

H/wk 10 (Selected Solutions)

3.16

(i) If R is a commutative ring, define \circ on R by

$$a \circ b := a + b - ab, \quad \text{for any } a, b \in R.$$

Prove that \circ is an associative operation and that $0 \circ a = a$ for every $a \in R$.

(ii) Prove that the ring R is a field if and only if $(R^\#, \circ)$ is an abelian group where $R^\# = \{r \in R \mid r \neq 1\}$.

Solution.

(i) For any $a, b, c \in R$ we have

$$a \circ (b \circ c) = a \circ (b + c - bc) = a + b + c - bc - a(b + c - bc) = a + b + c - bc - ab - ac + abc,$$

and

$$(a \circ b) \circ c = (a + b - ab) \circ c = a + b - ab + c - (a + b - ab)c = a + b + c - ab - ac - bc + abc,$$

so that $a \circ (b \circ c) = (a \circ b) \circ c$.

Also, for every $a \in R$

$$0 \circ a = 0 + a - 0 \cdot a = a,$$

as required.

(ii) Note first that for any ring R \circ is a commutative operation since

$$a \circ b = a + b - ab = b + a - ba = b \circ a.$$

(a) Suppose now that R is a field. We already know that \circ is an associative and commutative operation on R with 0 satisfying $0 \circ a = a \circ 0 = a$ for every $a \in R$. To show that $(R^\#, \circ)$ is an abelian group we need to check that $R^\#$ is closed under \circ and that for every $a \in R^\#$ there exists $b \in R^\#$ such that $a \circ b = 0$.

Let $a, b \in R^\#$, so that $a \neq 1, b \neq 1$. Suppose that $a \circ b \notin R^\#$, that is, $a \circ b = 1$. Then

$$\begin{aligned} 1 = a \circ b &= a + b - ab = a(1 - b) + b \Rightarrow 1 - b = a(1 - b) \Rightarrow \\ &\text{since } 1 - b \neq 0 \\ (1 - b)(1 - b)^{-1} &= a(1 - b)(1 - b)^{-1} \Rightarrow a = 1, \end{aligned}$$

yielding a contradiction. Thus $a \circ b \in R^\#$ so that $R^\#$ is closed under \circ .

Now let $a \in R^\#$, so that $a \in R, a \neq 1$. We need to prove that there exists $b \in R^\#$ such that $a \circ b = 0$. We have for $b \in R$

$$a \circ b = 0 \iff a + b - ab = 0 \iff b(1 - a) + a = 0 \iff b(1 - a) = -a$$

Since $a \neq 1$ we have $1 - a \neq 0$ and therefore $(1 - a)^{-1}$ exists since R is a field. Put $b = -a(1 - a)^{-1}$. The above computation shows that $a \circ b = 0$. It remains to check that $b \in R^\#$, that is, $b \neq 1$. If $b = 1$ then $-a(1 - a)^{-1} = 1$ and therefore $-a = 1 - a$ so that $0 = 1$, yielding a contradiction. Thus $b \neq 1$ and we have proved that $(R^\#, \circ)$ is an abelian group.

(b) Suppose that R is a ring such that $(R^\#, \circ)$ is an abelian group.

Let $x \in R$ be an arbitrary element such that $x \neq 0$. If $x = 1$ then $x^{-1} = 1$ is the multiplicative inverse of x . Suppose now that $x \neq 1$.

Put $a = x + 1$. Since $x \neq 0$, we have $a \neq 1$, so that $a \in R^\#$. Let b be the inverse of a in the abelian group $(R^\#, \circ)$. Put $y = b - 1$. We claim that $xy = yx = 1$.

Indeed, $a \circ b = 0$ implies $(x + 1) \circ b = 0$, so that $x + 1 + b - xb - b = 0$. Therefore

$$1 = xb - x = x(b - 1) = xy.$$

Thus y is a multiplicative inverse of x in R . Since $x \neq 0$ was arbitrary, this implies that R is a field.

3.18 Prove that if R is a finite domain then it is a field.

Solution 1.

Let R be a finite commutative ring such that R is a domain. Let $r \in R, r \neq 0$ be arbitrary.

Consider the function $f_r : R \rightarrow R$ defined as $f_r(x) = rx$ for every $x \in R$. We claim that f_r is injective. Indeed, suppose $f_r(x) = f_r(y)$. Then $rx = ry$ and therefore $r(x - y) = 0$. Since $r \neq 0$ and R is a domain, it follows that $x - y = 0$ and $x = y$.

Thus $f_r : R \rightarrow R$ is injective. Since R is a finite set, this implies that f_r is a bijection. Thus $1 \in f_r(R)$, so that there exists $x \in R$ with $f_r(x) = 1$, that is $rx = 1$.

Thus x is a multiplicative inverse of r and, since $r \neq 0$ was arbitrary, it follows that R is a field.

Solution 2.

Let $a \in R, a \neq 0$ be arbitrary. Consider the sequence

$$a, a^2, a^3, \dots$$

Since R is finite, there exist positive integers m, n such that $m < n$ and $a^m = a^n$. Then

$$a^n - a^m = a^m(a^{n-m} - 1) = 0.$$

Since $a \neq 0$ and R is an integral domain, it follows that $a^{n-m} - 1 = 0$, that is $a^{n-m} = 1$.

Note that since $n > m > 0$, we have $n - m - 1 \geq 0$ and thus there is $a^{n-m-1} \in R$.

Therefore $a^{n-m} = a \cdot a^{n-m-1} = 1$ and hence $a^{n-m-1} \in R$ is the multiplicative inverse of a . Since $a \neq 0$ was arbitrary, this implies that R is a field.