Introduction to Modern Algebra

Part IX. Factorization

IX.46. Euclidean Domains

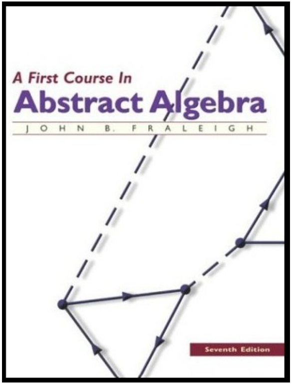

Table of contents

Theorem 46.4.

Theorem. 46.4. Every Euclidean domain is a PID.

Proof. Let D be a Euclidean domain with a Euclidean norm v and let N be an ideal in D. If $N = \{0\}$, then $N = \langle 0 \rangle$ and N is principal. Suppose that $N \neq \{0\}$. Then there exists $b \neq 0$ in N.

Theorem 46.4.

Theorem. 46.4. Every Euclidean domain is a PID.

Proof. Let D be a Euclidean domain with a Euclidean norm v and let N be an ideal in D. If $N = \{0\}$, then $N = \langle 0 \rangle$ and N is principal. Suppose that $N \neq \{0\}$. Then there exists $b \neq 0$ in N. Choose a nonzero $b \in N$ such that $v(b)$ is minimal among all $v(n)$ for $n \in N$ (this can be done since v is defined on the nonzero elements of D and v takes on nonnegative integer values).

Theorem 46.4.

Theorem. 46.4. Every Euclidean domain is a PID.

Proof. Let D be a Euclidean domain with a Euclidean norm v and let N be an ideal in D. If $N = \{0\}$, then $N = \langle 0 \rangle$ and N is principal. Suppose that $N \neq \{0\}$. Then there exists $b \neq 0$ in N. Choose a nonzero $b \in N$ such that $v(b)$ is minimal among all $v(n)$ for $n \in N$ (this can be done since v is defined on the nonzero elements of D and v takes on nonnegative integer values). We now show that $\langle b \rangle = N$. Let $a \in N$. By Condition 1 for a Euclidean domain, there exists q and r in D such that $a = bq + r$ where either $r = 0$ or $v(r) < v(b)$.

Theorem 46.4.

Theorem. 46.4. Every Euclidean domain is a PID.

Proof. Let D be a Euclidean domain with a Euclidean norm v and let N be an ideal in D. If $N = \{0\}$, then $N = \langle 0 \rangle$ and N is principal. Suppose that $N \neq \{0\}$. Then there exists $b \neq 0$ in N. Choose a nonzero $b \in N$ such that $v(b)$ is minimal among all $v(n)$ for $n \in N$ (this can be done since v is defined on the nonzero elements of D and v takes on nonnegative integer values). We now show that $\langle b \rangle = N$. Let $a \in N$. By Condition 1 for a Euclidean domain, there exists q and r in D such that $a = bq + r$ where either $r = 0$ or $v(r) < v(b)$. Now $r = a - bq$ where $a, b \in N$. We have $b(-q) = -bq \in N$ since N is an ideal (recall N is an ideal if $xN \subseteq N$ and $Ny \subseteq N$ for all $x, y \in D$).

Theorem 46.4.

Theorem. 46.4. Every Euclidean domain is a PID.

Proof. Let D be a Euclidean domain with a Euclidean norm v and let N be an ideal in D. If $N = \{0\}$, then $N = \langle 0 \rangle$ and N is principal. Suppose that $N \neq \{0\}$. Then there exists $b \neq 0$ in N. Choose a nonzero $b \in N$ such that $v(b)$ is minimal among all $v(n)$ for $n \in N$ (this can be done since v is defined on the nonzero elements of D and v takes on nonnegative integer values). We now show that $\langle b \rangle = N$. Let $a \in N$. By Condition 1 for a Euclidean domain, there exists q and r in D such that $a = bq + r$ where either $r = 0$ or $v(r) < v(b)$. Now $r = a - bq$ where $a, b \in N$. We have $b(-q) = -bq \in N$ since N is an ideal (recall N is an ideal if $xN \subseteq N$ and $Ny \subseteq N$ for all $x, y \in D$).

