Abstract Algebra II

George Voutsadakis[1]

[1] Mathematics and Computer Science
Lake Superior State University

LSSU Math 342

1. EDs, PIDs and UFDs
   - Euclidean Domains
   - Principal Ideal Domains
   - Unique Factorization Domains

Subsection 1

Euclidean Domains

Norms and Euclidean Domains

- The notion of a norm on an integral domain R is a measure of "size" in R.

Definition (Norm)

A 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 $a \neq 0$, N is called a **positive norm**.

- This notion of a norm is fairly weak and it is possible for the same integral domain R to possess several different norms.

Definition (Euclidean Domain)

The integral domain R is said to be a **Euclidean Domain** (or possess a **Division Algorithm**) if there is a norm N on R, such that, for any two elements a and b of R, with $b \neq 0$, there exist elements q and r in R with $a = qb + r$, with $r = 0$ or $N(r) < N(b)$. The element q is called the **quotient** and the element r the **remainder** of the division.

The Euclidean Algorithm

- The importance of the existence of a Division Algorithm on an integral domain R is that it allows a **Euclidean Algorithm** for two elements a and b of R.
  By successive "divisions" (in the field of fractions of R) we write:

$$\begin{array}{rcl} a & = & q_0 b + r_0 \\ b & = & q_1 r_0 + r_1 \\ r_0 & = & q_2 r_1 + r_2 \\ & \vdots & \\ r_{n-2} & = & q_n r_{n-1} + r_n \\ r_{n-1} & = & q_{n+1} r_n \end{array}$$

  where r_n is the last nonzero remainder.
  - Such an r_n exists since $N(b) > N(r_0) > N(r_1) > \cdots > N(r_n)$ is a decreasing sequence of nonnegative integers if the remainders are nonzero. Such a sequence cannot continue indefinitely.
  - There is no guarantee that these elements are unique.

Examples I

(0) Fields are trivial examples of Euclidean Domains where any norm will satisfy the defining condition (e.g., $N(a) = 0$, for all a).
This is because for every a, b, with $b \neq 0$, we have $a = qb + 0$, where $q = ab^{-1}$.

(1) The integers $\mathbb{Z}$ are a Euclidean Domain with norm given by $N(a) = |a|$, the usual absolute value. The existence of a Division Algorithm in $\mathbb{Z}$ (the familiar "long division" of elementary arithmetic) is verified as follows:
Let a and b be two nonzero integers.

- Suppose first that $b > 0$. The half open intervals $[nb, (n+1)b)$, $n \in \mathbb{Z}$, partition the real line. So a is in one of them, say $a \in [kb, (k+1)b)$. For $q = k$, we have $a - qb = r \in [0, |b|)$ as needed.
- If $b < 0$, $-b > 0$, whence, there is an integer q, such that $a = q(-b) + r$, with either $r = 0$ or $|r| < |-b|$. Thus, $a = (-q)b + r$ satisfies the requirements of the Division Algorithm for a and b.

This argument can be made more formal by using induction on $|a|$.

Example 1 (Additional Remarks)

- If a is not a multiple of b, there are always two possibilities for the pair q, r: The proof above always produced a positive remainder r.

  If for example $b > 0$ and q, r are as above with $r > 0$, then

  $$a = q'b + r', \text{ with } q' = q + 1 \text{ and } r' = r - b$$

  also satisfy the conditions of the Division Algorithm applied to a, b.

  E.g.,

  $$5 = 2 \cdot 2 + 1 = 3 \cdot 2 - 1$$

  are the two ways of applying the Division Algorithm in $\mathbb{Z}$ to $a = 5$ and $b = 2$.
- The quotient and remainder are unique if we require the remainder to be nonnegative.

Polynomial Rings over Fields

(2) If F is a field, then the polynomial ring $F[x]$ is a Euclidean Domain with norm given by $N(p(x)) =$ the degree of $p(x)$.

The Division Algorithm for polynomials is simply "long division" of polynomials which may be familiar for polynomials with real coefficients.

The proof is very similar to that for $\mathbb{Z}$ (for polynomials the quotient and remainder are shown to be unique).

- In order for a polynomial ring to be a Euclidean Domain the coefficients must come from a field, since the division algorithm ultimately rests on being able to divide arbitrary nonzero coefficients.

  We will see that $R[x]$ is not a Euclidean Domain if R is not a field.

The Gaussian Integers

(3) The Gaussian integers $\mathbb{Z}[i]$ are a Euclidean Domain with respect to the norm $N(a+bi)=a^2+b^2$:
Let $\alpha=a+bi$, $\beta=c+di$ be two elements of $\mathbb{Z}[i]$, with $\beta\neq 0$. Then in the field $\mathbb{Q}(i)$, we have

$$\frac{\alpha}{\beta}=r+si,\ \text{where } r=\frac{ac+bd}{c^2+d^2}, s=\frac{be-ad}{c^2+d^2}\in\mathbb{Q}.$$

Let p be an integer closest to the rational number r and let q be an integer closest to the rational number s, so that both $|r-p|$ and $|s-q|$ are at most $\frac{1}{2}$. We show

$$\alpha=(p+qi)\beta+\gamma,\ \text{for some } \gamma\in\mathbb{Z}[i], \text{ with } N(\gamma)\leq\frac{1}{2}N(\beta).$$

Let $\theta=(r-p)+(s-q)i$. Set $\gamma=\beta\theta$. Then $\gamma=\alpha-(p+qi)\beta$. So $\gamma\in\mathbb{Z}[i]$ is a Gaussian integer and $\alpha=(p+qi)\beta+\gamma$. But $N(\theta)=(r-p)^2+(s-q)^2\leq\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$. So the multiplicativity of the norm N implies that $N(\gamma)=N(\theta)N(\beta)\leq\frac{1}{2}N(\beta)$.

