$

Definition 3. If $a_1, \ldots, a_k \in R$, we define

$$(a_1, \ldots, a_k) = Ra_1 + \cdots + Ra_k = \{r_1a_1 + \cdots + r_ka_k \mid r_1, \ldots, r_k \in R\}.$$ 

$(a_1, \ldots, a_k)$ is the smallest ideal of $R$ which contains $a_1, \ldots, a_k$. We call $(a_1, \ldots, a_k)$ the ideal of $R$ generated by $a_1, \ldots, a_k$.

As a special case of this definition, we have

Definition 4. If $a \in R$, we define

$$(a) = Ra = \{ra \mid r \in R\}.$$ 

$(a)$ is the smallest ideal of $R$ which contains $a$. We call $(a)$ the ideal of $R$ generated by $a$ or the principal ideal of $R$ generated by $a$.

Proposition 5. Suppose that $a, b \in R$. Then,

(i) $(a) \subseteq (b) \iff b \mid a.$

(ii) $(a) = (b) \iff b \mid a$ and $a \mid b \iff a \sim b.$

Example 6. In $\mathbb{Z}$, $(2) = (-2)$ since $2 \sim -2$. Also, $(6) \subseteq (2)$, since $2 \mid 6$. However, $(6) \not= (2)$, since $6 \sim 2$.

Definition 7. A principal ideal domain (abbreviated as p.i.d.) is an integral domain $R$ so that every ideal of $R$ is of the form $(a)$ for some $a \in R$.

Example 8.

(i) $\mathbb{Z}$ is a p.i.d. So, by Proposition 5(ii) and Example 2(i), the ideals of $\mathbb{Z}$ are

$$(0), (1), (2), (3), \ldots.$$ 

Moreover, these ideals are distinct.

(ii) $F[\lambda]$ is a p.i.d. So, by Proposition 5(ii) and Example 2(ii), the ideals of $F[\lambda]$ are $(0)$ and

$$(a(\lambda)) \text{ with } a(\lambda) \text{ monic.}$$ 

Moreover, these ideals are distinct.

§3 GCD's and LCM's

In this section, assume that $R$ is a p.i.d.

Definition 9. Suppose that $a$ and $b$ are nonzero elements of $R$. A greatest common divisor (abbreviated gcd) of $a$ and $b$ is an element $d \in R$ so that

(i) $d$ is a common divisor of $a$ and $b$ (that is $d \mid a$ and $d \mid b$),

(ii) $d$ is divisible by any common divisor of $a$ and $b$. 
Proposition 10. Let $a$ and $b$ be nonzero elements of $R$. Then,

(i) If $d$ is an element of $R$ such that

$$(d) = (a, b)$$

(using the notation in Definition 3), then $d$ is a gcd of $a$ and $b$.

(ii) There exists a gcd of $a$ and $b$.

(iii) The gcd of $a$ and $b$ is unique up to association. That is, any two gcd's of $a$ and $b$ are associates of each other.

(iv) If $d$ is a gcd of $a$ and $b$, then

$$d = ra + sb$$

for some $r, s \in R$.

Notation 11. Suppose that $a$ and $b$ are nonzero elements of $R$. Since the gcd of $a$ and $b$ is unique up to association, it is reasonable to refer to the gcd of $a$ and $b$ and denote it by $\gcd(a, b)$. (This is really an abuse of terminology and notation since there is in general more than one gcd of $a$ and $b$. However, this will not cause any confusion.)

Example 12.

(i) Let $R = \mathbb{Z}$ and suppose that $a$ and $b$ are nonzero integers. Then, $a$ and $b$ have two different gcd's (which are negatives of each other). By convention, we always choose $\gcd(a, b)$ to be positive (thereby making it unique). For example,

$$\gcd(12, 20) = 4.$$ 

(ii) Let $R = F[\lambda]$ and suppose that $a(\lambda)$ and $b(\lambda)$ are nonzero polynomials in $F[\lambda]$. Then, any two gcd's of $a(\lambda)$ and $b(\lambda)$ are nonzero constant multiplies of each other. By convention, we always choose $\gcd(a(\lambda), b(\lambda))$ to be monic (thereby making it unique). For example, in $\mathbb{Q}[\lambda]$ we have

$$\gcd(\lambda^2 - 1, \lambda^2 + 2\lambda + 1) = \lambda + 1.$$ 

Definition 13. Suppose that $a$ and $b$ are nonzero elements of $R$. We say that $a$ and $b$ are relatively prime if $\gcd(a, b) = 1$. (Strictly speaking we mean here that $\gcd(a, b)$ is a unit. However, any unit is an associate of 1.)