Theorem 46.4. (Continued)

Theorem. 46.4. Every Euclidean domain is a PID.

Proof. (Continued) So $r = a - bq \in N$ ("clearly" N is closed under addition by the definition of ideal). But then $v(r) < v(b)$ is impossible since $v(b)$ is maximal over all nonzero elements of N, under $r = 0$. Then $a = bq$ and $a \in \langle b \rangle$. Therefore $N = \langle b \rangle$, that is N is a principal ideal, and D is a PID. □

Theorem 46.4. (Continued)

Theorem. 46.4. Every Euclidean domain is a PID.

Proof. (Continued) So $r = a - bq \in N$ ("clearly" N is closed under addition by the definition of ideal). But then $v(r) < v(b)$ is impossible since $v(b)$ is maximal over all nonzero elements of N, under $r = 0$. Then $a = bq$ and $a \in \langle b \rangle$. Therefore $N = \langle b \rangle$, that is N is a principal ideal, and D is a PID. □

Theorem 46.6.

Theorem. 46.6. For a Euclidean domain with a Euclidean norm $v, v(1)$ is minimal among all $v(a)$ nonzero $a \in D$, and $u \in D$ is a unit if and only if $v(u) = v(1)$.

Proof. Condition 2 implies that for nonzero $a \in D$ we have $v(1) \leq v(1a) = v(a)$, so $v(1)$ is minimal. Next, if u is a unit in D, with inverse u^{-1}, then $v(u) \leq v(uu^{-1} = v(1)$ and since $v(1)$ is minimal then $v(u) = v(1)$.

Theorem 46.6.

Theorem. 46.6. For a Euclidean domain with a Euclidean norm $v, v(1)$ is minimal among all $v(a)$ nonzero $a \in D$, and $u \in D$ is a unit if and only if $v(u) = v(1)$.

Proof. Condition 2 implies that for nonzero $a \in D$ we have $v(1) \leq v(1a) = v(a)$, so $v(1)$ is minimal. Next, if u is a unit in D, with inverse u^{-1}, then $v(u) \leq v(uu^{-1} = v(1)$ and since $v(1)$ is minimal then $v(u) = v(1)$.

Now suppose $v(u) = v(1)$ for nonzero $u \in D$. Then by Condition 1 there exists $q, v \in D$ such that $1 = uq + r$ where either $r = 0$ or $v(v) < v(u)$.

Theorem 46.6.

Theorem. 46.6. For a Euclidean domain with a Euclidean norm $v, v(1)$ is minimal among all $v(a)$ nonzero $a \in D$, and $u \in D$ is a unit if and only if $v(u) = v(1)$.

Proof. Condition 2 implies that for nonzero $a \in D$ we have $v(1) \leq v(1a) = v(a)$, so $v(1)$ is minimal. Next, if u is a unit in D, with inverse u^{-1}, then $v(u) \leq v(uu^{-1} = v(1)$ and since $v(1)$ is minimal then $v(u) = v(1)$.

Now suppose $v(u) = v(1)$ for nonzero $u \in D$. Then by Condition 1 there exists $q, v \in D$ such that $1 = uq + r$ where either $r = 0$ or $v(v) < v(u)$. But since $v(1) = v(u)$ is minimal, then it must be that $r = 0$ and $1 = uq$. So g is an inverse of u and u is a unit. □

Theorem 46.6.

Theorem. 46.6. For a Euclidean domain with a Euclidean norm $v, v(1)$ is minimal among all $v(a)$ nonzero $a \in D$, and $u \in D$ is a unit if and only if $v(u) = v(1)$.

Proof. Condition 2 implies that for nonzero $a \in D$ we have $v(1) \leq v(1a) = v(a)$, so $v(1)$ is minimal. Next, if u is a unit in D, with inverse u^{-1}, then $v(u) \leq v(uu^{-1} = v(1)$ and since $v(1)$ is minimal then $v(u) = v(1)$.