Gaussian Integers (Additional Remarks)

- The algorithm is explicit:
  - Given α, β, compute r and s;
  - From r and s, compute p and q;
  - Then calculate the remainder $\gamma = \alpha - (p + qi)\beta$.

  Note also that the quotient need not be unique: if r (or s) is half of an odd integer then there are two choices for p (or for q, respectively).
- We will show that $\mathbb{Z}[\sqrt{-5}]$ is not Euclidean with respect to any norm.
- We will also show that $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is not a Euclidean Domain with respect to any norm.

Ideals in Euclidean Domains

Proposition

Every ideal in a Euclidean Domain is principal. More precisely, if I is any nonzero ideal in the Euclidean Domain R, then $I = (d)$, where d is any nonzero element of I of minimum norm.

- If I is the zero ideal, there is nothing to prove. Otherwise, let d be any nonzero element of I of minimum norm. Such a d exists since the set $\{N(a) : a \in I\}$ has a minimum element by the Well Ordering of $\mathbb{Z}$.
  - Clearly $(d) \subseteq I$, since d is an element of I.
  - For the reverse inclusion, let $a \in I$. By the Division Algorithm, $a = qd + r$, with $r = 0$ or $N(r) < N(d)$. Then $r = a - qd$. But $a, qd \in I$. So $r \in I$. By the minimality of the norm of d, we see that r must be 0. Thus $a = qd \in (d)$.
- Every ideal of $\mathbb{Z}$ is principal.
- An integral domain R is not a Euclidean Domain if it has a non-principal ideal.

A Polynomial Ring

(1) Let $R = \mathbb{Z}[x]$.

Recall that the ideal $(2, x)$ is not principal.

It follows that the ring $\mathbb{Z}[x]$ of polynomials with integer coefficients is not a Euclidean Domain (for any choice of norm).

A Quadratic Integer Ring

(2) Let R be $\mathbb{Z}[\sqrt{-5}]$. Let N be the norm $N(a+b\sqrt{-5}) = a^2+5b^2$. Consider the ideal $I = (3, 2+\sqrt{-5})$ generated by 3 and $2+\sqrt{-5}$. Suppose $I = (a+b\sqrt{-5})$, $a, b \in \mathbb{Z}$, were principal, Then, $3 = \alpha(a+b\sqrt{-5})$ and $2+\sqrt{-5} = \beta(a+b\sqrt{-5})$, for some $\alpha, \beta \in R$. Taking norms in the first equation gives $9 = N(\alpha)(a^2+5b^2)$. But a^2+5b^2 is a positive integer. So, it must be $1, 3$ or 9.

- If the value is 9 then $N(\alpha) = 1$ and $\alpha = \pm 1$. So $a+b\sqrt{-5} = \pm 3$. This is impossible by the second equation, since the coefficients of $2+\sqrt{-5}$ are not divisible by 3.
- The value cannot be 3 since there are no $a, b \in \mathbb{Z}$, with $a^2+5b^2 = 3$.
- If the value is 1, then $a+b\sqrt{-5} = \pm 1$. The ideal I would be the entire ring R. But then $1 \in I$. So $3\gamma + (2+\sqrt{-5})\delta = 1$, for some $\gamma, \delta \in R$. Multiply both sides by $2-\sqrt{-5}$. We get $(1-3\gamma)(2-\sqrt{-5}) = 9\delta$. Thus, $2-\sqrt{-5}$ is a multiple of 3 in R. A contradiction.

It follows that I is not a principal ideal. So R is not a Euclidean Domain (with respect to any norm).

Multiples, Divisors and Greatest Common Divisor

Definition (Multiple, Divisor, Greatest Common Divisor)

Let R be a commutative ring and let $a, b \in R$, with $b \neq 0$.

(1) a is said to be a **multiple** of b if there exists an element $x \in R$, with $a = bx$. In this case b is said to **divide** a or be a **divisor** of a, written $b \mid a$.

(2) A **greatest common divisor** of a and b is a nonzero element d, such that:

   (i) $d \mid a$ and $d \mid b$;

   (ii) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

   A greatest common divisor of a and b will be denoted by g.c.d.(a, b), or (abusing the notation) simply (a, b).

Multiples and Divisors in terms of Ideals

- Note that $b \mid a$ in a ring R if and only if $a \in (b)$ if and only if $(a) \subseteq (b)$.
- In particular, if d is any divisor of both a and b then (d) must contain both a and b and hence must contain the ideal generated by a and b.
- The defining properties (i) and (ii) of a greatest common divisor of a and b translated into the language of ideals become (respectively):

  If I is the ideal of R generated by a and b, then d is a greatest common divisor of a and b if:

  (i) I is contained in the principal ideal (d);
  (ii) If (d') is any principal ideal containing I, then $(d) \subseteq (d')$.
- Thus a greatest common divisor of a and b (if such exists) is a generator for the unique smallest principal ideal containing a and b.
- There are rings in which greatest common divisors do not exist.

