EXERCISES 46

Computations

In Exercises 1 through 5, state whether the given function ν is a Euclidean norm for the given integral domain.

1. The function ν for $\mathbb{Z}$ given by $\nu(n) = n^2$ for nonzero $n \in \mathbb{Z}$
2. The function ν for $\mathbb{Z}[x]$ given by $\nu(f(x)) =$ (degree of $f(x)$) for $f(x) \in \mathbb{Z}[x]$, $f(x) \neq 0$
3. The function ν for $\mathbb{Z}[x]$ given by $\nu(f(x)) =$ (the absolute value of the coefficient of the highest degree nonzero term of $f(x)$) for nonzero $f(x) \in \mathbb{Z}[x]$
4. The function ν for $\mathbb{Q}$ given by $\nu(a) = a^2$ for nonzero $a \in \mathbb{Q}$
5. The function ν for $\mathbb{Q}$ given by $\nu(a) = 50$ for nonzero $a \in \mathbb{Q}$
6. By referring to Example 46.11, actually express the gcd 23 in the form $\lambda(22,471) + \mu(3,266)$ for $\lambda, \mu \in \mathbb{Z}$. [*Hint:* From the next to the last line of the computation in Example 46.11, $23 = (138)3 - 391$. From the line before that, $138 = 3,266 - (391)8$, so substituting, you get $23 = [3,266 - (391)8]3 - 391$, and so on. That is, work your way back up to actually find values for λ and μ.]
7. Find a gcd of 49,349 and 15,555 in $\mathbb{Z}$.
8. Following the idea of Exercise 6 and referring to Exercise 7, express the positive gcd of 49,349 and 15,555 in $\mathbb{Z}$ in the form $\lambda(49,349) + \mu(15,555)$ for $\lambda, \mu \in \mathbb{Z}$.
9. Find a gcd of

$$x^{10} - 3x^9 + 3x^8 - 11x^7 + 11x^6 - 11x^5 + 19x^4 - 13x^3 + 8x^2 - 9x + 3$$

and

$$x^6 - 3x^5 + 3x^4 - 9x^3 + 5x^2 - 5x + 2$$

in $\mathbb{Q}[x]$.

10. Describe how the Euclidean Algorithm can be used to find the gcd of n members $a_1, a_2, \cdots, a_n$ of a Euclidean domain.
11. Using your method devised in Exercise 10, find the gcd of 2178, 396, 792, and 726.

Concepts

12. Let us consider $\mathbb{Z}[x]$.
    - **a.** Is $\mathbb{Z}[x]$ a UFD? Why?
    - **b.** Show that $\{a + xf(x) \mid a \in 2\mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$ is an ideal in $\mathbb{Z}[x]$.
    - **c.** Is $\mathbb{Z}[x]$ a PID? (Consider part (b).)
    - **d.** Is $\mathbb{Z}[x]$ a Euclidean domain? Why?
13. Mark each of the following true or false.
    - _____ **a.** Every Euclidean domain is a PID.
    - _____ **b.** Every PID is a Euclidean domain.
    - _____ **c.** Every Euclidean domain is a UFD.
    - _____ **d.** Every UFD is a Euclidean domain.
    - _____ **e.** A gcd of 2 and 3 in $\mathbb{Q}$ is $\frac{1}{2}$.
    - _____ **f.** The Euclidean algorithm gives a constructive method for finding a gcd of two integers.
    - _____ **g.** If ν is a Euclidean norm on a Euclidean domain D, then $\nu(1) \leq \nu(a)$ for all nonzero $a \in D$.

_____ **h.** If ν is a Euclidean norm on a Euclidean domain D, then $\nu(1) < \nu(a)$ for all nonzero $a \in D$, $a \neq 1$.

_____ **i.** If ν is a Euclidean norm on a Euclidean domain D, then $\nu(1) < \nu(a)$ for all nonzero nonunits $a \in D$.