The following proposition follows easily from Proposition 10(iv).

Proposition 14. Suppose that $a$ and $b$ are nonzero elements of $R$. If $a$ and $b$ are relatively prime, then there exist $r, s \in R$ so that

$$1 = ra + sb.$$ 

Conversely, if there exist $r, s \in R$ so that $1 = ra + sb$, then $a$ and $b$ are relatively prime.
**Definition 15.** Suppose that $a$ and $b$ are nonzero elements of $R$. A *least common multiple* (abbreviated lcm) of $a$ and $b$ is an element $e \in R$ so that

(i) $e$ is a common multiple of $a$ and $b$ (that is $a \mid e$ and $b \mid e$),

(ii) Any common multiple of $a$ and $b$ is a multiple of $e$.

**Proposition 16.** Let $a$ and $b$ be nonzero elements of $R$. Then,

(i) If $e$ is an element of $R$ such that

$$ (e) = (a) \cap (b), $$

then $e$ is an lcm of $a$ and $b$.

(ii) There exists an lcm of $a$ and $b$.

(iii) The lcm of $a$ and $b$ is unique up to association. That is, any two lcm’s of $a$ and $b$ are associates of each other.

**Notation 17.** Suppose that $a$ and $b$ are nonzero elements of $R$. Since the lcm of $a$ and $b$ is unique up to association, it is reasonable to refer to the lcm of $a$ and $b$ and denote it by $\text{lcm}(a, b)$. (This is again an abuse of terminology and notation.)

**Example 18.**

(i) Let $R = \mathbb{Z}$ and suppose that $a$ and $b$ are nonzero integers. As in the case of the gcd, we always choose $\text{lcm}(a, b)$ to be positive. For example,

$$ \text{lcm}(12, 20) = 60. $$

(ii) Let $R = F[\lambda]$ and suppose that $a(\lambda)$ and $b(\lambda)$ are nonzero polynomials in $F[\lambda]$. As for gcd’s, we always choose $\text{lcm}(a(\lambda), b(\lambda))$ to be monic.

§4 UNIQUE FACTORIZATION

In this section, we again assume that $R$ is a p.i.d.

**Definition 19.** An *irreducible* element in $R$ is a nonzero nonunit element $p$ of $R$ so that

$$ a, b \in R, \ p = ab \implies a \text{ is a unit or } b \text{ is a unit}. $$

Any associate of an irreducible element of $R$ is irreducible.

**Example 20.**

(i) The irreducible elements of $\mathbb{Z}$ are the integers of the form $\pm p$, where $p$ is a positive prime.

(ii) The irreducible polynomials in $F[\lambda]$ are the polynomials over $F$ of degree at least 1 that cannot be factored in $F[\lambda]$ as the product of polynomials of smaller degree. For example, $\lambda + 2$ and $\lambda^2 + 1$ are irreducible polynomials in $\mathbb{Q}[\lambda]$.

**Lemma 21 (Euclid’s lemma for p.d.’s).** Suppose that $p, a, b \in R$ and $p$ is irreducible. If $p \mid ab$, then either $p \mid a$ or $p \mid b$. 
Theorem 22 (Unique factorization in pid's). Suppose that $R$ is a pid and $a$ is a nonzero nonunit in $R$. Then, there exist irreducible elements $p_1, \ldots, p_n$ of $R$ so that

$$a = p_1 \cdots p_n.$$ 

Moreover, the irreducible elements $p_1, \ldots, p_n$ are uniquely determined up to order and association.

The following proposition can be used to calculate gcd's and lcm's provided that one knows how to factor elements of $R$ as the product of irreducible elements of $R$. (In practice, it usually works the other way around.)