Existence of Greatest Common Divisors

- The preceding discussion gives the following sufficient condition for the existence of a greatest common divisor:

Proposition

If a and b are nonzero elements in the commutative ring R, such that the ideal generated by a and b is a principal ideal (d), then d is a greatest common divisor of a and b.

- An integral domain in which every ideal (a, b) generated by two elements is principal is called a **Bezout Domain**.

  There are Bezout Domains containing nonprincipal (necessarily infinitely generated) ideals.
- The condition in the proposition is not a necessary condition:

  In $R = \mathbb{Z}[x]$, the elements 2 and x generate a maximal, nonprincipal ideal. Thus, $R = (1)$ is the unique principal ideal containing both 2 and x. So 1 is a greatest common divisor of 2 and x.

Uniqueness of Greatest Common Divisors

Proposition

Let R be an integral domain. If two elements d and d' of R generate the same principal ideal, i.e., $(d) = (d')$, then $d' = ud$, for some unit u in R. In particular, if d and d' are both greatest common divisors of a and b, then $d' = ud$, for some unit u.

- This is clear if either d or d' is zero. So we may assume d and d' are nonzero. Since $d \in (d')$, there is some $x \in R$, such that $d = xd'$. Since $d' \in (d)$, there is some $y \in R$, such that $d' = yd$. Thus, $d = xyd$. So $d(1 - xy) = 0$. Since $d \neq 0$, $xy = 1$. Hence, both x and y are units.

  The second assertion follows from the first since any two greatest common divisors of a and b generate the same principal ideal (they divide each other).

Algorithmic Computation of Greatest Common Divisors

Theorem

Let R be a Euclidean Domain and let a and b be nonzero elements of R. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a and b. Then:

(1) d is a greatest common divisor of a and b;

(2) the principal ideal (d) is the ideal generated by a and b. In particular, d can be written as an R-linear combination of a and b, i.e., there are elements x and y in R, such that $d = ax + by$.

- Since R is Euclidean, the ideal generated by a and b is principal. So a, b do have a greatest common divisor, namely any element which generates the (principal) ideal (a, b). Both parts of the theorem will follow, therefore, once we show $d = r_n$ generates this ideal, i.e., once we show that:
  (i) $d \mid a$ and $d \mid b$ (so $(a, b) \subseteq (d)$);
  (ii) d is an R-linear combination of a and b (so $(d) \subseteq (a, b)$).

Algorithmic Computation of GCDs (Cont'd)

- To prove that d divides both a and b, simply keep track of the divisibilities in the Euclidean Algorithm:
  - Starting from the $(n+1)$st equation, $r_{n-1} = q_{n+1}r_n$, we see that $r_n \mid r_{n-1}$. Clearly $r_n \mid r_n$.
  - By induction (from index n downwards to 0) assume r_n divides r_{k+1} and r_k. By the $(k+1)$st equation, $r_{k-1} = q_{k+1}r_k + r_{k+1}$. Since r_n divides both terms on the right hand side, we see that r_n also divides r_{k-1}.
  - From the 1st equation in the Euclidean Algorithm, r_n divides b.
  - Then from the 0th equation we get that r_n divides a.
- To prove that r_n is in the ideal (a, b) generated by a and b, proceed similarly by induction proceeding from the 0th equation to the nth equation.
  - It follows from the 0th equation that $r_0 \in (a, b)$. By the 1st equation, $r_1 = b - q_1 r_0 \in (b, r_0) \subseteq (a, b)$.
  - By induction assume $r_{k-1}, r_k \in (a, b)$. Then, by the $(k+1)$st equation $r_{k+1} = r_{k-1} - q_{k+1}r_k \in (r_{k-1}, r_k) \subseteq (a, b)$.

Thus, $r_n \in (a, b)$.

An Example

- If $a = 2210$ and $b = 1131$ then the smallest ideal of $\mathbb{Z}$ that contains both a and b (the ideal generated by a and b) is $13\mathbb{Z}$, since 13 is the greatest common divisor of 2210 and 1131.

  This follows quickly from the Euclidean Algorithm:

$$\begin{array}{rcl} 2210 & = & 1 \cdot 1131 + 1079 \\ 1131 & = & 1 \cdot 1079 + 52 \\ 1079 & = & 20 \cdot 52 + 39 \\ 52 & = & 1 \cdot 39 + 13 \\ 39 & = & 3 \cdot 13 \end{array}$$

  So $13 = (2210, 1131)$ is the last nonzero remainder.

An Example (Cont'd)

- We got

$$\begin{aligned} 2210 &= 1 \cdot 1131 + 1079 \\ 1131 &= 1 \cdot 1079 + 52 \\ 1079 &= 20 \cdot 52 + 39 \\ 52 &= 1 \cdot 39 + 13 \\ 39 &= 3 \cdot 13. \end{aligned}$$

Using the procedure of the theorem we can also write 13 as a linear combination of 2210 and 1131:

$$\begin{aligned} 13 &= 52 - 1 \cdot 39 \\ &= 52 - (1079 - 20 \cdot 52) \\ &= 21 \cdot 52 - 1079 \\ &= 21(1131 - 1079) - 1079 \\ &= 21 \cdot 1131 - 22 \cdot 1079 \\ &= 21 \cdot 1131 - 22(2210 - 1131) \\ &= 43 \cdot 1131 - 22 \cdot 2210. \end{aligned}$$