_____ **j.** For any field F, $F[x]$ is a Euclidean domain.

14. Does the choice of a particular Euclidean norm ν on a Euclidean domain D influence the arithmetic structure of D in any way? Explain.

Theory

15. Let D be a Euclidean domain and let ν be a Euclidean norm on D. Show that if a and b are associates in D, then $\nu(a) = \nu(b)$.

16. Let D be a Euclidean domain and let ν be a Euclidean norm on D. Show that for nonzero $a, b \in D$, one has $\nu(a) < \nu(ab)$ if and only if b is not a unit of D. [*Hint:* Argue from Exercise 15 that $\nu(a) < \nu(ab)$ implies that b is not a unit of D. Using the Euclidean algorithm, show that $\nu(a) = \nu(ab)$ implies $\langle a \rangle = \langle ab \rangle$. Conclude that if b is not a unit, then $\nu(a) < \nu(ab)$.]

17. Prove or disprove the following statement: If ν is a Euclidean norm on Euclidean domain D, then $\{a \in D \mid \nu(a) > \nu(1)\} \cup \{0\}$ is an ideal of D.

18. Show that every field is a Euclidean domain.

19. Let ν be a Euclidean norm on a Euclidean domain D.

a. Show that if $s \in \mathbb{Z}$ such that $s + \nu(1) > 0$, then $\eta : D^* \to \mathbb{Z}$ defined by $\eta(a) = \nu(a) + s$ for nonzero $a \in D$ is a Euclidean norm on D. As usual, D^* is the set of nonzero elements of D.

b. Show that for $t \in \mathbb{Z}^+$, $\lambda : D^* \to \mathbb{Z}$ given by $\lambda(a) = t \cdot \nu(a)$ for nonzero $a \in D$ is a Euclidean norm on D.

c. Show that there exists a Euclidean norm μ on D such that $\mu(1) = 1$ and $\mu(a) > 100$ for all nonzero nonunits $a \in D$.

20. Let D be a UFD. An element c in D is a **least common multiple** (abbreviated lcm) of two elements a and b in D if $a \mid c$, $b \mid c$ and if c divides every element of D that is divisible by both a and b. Show that every two nonzero elements a and b of a Euclidean domain D have an lcm in D. [*Hint:* Show that all common multiples, in the obvious sense, of both a and b form an ideal of D.]

21. Use the last statement in Theorem 46.9 to show that two nonzero elements $r, s \in \mathbb{Z}$ generate the group $\langle \mathbb{Z}, + \rangle$ if and only if r and s, viewed as integers in the domain $\mathbb{Z}$, are **relatively prime,** that is, have a gcd of 1.

22. Using the last statement in Theorem 46.9, show that for nonzero $a, b, n \in \mathbb{Z}$, the congruence $ax \equiv b \pmod{n}$ has a solution in $\mathbb{Z}$ if a and n are relatively prime.

23. Generalize Exercise 22 by showing that for nonzero $a, b, n \in \mathbb{Z}$, the congruence $ax \equiv b \pmod{n}$ has a solution in $\mathbb{Z}$ if and only if the positive gcd of a and n in $\mathbb{Z}$ divides b. Interpret this result in the ring $\mathbb{Z}_n$.

24. Following the idea of Exercises 6 and 23, outline a constructive method for finding a solution in $\mathbb{Z}$ of the congruence $ax \equiv b \pmod{n}$ for nonzero $a, b, n \in \mathbb{Z}$, if the congruence does have a solution. Use this method to find a solution of the congruence $22x \equiv 18 \pmod{42}$.

SECTION 47 Gaussian Integers and Multiplicative Norms

Gaussian Integers

We should give an example of a Euclidean domain different from $\mathbb{Z}$ and $F[x]$.

47.1 Definition **A Gaussian integer** is a complex number $a + bi$, where $a, b \in \mathbb{Z}$. For a Gaussian integer $\alpha = a + bi$, the **norm** $N(\alpha)$ **of** α is $a^2 + b^2$. ■