Proofs from Ring Theory

Theorem 1: Let R be a commutative ring with identity, and let U be the set of units in R. Then U is a group under multiplication of R.

Proof: To start, $1 \in U$, so U is nonempty. Now, let $u_1, u_2 \in U$. By definition of unit, there exist $v_1, v_2 \in R$ such that $u_1 v_1 = 1$ and $u_2 v_2 = 1$. Now, since R is abelian and associative, $(u_1 u_2)(v_1 v_2) = (u_1 u_2)(v_2 v_1) = u_1(u_2 v_2)v_1 = u_1 v_1 = 1$. Hence, $u_1 u_2 \in U$ and U is closed under multiplication of R. Now, the inverse of a unit is also a unit, so $v_1 \in U$. Hence, U is a group under multiplication of R. ■

Theorem 2 (cancellation law): Let D be an integral domain and let $a, b, c \in D$ such that $a \neq 0$. If $ab = ac$, then $b = c$.

Proof: If $ab = ac$, then $ab - ac = 0$. By the distributive law of rings, it follows that $a(b - c) = 0$. Since D is an integral domain, then a is not a zero divisor. Thus, $b - c = 0$, and so $b = c$. ■

Theorem 3: If D is a finite integral domain, then D is a field.

Proof: Let $x \in D$ such that $x \neq 0$. We must prove that x is a unit. Now, let $f: D \to D$ be defined by $f(d) = xd$ for some $d \in D$. Suppose $d_1, d_2 \in D$ and $f(d_1) = f(d_2)$. Then $xd_1 = xd_2$, implying that $d_1 = d_2$ by the cancellation law. Since $f(d_1) = f(d_2)$ implies $d_1 = d_2$, then f is one-to-one. Since f maps a finite set onto itself, then by a previous theorem, f is onto as well, so $1 = f(a)$ for some $a \in D$. It follows that $ad = 1$, so d has an inverse. Since we have shown that every nonzero element of D has an inverse, then D is a field. ■

Theorem 4: Let $a \in \mathbb{Z}_n$ for some $n \geq 2$. If a is not a unit, then a must be a zero-divisor.

Proof: Let $d = \gcd(a, n)$. Since a is not a unit, then $d > 1$. Now, let $a = da_1$ and $n = dn_1$ for some integers a_1 and n_1 such that $1 < a_1 < a < n$ and $1 < n_1 < n$. Then $n_1 a = n_1(da_1) = (n_1 d)a_1 = (dn_1)a_1 = na_1$. Now, it follows that a is divisible by n, so $n_1 a \equiv 0 \ (mod\ n)$. This proves that a is a zero divisor. ■

Let R be a commutative ring such that $a^2 = a$ for every $a \in R$. Show that $a + a = 0$ every $a \in R$.

Proof: Let $a \in R$. Then $a + a = (a + a)^2 = (a + a)(a + a) = a^2 + a^2 + a^2 + a^2 = a + a + (a + a)$. Since $a + a = a + a + (a + a)$, then $a + a$ is the additive identity, so $a + a = 0$. ■

Let R be the set of all continuous functions from the set of real numbers onto itself. Prove that R is a commutative ring under the addition and multiplication of functions.

Proof: R is obviously abelian since addition and multiplication are commutative operations. Also, the sums and products of two continuous functions are continuous, so associativity, closure, and the distributive law hold true for R. Now, the zero function is continuous, so R has an additive identity. The function $\varphi: \mathbb{R} \to \mathbb{R}$ defined by $\varphi(x) = 1$ is continuous, so R also has the multiplicative identity. Finally, any multiple of a continuous function is also continuous, so R has the additive inverse. Hence, R forms a commutative ring. ■

Let R and S be commutative rings with identity. Prove that the set $R \oplus S = \{(r, s) | r \in R, s \in S\}$ forms a commutative ring with identity under the addition and multiplication of ordered pairs.

Proof: The set $R \oplus S$ forms an abelian group since the group structure is similar to the abelian direct product group $R \times S$. It follows that $R \oplus S$ is closed and associative under multiplication and has a multiplicative identity. To see that $R \oplus S$ is closed under addition, let $r_1, r_2 \in R$ and $s_1, s_2 \in S$. Now, $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \in R \oplus S$. To prove the associativity of addition, let $r_1, r_2, r_3 \in R$ and $s_1, s_2, s_3 \in S$. Now, $(r_1, s_1) + [(r_2, s_2) + (r_3, s_3)] = (r_1, s_1) + (r_2, s_2) + (r_3, s_3) = (r_1 + r_2 + r_3, s_1 + s_2 + s_3) = (r_1, s_1) + (r_2, s_2) + (r_3, s_3) = [(r_1, s_1) + (r_2, s_2)] + (r_3, s_3)$. Now, since $0 \in R$ and $0 \in S$, then $R \oplus S$ has the additive identity element $(0,0)$. Also, the distributive laws could easily be shown to hold for $R \oplus S$ since they hold for addition and muitlplication in the rings R and S. Hence, $R \oplus S$ is a commutative ring with identity. ■

Let n be an integer such that $n \geq 2$. Prove that $\mathbb{Z}_n$ is a commutative ring with identity.

Proof: We have already proven that $\mathbb{Z}_n$ is an abelian group under addition. It follows that the associative, commutative, and closure properties hold for addition in $\mathbb{Z}_n$. It can also be implied that $\mathbb{Z}_n$ has both an additive identity and an additive inverse. We have also proven that modular multiplication is well-defined, so $\mathbb{Z}_n$ is closed under multiplication as well. Now, let $[a]_n, [b]_n \in \mathbb{Z}_n$. By definition of modular multiplication, $[a]_n \cdot [b]_n = [ab]_n = [ba]_n = [b]_n \cdot [a]_n$, so multiplication in $\mathbb{Z}_n$ is commutative. Now, let $[c]_n \in \mathbb{Z}_n$. Then $[a]_n \cdot ([b]_n \cdot [c]_n) =$

$[a]_n \cdot [bc]_n = [abc]_n = [ab]_n \cdot [c]_n = ([a]_n \cdot [b]_n) \cdot [c]_n$, so multiplication in $\mathbb{Z}_n$ is associative. By definitions of modular addition and multiplication, $[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b + c]_n = [a(b + c)]_n = [ab + ac]_n = [ab]_n + [ac]_n = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$. Also, $([a]_n + [b]_n) \cdot [c]_n = [a + b]_n \cdot [c]_n = [(a + b) \cdot c]_n = [ac + bc]_n = [ac]_n + [bc]_n = [a]_n \cdot [c]_n + [b]_n \cdot [c]_n$. We have just proven that the distributive law holds for $\mathbb{Z}_n$. Finally, $[1]_n$ is a multiplicative identity for $\mathbb{Z}_n$ since $[a]_n \cdot [1]_n = [a \cdot 1]_n = [a]_n = [1 \cdot a]_n = [1]_n \cdot [a]_n$. Hence, $\mathbb{Z}_n$ is a commutative ring with identity. ■