Solutions of the Diophantine Equation $ax + by = N$

- Integers x and y in $(a, b) = ax + by$ are not unique.
  - Indeed, $x' = x + b$ and $y' = y - a$ satisfy $(a, b) = ax' + by'$.
  - This is essentially the only possibility: If x_0 and y_0 are solutions to the equation $ax + by = N$, then any other solutions x and y to this equation are of the form $x = x_0 + m\frac{b}{(a,b)}$ and $y = y_0 - m - \frac{a}{(a,b)}$, for some integer m (positive or negative).
- We get a complete solution of the **First Order Diophantine Equation** $ax + by = N$, provided we know there is at least one solution:
  - The equation $ax + by = N$ states that N is an element of the ideal generated by a and b. We know this ideal is (d), the principal ideal generated by the greatest common divisor d of a and b. Thus, existence of a solution amounts to $N \in (d)$, i.e., N is divisible by d.
  - The equation $ax + by = N$ is solvable in integers x and y if and only if N is divisible by the g.c.d. of a and b. Then the result quoted above gives a full set of solutions of this equation.

Universal Side Divisors in Integral Domains

- For any integral domain R, let
$$\widetilde{R} = R^{\times} \cup \{0\}$$
denote the collection of units of R together with 0.
- An element $u \in R - \widetilde{R}$ is called a **universal side divisor** if, for every $x \in R$, there is some $z \in \widetilde{R}$, such that u divides $x - z$ in R,

  i.e., there is a type of "division algorithm" for u: every $x \in R$ may be written
$$x = qu + z, \text{ where } z \text{ is zero or a unit.}$$

Criterion for Failure of the Euclidean Property

- The existence of universal side divisors is weaker than being Euclidean:

Proposition

Let R be an integral domain that is not a field. If R is a Euclidean Domain then there are universal side divisors in R.

- Suppose R is Euclidean with respect to some norm N.

  Since R is not a field $R - \widetilde{R} \neq \emptyset$.

  Let u be an element of $R - \widetilde{R}$ of minimal norm.

  For any $x \in R$, write $x = qu + r$, where r is either 0 or $N(r) < N(u)$.

  In either case the minimality of u implies $r \in \widetilde{R}$.

  Hence u is a universal side divisor in R.

Using the Proposition

- We prove that the quadratic integer ring $R = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is not a Euclidean Domain with respect to any norm.

  The strategy is to show that R contains no universal side divisors.

  Since all ideals in R are principal, the preceding technique does not apply to this ring.

  We have already determined that ± 1 are the only units in R. So $\widetilde{R} = \{0, \pm 1\}$. Suppose $u \in R$ is a universal side divisor. Let $N(a + b\frac{1+\sqrt{-19}}{2}) = a^2 + ab + 5b^2$ denote the field norm on R. If $a, b \in \mathbb{Z}$ and $b \neq 0$, then $a^2 + ab + 5b^2 = (a + \frac{b}{2})^2 + \frac{19}{4}b^2 \geq 5$. So the smallest nonzero values of N on R are 1 (for the units ± 1) and 4 (for ± 2). Let $x = 2$ in the definition of a universal side divisor. Then u must divide one of $2 - 0$ or 2 ± 1 in R. I.e., u is a nonunit divisor of 2 or 3 in R.

Using the Proposition (Cont'd)

- u must be a nonunit divisor of 2 or 3:
  - If $2 = \alpha\beta$, then $4 = N(\alpha)N(\beta)$ and by the remark above it follows that one of α or β has norm 1, i.e., equals ± 1. Hence, the only divisors of 2 in R are $\{\pm 1, \pm 2\}$.
  - Similarly, the only divisors of 3 in R are $\{\pm 1, \pm 3\}$.

  So the only possible values for u are ± 2 or ± 3.

  Taking $x = \frac{1+\sqrt{-19}}{2}$, we may check (many cases but straightforward) that none of $x, x \pm 1$ are divisible by ± 2 or ± 3 in R, so none of these is a universal side divisor.

Subsection 2

Principal Ideal Domains

Principal Ideal Domains

Definition (Principal Ideal Domain)

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

- We proved that every Euclidean Domain is a Principal Ideal Domain.
- Hence every result about Principal Ideal Domains automatically holds for Euclidean Domains.

  Examples:

  (1) The integers $\mathbb{Z}$ form a P.I.D.

  The polynomial ring $\mathbb{Z}[x]$ contains nonprincipal ideals, so is not a P.I.D.

  (2) The quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is not a P.I.D.. In fact the ideal $(3, 1+\sqrt{-5})$ is a nonprincipal ideal.

  It is possible for the product IJ of two nonprincipal ideals I and J to be principal: E.g., the ideals $(3, 1+\sqrt{-5})$ and $(3, 1-\sqrt{-5})$ are both non principal, but $(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (3)$.
- It is not true that every Principal Ideal Domain is a Euclidean Domain. E.g., $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, which is not a Euclidean Domain, is a P.I.D.

Properties of Principal Ideal Domains

- Many of the properties enjoyed by Euclidean Domains are also satisfied by Principal Ideal Domains.
- A significant advantage of Euclidean Domains over Principal Ideal Domains, however, is that there exists an algorithm for computing greatest common divisors.

Proposition

Let R be a Principal Ideal Domain and let a and b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then:

(1) d is a greatest common divisor of a and b;

(2) d can be written as an R-linear combination of a and b, i.e., there are elements x and y in R, with $d = ax + by$;

(3) d is unique up to multiplication by a unit of R.

- The statements summarize preceding propositions.

Prime and Maximal Ideals in P.I.D.s

- Recall that maximal ideals are always prime ideals but the converse is not true in general.
- However, in $\mathbb{Z}$, every nonzero prime ideal is a maximal ideal.

