Introduction to Modern Algebra

Part IV. Rings and Fields

IV.19. Integral Domains

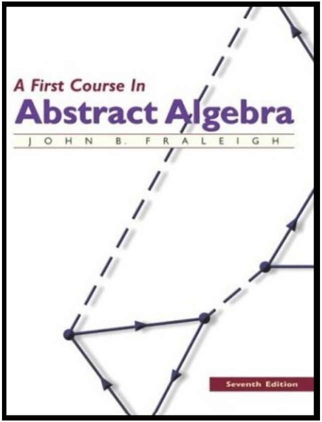

Table of contents

Theorem 19.3

Theorem 19.3. In the ring $\mathbb{Z}_n$, the divisors of 0 are precisely the nonzero elements that are not relatively prime to n.

Proof. Suppose m is not relatively prime to n, say $\gcd(m, n) = d \neq 1$. Then $m(n/d) = (m/d)\, n \equiv 0 \pmod{n}$ and so m is a divisor of 0.

Theorem 19.3

Theorem 19.3. In the ring $\mathbb{Z}_n$, the divisors of 0 are precisely the nonzero elements that are not relatively prime to n.

Proof. Suppose m is not relatively prime to n, say $\gcd(m, n) = d \neq 1$. Then $m(n/d) = (m/d)\, n \equiv 0 \pmod{n}$ and so m is a divisor of 0.

Suppose m is relatively prime to n. If for $s \in \mathbb{Z}_n$ we have $ms \equiv 0 \pmod{n}$, then ms is a multiple of n or equivalently n divides this product ms (as elements of $\mathbb{Z}$). With n relatively prime to m, it must be that n divides s and so $s \equiv 0 \pmod{n}$ (this result is in my online Elementary Number Theory [MATH 3120] notes on Section 1. Integers; see Corollary 1.1). So $s = 0$ in $\mathbb{Z}_n$ and m is not a divisor of 0. □

Theorem 19.3

Theorem 19.3. In the ring $\mathbb{Z}_n$, the divisors of 0 are precisely the nonzero elements that are not relatively prime to n.

Proof. Suppose m is not relatively prime to n, say $\gcd(m, n) = d \neq 1$. Then $m(n/d) = (m/d)\, n \equiv 0 \pmod{n}$ and so m is a divisor of 0.

Suppose m is relatively prime to n. If for $s \in \mathbb{Z}_n$ we have $ms \equiv 0 \pmod{n}$, then ms is a multiple of n or equivalently n divides this product ms (as elements of $\mathbb{Z}$). With n relatively prime to m, it must be that n divides s and so $s \equiv 0 \pmod{n}$ (this result is in my online Elementary Number Theory [MATH 3120] notes on Section 1. Integers; see Corollary 1.1). So $s = 0$ in $\mathbb{Z}_n$ and m is not a divisor of 0. □

Theorem 19.5

Theorem. 19.5. The left cancellation law states that "$ab = ac$ with $a \neq 0$ implies $b = c$". The right cancellation law states that "$ba = ca$ with $a \neq 0$ implies $b = c$". The cancellation laws hold in a ring R if and only if R has no divisor of 0.

Proof. Let R be a ring in which the cancellation laws hold and suppose $ab = 0$ for some $a, b \in R$. If $a \neq 0$ then $ab = a0$ implies $b = 0$ by the left cancellation law. Similarly, if $b \neq 0$ then $ab = 0b$ implies $a = 0$ by the right cancellation law. Since a, b are arbitrary elements of R, then R has no 0 divisors, as claimed.

Theorem 19.5

Theorem. 19.5. The left cancellation law states that "$ab = ac$ with $a \neq 0$ implies $b = c$". The right cancellation law states that "$ba = ca$ with $a \neq 0$ implies $b = c$". The cancellation laws hold in a ring R if and only if R has no divisor of 0.

Proof. Let R be a ring in which the cancellation laws hold and suppose $ab = 0$ for some $a, b \in R$. If $a \neq 0$ then $ab = a0$ implies $b = 0$ by the left cancellation law. Similarly, if $b \neq 0$ then $ab = 0b$ implies $a = 0$ by the right cancellation law. Since a, b are arbitrary elements of R, then R has no 0 divisors, as claimed.

Now suppose R has no 0 divisors and suppose $ab = ac$ with $a \neq 0$. Then $ab - ac = a(b - c) = 0$. Since $a \neq 0$ and R has no divisors of 0, it must be that $b - c = 0$, or $b = c$. So the left cancellation law holds, as claimed.