Proposition 23. Suppose that $a$ and $b$ are nonzero elements of $R$. Suppose that

$$a = up_1^{k_1} p_2^{k_2} \cdots p_n^{k_n} \quad \text{and} \quad b = vp_1^{\ell_1} p_2^{\ell_2} \cdots p_n^{\ell_n},$$

where $u, v$ are units in $R$, $p_1, \ldots, p_n$ are irreducible elements of $R$ so that $p_i \sim p_j$ for $i \neq j$, and $k_1, \ldots, k_n, \ell_1, \ldots, \ell_n$ are integers $\geq 0$. Then,

$$\gcd(a, b) = p_1^{\min(k_1, \ell_1)} p_2^{\min(k_2, \ell_2)} \cdots p_n^{\min(k_n, \ell_n)}$$

and

$$\text{lcm}(a, b) = p_1^{\max(k_1, \ell_1)} p_2^{\max(k_2, \ell_2)} \cdots p_n^{\max(k_n, \ell_n)}.$$

Consequently,

$$\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$  

Example 24. In $\mathbb{Z}$, we have

$$200 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2 7^0 \quad \text{and} \quad 245 = 5 \cdot 7 \cdot 7 = 2^0 5^1 7^2.$$ 

Hence,

$$\gcd(200, 245) = 2^0 5^1 7^0 = 5 \quad \text{and} \quad \text{lcm}(200, 245) = 2^2 5^2 7^2 = 9800.$$ 

Euclidean domains

Assume again that $R$ is a integral domain.

Definition 25. A norm on $R$ is a function $N$ which assigns to each nonzero element $a$ of $R$ a nonnegative integer $N(a)$.

Definition 26. A Euclidean domain is an integral domain $R$ together with a norm $N$ on $R$ so that the following condition holds:

If $a$ and $b$ are elements of $R$ with $b \neq 0$, then there exist elements $q$ and $r$ of $R$ so that

$$a = qb + r$$

and either $r = 0$ or $N(r) < N(b)$. 
**Terminology 27.** The elements \( q \) and \( r \) appearing in the above definition are called respectively the *quotient* and the *remainder* in the division of \( a \) by \( b \) (even though \( q \) and \( r \) are not in general uniquely determined by \( a \) and \( b \)). We say that a Euclidean domain has a *division algorithm*.

**Example 28.**
(i) \( \mathbb{Z} \) is a Euclidean domain with norm \( N \) defined by \( N(a) = |a| \) for nonzero \( a \) in \( \mathbb{Z} \).
(ii) \( F[\lambda] \) is a Euclidean domain with norm \( N \) defined by \( N(a(\lambda)) = \deg(a(\lambda)) \) for nonzero \( a(\lambda) \) in \( F[\lambda] \).

**Theorem 29.** *If \( R \) is a Euclidean domain, then \( R \) is a pid.*

The converse of Theorem 29 is not true (although it is not so easy to give an example of a pid which is not a Euclidean domain for any choice of norm \( N \)).

It follows from Theorem 29 that all of the facts that were stated in earlier sections for pid's apply in particular to Euclidean domains. However, Euclidean domains have one big advantage over general pid's. Namely, it is easy to compute \( \gcd(a, b) \) and \( \text{lcm}(a, b) \) and to express \( \gcd(a, b) \) as a sum of multiples of \( a \) and \( b \) (as in Proposition 10(iv)). This is done using the *Euclidean algorithm* which consists of repeated uses of the Division algorithm.

**Example 30.** Consider once again \( a = 200 \) and \( b = 245 \) in \( \mathbb{Z} \). We have

\[
245 = 1 \cdot 200 + 45, \\
200 = 4 \cdot 45 + 20, \\
45 = 2 \cdot 20 + 5, \\
20 = 4 \cdot 5 + 0. 
\]

\( (*) \)

Consequently, we have

\[ \gcd(200, 245) = 5 \]

(the last nonzero remainder) and so

\[ \text{lcm}(200, 245) = \frac{200 \cdot 245}{5} = 9800. \]

Also working backwards using the equations \( (*) \) (except the last one), we have

\[
5 = 45 - 2 \cdot 20 \\
= 45 - 2(200 - 4 \cdot 45) = 9 \cdot 45 - 2 \cdot 200 \\
= 9(245 - 1 \cdot 200) - 2 \cdot 200 = 9 \cdot 245 - 11 \cdot 200
\]

So

\[ 5 = (-11) \cdot 200 + 9 \cdot 245 \]

as in Proposition 10(iv).