Proposition

Every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

- Let (p) be a nonzero prime ideal in the Principal Ideal Domain R. Let $I = (m)$ be any ideal containing (p). We must show that $I = (p)$ or $I = R$. Now $p \in (m)$ so $p = rm$, for some $r \in R$. Since (p) is a prime ideal and $rm \in (p)$, either r or m must lie in (p).
  - If $m \in (p)$ then $(p) = (m) = I$.
  - If, on the other hand, $r \in (p)$, write $r = ps$. In this case $p = rm = psm$. So, since R is an integral domain, $sm = 1$. Thus, m is a unit and, hence, $I = R$.

Fields and their Polynomial Rings

- If F is a field, then the polynomial ring $F[x]$ is a Euclidean Domain. So, it is a Principal Ideal Domain.
- The converse to this is also true: Intuitively, if I is an ideal in R (such as the ideal (2) in $\mathbb{Z}$), then the ideal (I, x) in $R[x]$ (such as the ideal $(2, x)$ in $\mathbb{Z}[x]$) requires one more generator than does I. Hence, in general, it is not principal.

Corollary

If R is any commutative ring, such that the polynomial ring $R[x]$ is a Principal Ideal Domain (or a Euclidean Domain), then R is a field.

- Assume $R[x]$ is a Principal Ideal Domain. R is a subring of $R[x]$. Moreover, since $R[x]$ has an identity if and only if R does, R does have an identity. Hence, R must be an integral domain. The ideal (x) is a nonzero prime ideal in $R[x]$ because $R[x]/(x)$ is isomorphic to the integral domain R. By the preceding proposition, (x) is a maximal ideal. Hence, the quotient R is a field.

Dedekind-Hasse Norms

- The next result will be used to prove that not every P.I.D. is a Euclidean Domain.

Definition (Dedekind-Hasse Norm)

Define N to be a **Dedekind-Hasse norm** if N is a positive norm and, for every nonzero $a, b \in R$,

- either a is an element of the ideal (b)
- or there is a nonzero element in the ideal (a, b) of norm strictly smaller than the norm of b

(i.e., either $b \mid a$ in R or there exist $s, t \in R$, with $0 < N(sa - tb) < N(b)$).

- Suppose R is Euclidean with respect to a positive norm N.

  Then, it is always possible to satisfy the Dedekind-Hasse condition with $s = 1$.
- So this condition is a weakening of the Euclidean condition.

Principal Ideal Domains and Dedekind-Hasse Norms

Proposition

The integral domain R is a P.I.D. if and only if R has a Dedekind-Hasse norm.

- Assume that R has a Dedekind-Hasse norm N.

  Let I be any nonzero ideal in R.

  Let b be a nonzero element of I with $N(b)$ minimal.

  Suppose a is any nonzero element in I.

  Then the ideal (a, b) is contained in I.

  The Dedekind-Hasse condition on N and the minimality of b implies that $a \in (b)$. So $I = (b)$ is principal.

  The converse will be proved shortly.

A non-Euclidean P.I.D.

- Let $R = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ be the quadratic integer ring considered at the end of the previous section. We show that the positive field norm $N(a + b\frac{1+\sqrt{-19}}{2}) = a^2 + ab + 5b^2$ defined on R is a Dedekind-Hasse norm. By the proposition this will prove that R is a P.I.D. Suppose α, β are nonzero elements of R and $\frac{\alpha}{\beta} \notin R$. We must show that there are elements $s, t \in R$, with $0 < N(s\alpha - t\beta) < N(\beta)$, which by the multiplicativity of the field norm is equivalent to $0 < N(\frac{\alpha}{\beta}s - t) < 1$. Write $\frac{\alpha}{\beta} = \frac{a+b\sqrt{-19}}{c} \in \mathbb{Q}[\sqrt{-19}]$, with integers a, b, c having no common divisor and with $c > 1$ (since β is assumed not to divide α). Since a, b, c have no common divisor there are integers x, y, z, with $ax + by + cz = 1$. Write $ay - 19bx = cq + r$, for some quotient q and remainder r with $|r| \leq \frac{c}{2}$. Let $s = y + x\sqrt{-19}$, $t = q - z\sqrt{-19}$.

A non-Euclidean P.I.D. (Cont'd)

- Now we compute

$$\begin{array}{rcl} 0 & < & N(\frac{\alpha}{\beta}s-t) \\ & = & N(\frac{a+b\sqrt{-19}}{c}(y+x\sqrt{-19})-(q-z\sqrt{-19})) \\ & = & N(\frac{ay-19bx}{c}-q+(\frac{ax+by}{c}+z)\sqrt{-19}) \\ & = & \frac{(ay-19bx-cq)^2+19(ax+by+cz)^2}{c^2} \\ & = & \frac{r^2}{c^2}+\frac{19}{c^2} \\ & \leq & \frac{1}{4}+\frac{19}{c^2}. \end{array}$$

  This finishes the proof for $c \geq 5$.