Now suppose $v(u) = v(1)$ for nonzero $u \in D$. Then by Condition 1 there exists $q, v \in D$ such that $1 = uq + r$ where either $r = 0$ or $v(v) < v(u)$. But since $v(1) = v(u)$ is minimal, then it must be that $r = 0$ and $1 = uq$. So g is an inverse of u and u is a unit. □

Theorem 46.9. Euclidean Algorithm

Theorem. 46.9. Euclidean Algorithm Let D be a Euclidean domain with a Euclidean norm v, and let a and b be nonzero elements of D. Let r_1 be as in Condition 1 for a Euclidean norm, that is $a = bq_1 + r_1$ where either $r_1 = 0$ or $v(r_1) < v(b)$. If $r_1 \neq 0$, let r_2 be such that $b = r_1 q_2 + r_2$ where either $r_2 = 0$ or $v(r_2) < v(r_1)$. Recursively, let r_{i+1} be such that $r_{i-1} = r_i q_{i+1} + r_{i+1}$ where either $r_{i+1} = 0$ or $v(r_{i+1}) < v(r_i)$. Then the sequence $r_1, r_2, \ldots$ must terminate with some $r_3 = 0$. If $r_1 = 0$, then b is a gcd of a and b. If $r_1 \neq 0$ and $r_s = 0$ is the first $r_i = 0$ then a gcd of a and b is r_{s-1}. Furthermore, if d is a gcd of a and b, then there exist λ and μ in D such that $d = \lambda a + \mu b$.

Theorem 46.9. Euclidean Algorithm

Theorem. 46.9. Euclidean Algorithm

Proof. Since $v(r_i) < v(r_{i-1})$ and $v(r_i)$ is a nonnegative integer, then after some finite number of steps we must arrive at a point where we cannot have $v(r_s) < v(r_{s-1})$ and so $r_s = 0$.
If $r_1 = 0$ then $a = bq_1$ and b is a gcd of a and b. Suppose $r_1 \neq 0$. (1) Then if $d \mid a$ and $d \mid b$ we have $d \mid (a - bq_1)$ and so $d \mid r_1$ since $r_1 = a - bq_1$. (2) But if $d_1 \mid r_1$ and $d_1 \mid b$ then $d_1 \mid (bq_1 + r_1)$ and so $d_1 \mid a$ since $a = bq_1 + r_1$.

Theorem 46.9. Euclidean Algorithm

Theorem. 46.9. Euclidean Algorithm

Proof. Since $v(r_i) < v(r_{i-1})$ and $v(r_i)$ is a nonnegative integer, then after some finite number of steps we must arrive at a point where we cannot have $v(r_s) < v(r_{s-1})$ and so $r_s = 0$.
If $r_1 = 0$ then $a = bq_1$ and b is a gcd of a and b. Suppose $r_1 \neq 0$. (1) Then if $d \mid a$ and $d \mid b$ we have $d \mid (a - bq_1)$ and so $d \mid r_1$ since $r_1 = a - bq_1$. (2) But if $d_1 \mid r_1$ and $d_1 \mid b$ then $d_1 \mid (bq_1 + r_1)$ and so $d_1 \mid a$ since $a = bq_1 + r_1$. These two conditions show that the set of commons divisors of a and b is the same set as the set of commons divisors of b and r_1.