Theorem 19.5

Theorem. 19.5. The left cancellation law states that "$ab = ac$ with $a \neq 0$ implies $b = c$". The right cancellation law states that "$ba = ca$ with $a \neq 0$ implies $b = c$". The cancellation laws hold in a ring R if and only if R has no divisor of 0.

Proof. Let R be a ring in which the cancellation laws hold and suppose $ab = 0$ for some $a, b \in R$. If $a \neq 0$ then $ab = a0$ implies $b = 0$ by the left cancellation law. Similarly, if $b \neq 0$ then $ab = 0b$ implies $a = 0$ by the right cancellation law. Since a, b are arbitrary elements of R, then R has no 0 divisors, as claimed.

Now suppose R has no 0 divisors and suppose $ab = ac$ with $a \neq 0$. Then $ab - ac = a(b - c) = 0$. Since $a \neq 0$ and R has no divisors of 0, it must be that $b - c = 0$, or $b = c$. So the left cancellation law holds, as claimed.

Similarly, suppose $ba = ca$ with $a \neq 0$. Then $ba - ca = (b - c)a$ and again since $a \neq 0$ and R has no divisors of 0, it must be that $b - c = 0$ or $b = c$. So the right cancellation law holds, as claimed. □

Theorem 19.5

Theorem. 19.5. The left cancellation law states that "$ab = ac$ with $a \neq 0$ implies $b = c$". The right cancellation law states that "$ba = ca$ with $a \neq 0$ implies $b = c$". The cancellation laws hold in a ring R if and only if R has no divisor of 0.

Proof. Let R be a ring in which the cancellation laws hold and suppose $ab = 0$ for some $a, b \in R$. If $a \neq 0$ then $ab = a0$ implies $b = 0$ by the left cancellation law. Similarly, if $b \neq 0$ then $ab = 0b$ implies $a = 0$ by the right cancellation law. Since a, b are arbitrary elements of R, then R has no 0 divisors, as claimed.

Now suppose R has no 0 divisors and suppose $ab = ac$ with $a \neq 0$. Then $ab - ac = a(b - c) = 0$. Since $a \neq 0$ and R has no divisors of 0, it must be that $b - c = 0$, or $b = c$. So the left cancellation law holds, as claimed.

Similarly, suppose $ba = ca$ with $a \neq 0$. Then $ba - ca = (b - c)a$ and again since $a \neq 0$ and R has no divisors of 0, it must be that $b - c = 0$ or $b = c$. So the right cancellation law holds, as claimed. □

Theorem 19.9

Theorem 19.9. Every field F is an integral domain.

Proof. Recall that a field is a commutative divisor ring. So we only need to show that F has no divisor of 0. Let $a, b \in F$ with $a \neq 0$ and $ab = 0$. Then $a^{-1}(ab) = a^{-1}0 = 0$ and so $0 = a^{-1}(ab) = \left(a^{-1}a\right)b = eb = b$. So $b = 0$. Since F is commutative in $\cdot$, $ba = 0$ and $a \neq 0$ also implies $b = 0$. So F has no 0 divisors and therefore is an integral domain, as claimed. □

Theorem 19.9

Theorem 19.9. Every field F is an integral domain.

Proof. Recall that a field is a commutative divisor ring. So we only need to show that F has no divisor of 0. Let $a, b \in F$ with $a \neq 0$ and $ab = 0$. Then $a^{-1}(ab) = a^{-1}0 = 0$ and so $0 = a^{-1}(ab) = \left(a^{-1}a\right) b = eb = b$. So $b = 0$. Since F is commutative in $\cdot$, $ba = 0$ and $a \neq 0$ also implies $b = 0$. So F has no 0 divisors and therefore is an integral domain, as claimed. □

Theorem 19.11

Theorem 19.11. Every finite integral domain is a field.

Proof. We need only show that each nonzero element of a finite integral domain is a limit. Let the elements of the integral domain D be $0, 1, a_1, \ldots, a_n$. Let $a \in D$, $a \neq 0$, and consider $a1, aa_1, \ldots, aa_n$. These elements of D are distinct since $aa_i = aa_j$ implies $a_i = a_j$ by the left cancellation law (Theorem 19.5).

Theorem 19.11

Theorem 19.11. Every finite integral domain is a field.