- The case $c=2$: One of a, b must be even and the other odd (otherwise $\frac{\alpha}{\beta} \in R$). Let $s=1$, $t=\frac{(a-1)+b\sqrt{-19}}{2}$. Then $s, t \in R$ and

$$0 < N(\frac{\alpha}{\beta}s-t) = N(\frac{a+b\sqrt{-19}}{2}-\frac{(a-1)+b\sqrt{-19}}{2}) = N(\frac{1}{2}) = \frac{1}{4} < 1.$$

A non-Euclidean P.I.D. (Cont'd)

- The case $c = 3$: The integer $a^2 + 19b^2$ is not divisible by 3 (modulo 3 this is $a^2 + b^2$; this is 0 modulo 3 if and only if a and b are both 0 modulo 3; but then a, b, c have a common factor). Write $a^2 + 19b^2 = 3q + r$ with $r = 1$ or 2. Then $s = a - b\sqrt{-19}$, $t = q$ are elements of R that satisfy the required inequality.
- The case $c = 4$: a and b are not both even.
  - Suppose one of a, b is even and the other odd. Then $a^2 + 19b^2$ is odd. Write $a^2 + 19b^2 = 4q + r$, for some $q, r \in \mathbb{Z}$ and $0 < r < 4$. Then $s = a - b\sqrt{-19}$, $t = q$ satisfy the inequality.
  - Suppose a and b are both odd. Then $a^2 + 19b^2 = 1 + 3 \mod 8$. Write $a^2 + 19b^2 = 8q + 4$, for some $q \in \mathbb{Z}$. Then $s = \frac{a-b\sqrt{-19}}{2}$, $t = q$ are elements of R satisfying the inequality.

Subsection 3

Unique Factorization Domains

Factorization

- In $\mathbb{Z}$, another method for determining the greatest common divisor of two elements a and b is the "factorization into primes" for a and b, from which the greatest common divisor can easily be determined.
- This can also be extended to a larger class of rings called Unique Factorization Domains (U.F.D.s).
- Every Principal Ideal Domain is a Unique Factorization Domain.
- We saw every Euclidean Domain is a Principal Ideal Domain.
- Thus, every result about Unique Factorization Domains will automatically hold for both Euclidean Domains and Principal Ideal Domains.

Irreducible Elements, Prime Elements and Associates

Definition

Let R be an integral domain.

(1) Suppose $r \in R$ is nonzero and is not a unit. Then 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. In other words, a nonzero element p is a prime if it is not a unit and whenever $p \mid ab$, for any $a, b \in R$, then either $p \mid a$ or $p \mid b$.

(3) Two elements a and b of R differing by a unit are said to be **associate** in R, i.e., $a = ub$, for some unit u in R.

Prime Elements and Irreducible Elements

Proposition

In an integral domain a prime element is always irreducible.

- Suppose (p) is a nonzero prime ideal and $p = ab$. Then $ab = p \in (p)$. So, by definition of prime ideal, one of a or b, say a, is in (p). Thus, $a = pr$, for some r. This implies $p = ab = prb$. So $rb = 1$ and b is a unit. This shows that p is irreducible.
- It is not true in general that an irreducible element is necessarily prime:

  Example: Consider the element 3 in the quadratic integer ring $R = \mathbb{Z}[\sqrt{-5}]$.

  - 3 is irreducible in R;
  - 3 is not a prime: $(2+\sqrt{-5})(2-\sqrt{-5}) = 3^2$ is divisible by 3, but neither $2+\sqrt{-5}$ nor $2-\sqrt{-5}$ is divisible by 3 in R.

Prime and Irreducible Elements in P.I.D.s

- If R is a Principal Ideal Domain, the notions of prime and irreducible elements are the same.

  In particular these notions coincide in $\mathbb{Z}$ and in $F[x]$ (F a field).

Proposition

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

- We have shown above that prime implies irreducible. We must show conversely that if p is irreducible, then p is a prime, i.e., the ideal (p) is a prime ideal. We show that (p) is, in fact, maximal.

  Suppose M is any ideal containing (p). By hypothesis, $M = (m)$ is a principal ideal. Since $p \in (m)$, $p = rm$, for some r. But p is irreducible. So, by definition, either r or m is a unit. This means either $(p) = (m)$ or $(m) = (1)$, respectively. Thus, the only ideals containing (p) are (p) or (1), i.e., (p) is a maximal ideal.

Prime Factorization in the Integers

Example: Since 3 is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$, by the proposition, this quadratic integer ring is not a P.I.D.

- The irreducible elements in the integers $\mathbb{Z}$ are the prime numbers (and their negatives) familiar from elementary arithmetic; Two integers a and b are associates of one another if and only if $a = \pm b$.
- In the integers $\mathbb{Z}$, any integer n can be written as a product of primes (not necessarily distinct), as follows: If n is not itself a prime, then by definition it is possible to write $n = n_1 n_2$, for two other integers n_1 and n_2 neither of which is a unit, i.e., neither of which is ± 1. Both n_1 and n_2 must be smaller in absolute value than n itself. If they are both primes, we have already written n as a product of primes. If one of n_1 or n_2 is not prime, then it, in turn, can be factored into two (smaller) integers. Integers cannot decrease in absolute value indefinitely. So, we must, at some point, be left only with prime integer factors. I.e., we have written n as a product of primes.

An Example of Prime Factorization in the Integers

Example: If $n = 2210$, the algorithm above proceeds as follows: n is not itself prime, since we can write $n = 2 \cdot 1105$. The integer 2 is a prime, but 1105 is not: $1105 = 5 \cdot 221$. The integer 5 is prime, but 221 is not: $221 = 13 \cdot 17$. Here the algorithm terminates, since both 13 and 17 are primes. The prime factorization is $2210 = 2 \cdot 5 \cdot 13 \cdot 17$. Similarly, we find $1131 = 3 \cdot 13 \cdot 29$. Generally, each prime need not occur only to the first power.