Theorem 46.9. Euclidean Algorithm

Theorem. 46.9. Euclidean Algorithm

Proof. Since $v(r_i) < v(r_{i-1})$ and $v(r_i)$ is a nonnegative integer, then after some finite number of steps we must arrive at a point where we cannot have $v(r_s) < v(r_{s-1})$ and so $r_s = 0$.
If $r_1 = 0$ then $a = bq_1$ and b is a gcd of a and b. Suppose $r_1 \neq 0$. (1) Then if $d \mid a$ and $d \mid b$ we have $d \mid (a - bq_1)$ and so $d \mid r_1$ since $r_1 = a - bq_1$. (2) But if $d_1 \mid r_1$ and $d_1 \mid b$ then $d_1 \mid (bq_1 + r_1)$ and so $d_1 \mid a$ since $a = bq_1 + r_1$. These two conditions show that the set of commons divisors of a and b is the same set as the set of commons divisors of b and r_1. In general, we have hypothesized that $r_{i-1} = r_i q_{i+1} + r_{i+1}$ so we similarly have (replacing a with r_{i-1}, b with r_i, q_1 with q_{i+1}, and r_1 with r_{i+1}) that if $r_{i+1} \neq 0$ then the set of common divisors of r_{i-1} and r_i is the same as the set of commons divisors of r_i and r_{i+1}.

Theorem 46.9. Euclidean Algorithm

Theorem. 46.9. Euclidean Algorithm

Proof. Since $v(r_i) < v(r_{i-1})$ and $v(r_i)$ is a nonnegative integer, then after some finite number of steps we must arrive at a point where we cannot have $v(r_s) < v(r_{s-1})$ and so $r_s = 0$.
If $r_1 = 0$ then $a = bq_1$ and b is a gcd of a and b. Suppose $r_1 \neq 0$. (1) Then if $d \mid a$ and $d \mid b$ we have $d \mid (a - bq_1)$ and so $d \mid r_1$ since $r_1 = a - bq_1$. (2) But if $d_1 \mid r_1$ and $d_1 \mid b$ then $d_1 \mid (bq_1 + r_1)$ and so $d_1 \mid a$ since $a = bq_1 + r_1$. These two conditions show that the set of commons divisors of a and b is the same set as the set of commons divisors of b and r_1. In general, we have hypothesized that $r_{i-1} = r_i q_{i+1} + r_{i+1}$ so we similarly have (replacing a with r_{i-1}, b with r_i, q_1 with q_{i+1}, and r_1 with r_{i+1}) that if $r_{i+1} \neq 0$ then the set of common divisors of r_{i-1} and r_i is the same as the set of commons divisors of r_i and r_{i+1}.

Theorem 46.9. Euclidean Algorithm (Continued)

Theorem. 46.9. Euclidean Algorithm

Proof. (Continued) So inductively, the set of common divisors of a and b (say, when $i = D$ set $r_{-1} = a$ and $r_0 = b$) is the same as the set of common divisors of r_{s-2} and r_{s-1} (with $i = s - 2$), where r_s is the first r_i equal to 0. Then a gcd of r_{s-2} and r_{s-1} is also a gcd of a and b. But we have

$$r_{s-2} = r_{s-1}q_s + r_s = q_s r_{s-1} \tag{1}$$

since $r_s = 0$, a a gcd of r_{s-2} and r_{s-1} in r_{s-1}.

Theorem 46.9. Euclidean Algorithm (Continued)

Theorem. 46.9. Euclidean Algorithm

Proof. (Continued) So inductively, the set of common divisors of a and b (say, when $i = D$ set $r_{-1} = a$ and $r_0 = b$) is the same as the set of common divisors of r_{s-2} and r_{s-1} (with $i = s - 2$), where r_s is the first r_i equal to 0. Then a gcd of r_{s-2} and r_{s-1} is also a gcd of a and b. But we have

$$r_{s-2} = r_{s-1}q_s + r_s = q_s r_{s-1} \tag{1}$$

since $r_s = 0$, a a gcd of r_{s-2} and r_{s-1} in r_{s-1}.

Theorem 46.9. Euclidean Algorithm (Continued)

Theorem. 46.9. Euclidean Algorithm

Proof. (Continued) Now for the "furthermore" claim. That is, if d is a gcd of 'a' and b then $d = \lambda a + \mu b$ for some $\lambda, \mu \in D$. If $d = b$ (and $r_1 = 0$) then $d = 0a + 1b$ and we are done. If $d = r_s$ then working backward through the equations given above, we can inductively express each r_i in the form $r_i = \lambda_i r_{i-1} + \mu_i r_{i-2}$ for some $\lambda_i, \mu_i \in D$ (namely, since we hypothesize $r_{i-1} = r_i q_{i+1} + r_{i+1}$ OR $r_{i-2} = r_{i-1} q_i + r_i$, we have $r_i = -q_i r_{i-1} + r_{i-2}$, so we take $\lambda_i = -q_i$ and $\mu_i = 1$).