Proof. We need only show that each nonzero element of a finite integral domain is a limit. Let the elements of the integral domain D be $0, 1, a_1, \dots, a_n$. Let $a \in D$, $a \neq 0$, and consider $a1, aa_1, \dots, aa_n$. These elements of D are distinct since $aa_i = aa_j$ implies $a_i = a_j$ by the left cancellation law (Theorem 19.5). Since D has no 0 divisors, none of $a1, aa_1, \dots, aa_n$ is 0. So this list must include all nonzero elements of D. Hence one of these is 1. That is $aa_i = 1$ for some $0 \leq i \leq n$ (where we take $a_0 = 1$). Therefore, a has an inverse (namely a_i) and a is a unit. We now have that, D is a field, as claimed. □

Theorem 19.11

Theorem 19.11. Every finite integral domain is a field.

Proof. We need only show that each nonzero element of a finite integral domain is a limit. Let the elements of the integral domain D be $0, 1, a_1, \ldots, a_n$. Let $a \in D$, $a \neq 0$, and consider $a1, aa_1, \ldots, aa_n$. These elements of D are distinct since $aa_i = aa_j$ implies $a_i = a_j$ by the left cancellation law (Theorem 19.5). Since D has no 0 divisors, none of $a1, aa_1, \ldots, aa_n$ is 0. So this list must include all nonzero elements of D. Hence one of these is 1. That is $aa_i = 1$ for some $0 \leq i \leq n$ (where we take $a_0 = 1$). Therefore, a has an inverse (namely a_i) and a is a unit. We now have that, D is a field, as claimed. □

Corollary 19.12

Corollary 19.12. If p is a prime, then $\mathbb{Z}_p$ is a field.

Proof. For p prime, $\mathbb{Z}_p$ is an integral domain by Corollary 19.4. So by Theorem 19.11, $\mathbb{Z}_p$ is a field, as claimed. □

Corollary 19.12

Corollary 19.12. If p is a prime, then $\mathbb{Z}_p$ is a field.

Proof. For p prime, $\mathbb{Z}_p$ is an integral domain by Corollary 19.4. So by Theorem 19.11, $\mathbb{Z}_p$ is a field, as claimed. □

Theorem 19.15

Theorem 19.15. Let R be a ring with unity. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$, then R has characteristic 0. If $n \cdot 1 = 0$ for some $n \in \mathbb{N}$, then the smallest such integer n is the characteristic of R.

Proof. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$, then we cannot have $n \cdot a = 0$ for all $a \in R$ and some given $n \in \mathbb{N}$ (since the result does not ever hold for $a = 1$). So R has characteristic 0, as claimed.

Theorem 19.15

Theorem 19.15. Let R be a ring with unity. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$, then R has characteristic 0. If $n \cdot 1 = 0$ for some $n \in \mathbb{N}$, then the smallest such integer n is the characteristic of R.

Proof. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$, then we cannot have $n \cdot a = 0$ for all $a \in R$ and some given $n \in \mathbb{N}$ (since the result does not ever hold for $a = 1$). So R has characteristic 0, as claimed.

Suppose that $n \in \mathbb{N}$ such that $n \cdot 1 = 0$ and n is the smallest such element of $\mathbb{N}$ with this property. Let $a \in R$. Then

$$n \cdot a = \underbrace{a + a + a + \cdots + a}_{n \text{ times}} = a(\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}) = a\,(n \cdot 1) = a \cdot 0 = 0.$$

So R is of characteristic n (notice there is no smaller n for which $n \cdot a = 0$ when $a = 1$, so there is no small such n), as claimed. □

Theorem 19.15

Theorem 19.15. Let R be a ring with unity. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$, then R has characteristic 0. If $n \cdot 1 = 0$ for some $n \in \mathbb{N}$, then the smallest such integer n is the characteristic of R.

Proof. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$, then we cannot have $n \cdot a = 0$ for all $a \in R$ and some given $n \in \mathbb{N}$ (since the result does not ever hold for $a = 1$). So R has characteristic 0, as claimed.

Suppose that $n \in \mathbb{N}$ such that $n \cdot 1 = 0$ and n is the smallest such element of $\mathbb{N}$ with this property. Let $a \in R$. Then

$$n \cdot a = \underbrace{a + a + a + \cdots + a}_{n \text{ times}} = a(\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}) = a\,(n \cdot 1) = a \cdot 0 = 0.$$

So R is of characteristic n (notice there is no smaller n for which $n \cdot a = 0$ when $a = 1$, so there is no small such n), as claimed. □