- In the ring $\mathbb{Z}$ not only is it true that every integer n can be written as a product of primes, but in fact this decomposition is unique in the sense that any two prime factorizations of the same positive integer n differ only in the order in which the positive prime factors are written. The restriction to positive integers is to avoid considering the factorizations $(3)(5)$ and $(-3)(-5)$ of 15 as essentially distinct.
- This *unique factorization property* of $\mathbb{Z}$ is extremely useful for the arithmetic of the integers.

Unique Factorization Domains

Definition

A **Unique Factorization Domain** (U.F.D.) is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:

(i) r can be written as a finite product of irreducibles p_i of R (not necessarily distinct): $r = p_1 p_2 \cdots p_n$;

(ii) the decomposition in (i) is unique up to associates: namely, if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles, then $m = n$ and there is some renumbering of the factors so that p_i is associate to q_i for $i = 1, 2, \ldots, n$.

Example:

(1) A field F is trivially a Unique Factorization Domain: In F, every nonzero element is a unit. So there are no elements for which properties (i) and (ii) must be verified.

The Polynomial Ring $\mathbb{Z}[x]$

(2) As indicated above, we shall prove shortly that every Principal Ideal Domain is a Unique Factorization Domain.

In particular, $\mathbb{Z}$ and $F[x]$, where F is a field, are both Unique Factorization Domains.

(3) We will prove that the ring $R[x]$ of polynomials is a Unique Factorization Domain whenever R itself is a Unique Factorization Domain.

Contrast this to the properties of being a Principal Ideal Domain or being a Euclidean Domain, which do not carry over from a ring R to the polynomial ring $R[x]$.

This result together with the preceding example will show that $\mathbb{Z}[x]$ is a Unique Factorization Domain.

The Gaussian Integers $\mathbb{Z}[i]$

(4) The subring of the Gaussian integers

$$R = \mathbb{Z}[2i] = \{a + 2bi : a, b \in \mathbb{Z}\},$$

where $i^2 = -1$, is an integral domain but not a Unique Factorization Domain:

- The elements 2 and $2i$ are irreducibles which are not associates in R since $i \notin R$;
- $4 = 2 \cdot 2 = (-2i) \cdot (2i)$ has two distinct factorizations in R.

One may also check directly that $2i$ is irreducible but not prime in R (since $R/(2i) \cong \mathbb{Z}/4\mathbb{Z}$).

In the larger ring of Gaussian integers, $\mathbb{Z}[i]$, (which is a Unique Factorization Domain) 2 and $2i$ are associates since i is a unit in this larger ring.

The Quadratic Integer Ring $\mathbb{Z}[\sqrt{-5}]$

(5) The quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is another example of an integral domain that is not a Unique Factorization Domain:

- $2, 3, 1-\sqrt{5}, 1+\sqrt{5}$ are irreducibles;
- $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ gives two distinct factorizations of 6 into irreducibles.

The principal ideal (6) in $\mathbb{Z}[\sqrt{-5}]$ can be written as a product of 4 nonprincipal prime ideals: $(6) = P_2^2 P_3 P_3'$.

The two distinct factorizations of the element 6 in $\mathbb{Z}[\sqrt{-5}]$ can be interpreted as arising from two rearrangements of this product of ideals into products of principal ideals:

- The product of $P_2^2 = (2)$ with $P_3 P_3' = (3)$;
- The product of $P_2 P_3 = (1+\sqrt{-5})$ with $P_2 P_3' = (1-\sqrt{-5})$.

Prime and Irreducible Elements in U.F.D.s

Proposition

In a Unique Factorization Domain a nonzero element is a prime if and only if it is irreducible.

- Let R be a Unique Factorization Domain. We have already shown that primes of R are irreducible. For the converse, let p be an irreducible in R and assume $p \mid ab$, for some $a, b \in R$. We must show that p divides either a or b. Since p divides ab, $ab = pc$, for some c in R. Write a and b as a product of irreducibles. By the uniqueness of the decomposition into irreducibles of ab, p must be associate to one of the irreducibles occurring either in the factorization of a or in the factorization of b. We may assume that p is associate to one of the irreducibles in the factorization of a. So a can be written as $a = (up)p_2 \cdots p_n$, for u a unit and some (possibly empty set of) irreducibles $p_2, \ldots, p_n$. But then $a = pd$, with $d = up_2 \cdots p_n$. Hence, p divides a.

Greatest Common Divisors in U.F.D.s

Proposition

Let a and b be two nonzero elements of the Unique Factorization Domain R and suppose $a = up_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$ and $b = vp_1^{f_1}p_2^{f_2}\cdots p_n^{f_n}$ are prime factorizations for a and b, where u and v are units, the primes $p_1, p_2, \ldots, p_n$ are distinct and the exponents e_i and f_i are ≥ 0. Then the element $d = p_1^{\min(e_1,f_1)}p_2^{\min(e_2,f_2)}\cdots p_n^{\min(e_n,f_n)}$ (where $d = 1$ if all the exponents are 0) is a greatest common divisor of a and b.

- Clearly, d divides both a and b. Let c be a common divisor of a and b. Let $c = q_1^{g_1}q_2^{g_2}\cdots q_m^{g_m}$ be the prime factorization of c. Each q_i divides c. By the preceding proposition, q_i divides a and b. Thus, q_i must divide one of the primes p_j. In particular, up to associates, the primes occurring in c must be a subset of the primes occurring in a and b, i.e., $\{q_1, q_2, \ldots, q_m\} \subseteq \{p_1, p_2, \ldots, p_n\}$. Similarly, the exponents for the primes occurring in c must be no larger than those occurring in d. This implies that c divides d.

