Dummit & Foote Ch. 7.1: Introduction to Rings

Scott Donaldson

Jul. 2024

Let R be a ring with 1.

1. (7/1/24)

Show that $(-1)^2 = 1$ in $\mathbb{R}$.

Proof. We have:

$$(-1) + (-1)^2 = \underbrace{(-1)(1)}_{\text{identity}} + (-1)(-1) = \underbrace{(-1)(1 + (-1))}_{\text{distribution}} = (-1) \underbrace{(0)}_{\text{inverses}} = 0,$$

and therefore, since $(-1) + (-1)^2 = 0$, $(-1)^2 = 1$. $\square$

2. (7/1/24)

Prove that if u is a unit in R then so is $-u$.

Proof. Recall that u is a unit in R if there exists some $v \in R$ such that $uv = vu = 1$.

Now:

$$\begin{aligned} (-u)(v) &= -(uv) = -1, \text{ which implies that} \\ (-u)(v)(-1) &= (-1)^2 = 1, \text{ so} \\ (-u)(-v) &= 1, \end{aligned}$$

which implies that $-u$ is also a unit in R. $\square$

7. (7/5/24)

The *center* of a ring R is $\{z \in R \mid zr = rz \text{ for all } r \in R\}$ (i.e., is the set of all elements which commute with every element of R). Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.

Proof. Let $a, b \in R$ be in the center of R and let $x \in R$. Then:

$$(a-b)x = ax - bx = xa - xb = x(a-b),$$

so $a - b$ is in the center of R. And, since a and b both commute with x, we have $(ab)x = abx = xab = x(ab)$, so ab lies in the center of R as well. Since by definition 1 commutes with every element of R, the center of R is a subring of R containing the identity.

If R is a division ring, then every element in its center (except 0) has a multiplicative inverse (is a unit). Every element in its center also commutes with every other element. A field is a commutative ring where every nonzero element is a unit; therefore the center of a division ring is a field. $\square$

8. (7/9/24)

Describe the center of the Hamilton Quaternions $\mathbb{H}$. Prove that $\{a+bi \mid a, b \in \mathbb{R}\}$ is a subring of $\mathbb{H}$ which is a field but is not contained in the center of $\mathbb{H}$.

Proof. Let $a+bi+cj+dk$ ($a, b, c, d \in \mathbb{R}$) lie in the center of $\mathbb{H}$. It must commute with i ($= 0 + 1i + 0j + 0k$). Then:

$$\begin{aligned}(a+bi+cj+dk)i &= ai + bi^2 + cji + dki \\ &= -b + ai + dj - ck, \text{ and} \\ i(a+bi+cj+dk) &= ai + bi^2 + cij + dik \\ &= -b + ai - dj + ck.\end{aligned}$$

If these are equal, then we have:

$$\begin{aligned}-b + ai + dj - ck &= -b + ai - dj + ck \\ dj - ck &= -dj + ck \\ 2dj &= 2ck \\ dj &= ck,\end{aligned}$$

and since $c, d \in \mathbb{R}$, there are no nonzero values of c, d such that $dj = ck$. Thus we must have $c = d = 0$.

Repeating the above steps for the product of $a + bi + cj + dk$ and j or k, we see that b must also be 0.

Now because real coefficients of i, j, k commute, a may take any value, and so the center of $\mathbb{H}$ consists of the real numbers (that is, quaternions of the form $a + 0i + 0j + 0k$).

Consider the subset $\{a + bi \mid a, b \in \mathbb{R}\}$. Let $a + bi, c + di$ be two elements of this subset. We see that $(a+bi)-(c+di) = (a-c)+(b-d)i$ and $(a+bi)(c+di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$. Since this subset is closed under subtraction and multiplication, it is a subring of $\mathbb{H}$. However, since it includes elements with nonzero i components, it is not contained in the center of $\mathbb{H}$. $\square$

9. (7/9/24)

For a fixed element $a \in R$ define $C(a) = \{r \in R \mid ra = ar\}$. Prove that $C(a)$ is a subring of R containing a. Prove that the center of R is the intersection of the subrings $C(a)$ over all $a \in R$.

Proof. Let $a \in R$ and let $c, d \in C(a)$. Then:

$$(c-d)a = ca - da = ac - ad = a(c-d), \text{ and}$$
$$(cd)a = cda = cad = acd = a(cd),$$

so $C(a)$ is a subring of R. Since elements commute with themselves, $a \in C(a)$.

Next, consider the intersection of all subrings $C(a)$ for $a \in R$, $\bigcap_{a \in R} C(a)$. Let $c \in \bigcap_{a \in R} C(a)$. Then $ca = ac$ for all $a \in R$, so c is in the center of R. Conversely, if c is in the center of R, then for all $a \in R$, $ca = ac$, and so $c \in \bigcap_{a \in R} C(a)$. Thus the center of R is the intersection of the subrings $C(a)$ over all $a \in R$. □

10. (7/9/24)

Prove that if D is a division ring then $C(a)$ is a division ring for all $a \in D$.

Proof. Let D be a division ring and let $a \in D$. Recall that, in a division ring, every nonzero element has a multiplicative inverse (denote x's inverse by x^{-1}).

Let $c \neq 0 \in C(a)$. We see that:

$$\begin{aligned} a &= a \\ a &= acc^{-1} \ (cc^{-1} = 1) \\ a &= cac^{-1} \ (ca = ac) \\ c^{-1}a &= ac^{-1} \text{ (left-multiply by } c^{-1}), \end{aligned}$$

so $c^{-1} \in C(a)$. Since the multiplicative inverse of every element $c \in C(a)$ lies in $C(a)$, it is therefore a division ring. □

11. (7/9/24)

Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.

Proof. Recall that an integral domain is a commutative ring with identity $1 \neq 0$ and no zero divisors. Suppose that $x^2 = 1$ for some $x \in R$. Then:

$$\begin{aligned} x^2 &= 1 \\ x^2 + x &= x + 1 \\ x(x+1) &= x + 1. \end{aligned}$$

By the cancellation property of integral domains (Proposition 2), either $x + 1 = 0$, which implies that $x = -1$, or else $x = 1$. □

12. (7/17/24)

Prove that any subring of a field which contains the identity is an integral domain.

Proof. Let F be a field and let R be a subring of F containing 1. Since a field is a commutative division ring, every element of F commutes multiplicatively with every other element, and so R must also be commutative. Further, since every nonzero element of F is a unit, and no element is both a unit and a zero divisor, R contains no zero divisors. Therefore R must be an integral domain. $\square$