Proof a Day — 2026

Alexander Crabtree

Contents

1 Weeks 1–13

1.1 Week 1 (Jan 1–Jan 7)

2026-01-01 Divisibility

Theorem 1.1. *If* $a|c$ *and* $b|c$ *and* $\gcd(a, b) = d$*, then* $ab|cd$*.* $a, b, c \in \mathbb{Z}$

Proof. As $d = \gcd(a, b)$, we have that $d = au + bv$ for some $u, v \in \mathbb{Z}$. We now have that $cd = c(au + bv) = cau + cbv$. Since $a|c$ and $b|c$, $c = ax = by$ for some $x, y \in \mathbb{Z}$. Substituing c results in $cd = cau + cbv = (by)au + (ax)bv = (ab)(yu + xv)$. As $u, v, x, y \in \mathbb{Z}$, $yu + xv \in \mathbb{Z}$. By definition of divisibility, $ab|cd$. □

2026-01-02 Divisibility

Theorem 1.2. *If* $a|bc$ *and* $\gcd(a, b) = 1$*, then* $a|c$*.*

Proof. Assume that $a|bc$ and $\gcd(a, b) = 1$. As a and b are relatively prime, $au + bv = 1$ for some $u, v \in \mathbb{Z}$. If we multiply $au + bv = 1$ by c, then we have $cau + cbv = c$. As $a|bc$, $bc = ax$ for some $x \in \mathbb{Z}$. Now, we have that

$$c = cau + cbv = cau + bcv = cau + (ax)v = a(cu + xv)$$

Since $c, u, x, v \in \mathbb{Z}$ and by the definition of divisibility, $a|c$. □

2026-01-03 Divisibility

Theorem 1.3. *If* $\gcd(a, c) = 1$ *and* $\gcd(b, c) = 1$*, then* $\gcd(ab, c) = 1$*.*

Proof. By way of contradiction, assume that $\gcd(ab, c) \neq 1$. Thus, there exists a prime p such that

$$p|ab \text{ and } p|c.$$

Since p is prime, $p|a$ or $p|b$. If $p|a$, then $\gcd a, c \geq p > 1$, which contradiscts the assumption that $\gcd(a, c) = 1$. If $p|b$, then $\gcd b, c \geq p > 1$, which contradicts the assumption that $\gcd(b, c) = 1$. Therefore ab and c share no such prime factors p, so $\gcd(ab, c) = 1$. □

2026-01-04 Rings

Theorem 1.4. *If* $a + b = a + c$ *in a ring* R*, then* $b = c$*.*

Proof. Assume that for $a, b, c \in R$, $a + b = a + c$. If we add $-a$ and by using the associtivity property of rings and negatives, we can show that

$$\begin{aligned} -a + (a + b) &= -a + (a + c) \\ (-a + a) + b &= (-a + a) + c \\ 0_R + b &= 0_R + c \\ b &= c \end{aligned}$$

$\square$

2026-01-05 Rings

Theorem 1.5. *If $a \neq 0_R$ and $ab = ac$ in an integral domain R, then $b = c$.*

Proof. If $ab = ac$, then $ab - ac = 0_R$. Thus, $a(b - c) = 0_R$. As R is an integral domain and $a \neq 0_R$, it must be that $b - c = 0_R$. If $b - c \neq 0_R$, then a would be a zero divisor contradicting the zero-product property of integral domains. Thus $b = c$. $\square$