P.I.D.s and U.F.D.s

Theorem

Every Principal Ideal Domain is a Unique Factorization Domain. In particular, every Euclidean Domain is a Unique Factorization Domain.

- Let R be a Principal Ideal Domain and let r be a nonzero element of R which is not a unit. We show first that r can be written as a finite product of irreducible elements of R. If r is itself irreducible, then we are done. If not, then by definition r can be written as a product $r = r_1 r_2$, where neither r_1 nor r_2 is a unit. If both these elements are irreducibles, then again we are done, having written r as a product of irreducible elements. Otherwise, at least one of the two elements, say r_1 is reducible. Hence r_1 can be written as a product of two nonunit elements $r_1 = r_{11} r_{12}$, and so forth.

P.I.D.s and U.F.D.s (Termination)

- This process terminates: Suppose this is not the case. From the factorization $r = r_1 r_2$, we obtain a proper inclusion of ideals: $(r) \subset (r_1) \subset R$. The first inclusion is proper since r_2 is not a unit, and the last inclusion is proper since r_1 is not a unit. From the factorization of r_1, we similarly obtain $(r) \subset (r_1) \subset (r_{11}) \subset R$. If this process of factorization did not terminate after a finite number of steps, then we would obtain an infinite ascending chain of ideals:

$$(r) \subset (r_1) \subset (r_{11}) \subset \cdots \subset R,$$

where all containments are proper.

P.I.D.s and U.F.D.s (Chain Becomes Stationary)

- We now show that any ascending chain $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$ of ideals in a Principal Ideal Domain eventually becomes stationary, i.e., there is some positive integer n, such that $I_k = I_n$, for all $k \geq n$.

  In particular, it is not possible to have an infinite ascending chain of ideals where all containments are proper.

  Let $I = \bigcup_{i=1}^{\infty} I_i$. It follows easily that I is an ideal. Since R is a Principal Ideal Domain it is principally generated, say $I = (a)$. Since I is the union of the ideals above, a must be an element of one of the ideals in the chain, say $a \in I_n$. But then we have $I_n \subseteq I = (a) \subseteq I_n$. So $I = I_n$ and the chain becomes stationary at I_n.

  This proves that every nonzero element of R which is not a unit has some factorization into irreducibles in R.

P.I.D.s and U.F.D.s (Uniqueness)

- To show uniqueness of the decomposition, we proceed by induction on the number n of irreducible factors in some factorization of r.
  - If $n = 0$, then r is a unit.
    If we had $r = qc$ (some other factorization) for some irreducible q, then q would divide a unit, hence would itself be a unit, a contradiction.
  - Let $n \geq 1$ and $r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, $m \geq n$, where the p_i and q_j are (not necessarily distinct) irreducibles.
    Since then p_1 divides the product on the right, p_1 must divide one of the factors. Renumbering if necessary, we may assume p_1 divides q_1. But then $q_1 = p_1 u$, for some element u of R. Since q_1 is irreducible, u must be a unit. Thus, p_1 and q_1 are associates.
    Canceling p_1 (legitimate in an integral domain), we obtain the equation $p_2 \cdots p_n = uq_2 q_3 \cdots q_m = q_2' q_3 \cdots q_m$, $m \geq n$, where $q_2' = uq_2$ is again an irreducible (associate to q_2). By induction on n, we conclude that each of the factors on the left matches bijectively (up to associates) with the factors on the far right. And with the factors in the middle (which are the same, up to associates). p_1 and q_1 (after the initial renumbering) have already been shown to be associate.

The Fundamental Theorem of Arithmetic

Corollary (Fundamental Theorem of Arithmetic)

The integers $\mathbb{Z}$ are a Unique Factorization Domain.

- The integers $\mathbb{Z}$ are a Euclidean Domain.

  By the Theorem, they are a Unique Factorization Domain.

Multiplicative Dedekind-Hasse Norms in P.I.D.s

Corollary

Let R be a P.I.D. Then there exists a multiplicative Dedekind-Hasse norm on R.

- If R is a P.I.D., then R i s a U.F.D. Define the norm N by setting:

$$\begin{array}{rcl} N(0) & = & 0; \\ N(u) & = & 1, \text{ if } u \text{ is a unit;} \\ N(a) & = & 2^n, \text{ if } a = p_1 p_2 \cdots p_n \text{ where the } p_i \\ & & \qquad\qquad \text{are irreducibles in } R. \end{array}$$

  N is well defined since the number of irreducible factors of a is unique.

  Clearly $N(ab) = N(a)N(b)$.

  So N is positive and multiplicative.

Multiplicative Dedekind-Hasse Norms in P.I.D.s (Cont'd)

- To show that N is a Dedekind-Hasse norm, suppose that a, b are nonzero elements of R.

  The ideal generated by a and b is principal by assumption, say $(a, b) = (r)$.

  If a is not contained in the ideal (b), then also r is not contained in (b), i.e., r is not divisible by b.

  But $b = xr$, for some $x \in R$. So x is not a unit in R.

  Thus, $N(b) = N(x)N(r) > N(r)$.

  Hence, (a, b) contains a nonzero element with norm strictly smaller than the norm of b.