Theorem 46.9. Euclidean Algorithm (Continued)

Theorem. 46.9. Euclidean Algorithm

Proof. (Continued) Now for the "furthermore" claim. That is, if d is a gcd of 'a' and b then $d = \lambda a + \mu b$ for some $\lambda, \mu \in D$. If $d = b$ (and $r_1 = 0$) then $d = 0a + 1b$ and we are done. If $d = r_s$ then working backward through the equations given above, we can inductively express each r_i in the form $r_i = \lambda_i r_{i-1} + \mu_i r_{i-2}$ for some $\lambda_i, \mu_i \in D$ (namely, since we hypothesize $r_{i-1} = r_i q_{i+1} + r_{i+1}$ OR $r_{i-2} = r_{i-1} q_i + r_i$, we have $r_i = -q_i r_{i-1} + r_{i-2}$, so we take $\lambda_i = -q_i$ and $\mu_i = 1$). So we have

$$\begin{aligned} d = r_{s-1} &= \lambda_{s-1} r_{s-2} + \mu_{s-1} r_{s-3} \\ &= \lambda_{s-1}(\lambda_{s-2} r_{s-3} + \mu_{s-2} r_{s-4}) + \mu_{s-1} r_{s-3} \\ &= (\lambda_{s-1}\lambda_{s-2} + \mu_{s-1}) r_{s-3} + \mu_{s-2} r_{s-4} \end{aligned} \tag{2}$$

which can be written in the form of a "linear combination" of r_{s-3} and r_{s-4}, then as a "linear combination of r_{s-4} and r_{s-5}.

Theorem 46.9. Euclidean Algorithm (Continued)

Theorem. 46.9. Euclidean Algorithm

Proof. (Continued) Now for the "furthermore" claim. That is, if d is a gcd of 'a' and b then $d = \lambda a + \mu b$ for some $\lambda, \mu \in D$. If $d = b$ (and $r_1 = 0$) then $d = 0a + 1b$ and we are done. If $d = r_s$ then working backward through the equations given above, we can inductively express each r_i in the form $r_i = \lambda_i r_{i-1} + \mu_i r_{i-2}$ for some $\lambda_i, \mu_i \in D$ (namely, since we hypothesize $r_{i-1} = r_i q_{i+1} + r_{i+1}$ OR $r_{i-2} = r_{i-1} q_i + r_i$, we have $r_i = -q_i r_{i-1} + r_{i-2}$, so we take $\lambda_i = -q_i$ and $\mu_i = 1$). So we have

$$\begin{aligned} d &= r_{s-1} = \lambda_{s-1} r_{s-2} + \mu_{s-1} r_{s-3} \\ &= \lambda_{s-1}(\lambda_{s-2} r_{s-3} + \mu_{s-2} r_{s-4}) + \mu_{s-1} r_{s-3} \\ &= (\lambda_{s-1}\lambda_{s-2} + \mu_{s-1}) r_{s-3} + \mu_{s-2} r_{s-4} \end{aligned} \tag{2}$$

which can be written in the form of a "linear combination" of r_{s-3} and r_{s-4}, then as a "linear combination of r_{s-4} and r_{s-5}.

Theorem 46.9. Euclidean Algorithm (Continued)

Theorem. 46.9. Euclidean Algorithm

Proof. (Continued) Continuing this process (inductively) we get d as a linear combination of $a = r_{-1}$ and $b = r_0$: $d = \lambda a + \mu b$ for some $\lambda, \mu \in D$. Finally, if d' is any other gcd of a and b then $d' = du$ for some unit $u \in D$ (see the note after Definition 45.19), so $d' = (\lambda u)a + (\mu u)b$. □