2026-01-06 Rings

Theorem 1.6. *Every field is an integral domain.*

Proof. To show that a field F is an integral domain, it suffices to show that F satisfies the zero product property. Take any $a, b \in F$ such that $ab = 0_F$. We must show that $a = 0_F$ or $b = 0_F$. Assume that $ab = 0_F$. Without loss of generality, if $b = 0_F$, then we are done, so assume that $b \neq 0_F$. As F is a field, b is a unit in F. By definition of a unit, we have that

$$a = a1_F = a(bb^{-1}) = (ab)b^{-1} = 0_F b^{-1} = 0_F$$

So, for all $a, b \in F$, $a = 0_F$ or $b = 0_F$. $\square$

2026-01-07 Rings

Theorem 1.7. *Every finite integral domain is a field.*

Proof. To show that an integral domain R is a field, it suffices to show that for all $a \in R$ where $a \neq 0_R$, the equation $ax = 1_R$. Let $a_1, a_2, \ldots, a_n$ be the n distinct elements in R and $a_t \neq 0$. Consider the products $a_t a_1, a_t a_2, \ldots, a_t a_n$. If $a_i \neq a_j$ for $i \neq j$, we must have that $a_t a_i \neq a_t a_j$. Therefore $a_t a_1, a_t a_2, \ldots, a_t a_n$ has n distinct elements in R. So, all n elements of R are expressed in the products in some order. So, for some j, $a_t a_j = 1_R$. Therefore the equation $ax = 1_R$ has a solution and R is a field. $\square$

1.2 Week 2 (Jan 8–Jan 14)

2026-01-08 Rings

Theorem 1.8. *Let $f : R \to S$ be a homomorphism of rings, Then*

$$\begin{aligned} &(1) \quad f(0_R) = 0_S \\ &(2) \quad f(-a) = -f(a) \quad \forall a \in R \\ &(3) \quad f(a-b) = f(a) - f(b) \quad \forall a, b \in R \end{aligned}$$

Proof. (1) As f is a homomorphism of rings, we have the following:

$$\begin{aligned} f(0_R) + f(0_R) &= f(0_R + 0_R) \\ f(0_R) + f(0_R) &= f(0_R) \quad [0_R + 0_R = 0_R \,\text{in}\, R] \\ f(0_R) + f(0_R) &= f(0_R) + 0_S \, [f(0_R) + 0_S = f(0_R) \,\text{in}\, S] \\ f(0_R) &= 0_S \end{aligned}$$

(2) Note that: $f(a) + f(-a) = f(a + (-a)) = f(0_R) = 0_S$ by (1) and f is a homomorphism. So, $f(-a)$ is a solution to the equation $f(a) + x = 0_S$. But as S is a ring, there exists only one unique solution to this equation which is $-f(a)$. Therefore by [theorem to be proved at a later date], $f(-a) = -f(a)$.

(3) As f is a homomorphism and by (2), we have the following:

$$\begin{aligned} f(a-b) &= f(a + (-b)) \\ &= f(a) + f(-b) \\ &= f(a) - f(b) \end{aligned}$$

□

2026-01-09 Rings

Theorem 1.9. *Let $f : R \to S$ be a homomorphism of rings. If R is a ring with identity and f is surjective, then*

(1) S is a ring with identity $f(1_R)$.

(2) Whenever u is a unit in R, then $f(u)$ is a unit in S and $f(u)^{-1} = f(u^{-1})$.

Proof. (1) Let s be some element in S. As f is surjective, there exists some $r \in R$ such that $f(r) = s$. Then we have that

$$s * f(1_R) = f(r)f(1_R) = f(r * 1_R) = f(r) = s$$

Similarly $f(1_R) * s = s$. Therefore $1_S = f(1_R)$.

(2) As u is a unit, there exists some $v \in R$ such that $uv = 1_R = vu$. By (1), we have that $f(u)f(v) = f(uv) = f(1_R) = 1_S$. Similarly, $vu = 1_R$ which implies that $f(v)f(u) = 1_S$. Therefore $f(u)$ is a unit in S with inverse $f(v)$. Said differently $f(u)^{-1} = f(v)$. As v is the inverse of u ($v = u^{-1}$), we see that $f(u)^{-1} = f(v) = f(u^{-1})$. □

2026-01-10 Groups

Theorem 1.10. *Every ring is an abelian group under addition.*

Proof. The first five axioms for a ring are identical to the five axioms for an abelian group, with addition as the operation, the identity element being 0_R, and the inverse for any element $a \in R$ being $-a$. □