

Math 541
 Problem Set 2

0.3.12. Since a and n are not relatively prime, there is an integer $d > 1$ such that $d \mid a$ and $d \mid n$. Observe that $d \leq n$. Take $b = n/d$, so $1 \leq b < n$. Then $ab = a(n/d) = n(a/d) \equiv 0 \pmod{n}$.

Now suppose there is a c such that $ac \equiv 1 \pmod{n}$. Then mod n , we have

$$b \equiv 1 \cdot b \equiv (ac)b \equiv (ab)c \equiv 0 \cdot c \equiv 0,$$

but this is not true since $1 \leq b < n$.

0.3.15. (a) Since 13 is prime and $20 = 2^2 \cdot 5$, they have no common prime factors, hence are relatively prime. 17 is an inverse since $13 \cdot 17 = 221 \equiv 1 \pmod{20}$.

1.1.1. (a) No. $(5 - 3) - 1 = 1$, but $5 - (3 - 1) = 3$.

(b) Yes.

$$\begin{aligned} (a \star b) \star c &= (a + b + ab) \star c = a + b + ab + c + ac + bc + abc \\ a \star (b \star c) &= a \star (b + c + bc) = a + b + c + bc + ab + ac + abc \end{aligned}$$

which are equal.

(c) No. $(1 \star 1) \star 2 = 2/5 \star 2 = 12/25$, but $1 \star (1 \star 2) = 1 \star 3/5 = 8/25$.

(d) Yes. This is just addition of fractions. For a proof,

$$\begin{aligned} [(a, b) \star (c, d)] \star (e, f) &= (ad + bc, bd) \star (e, f) = ((ad + bc)f + bde, bdf) \\ (a, b) \star [(c, d) \star (e, f)] &= (a, b) \star (cf + de, df) = (adf + b(cf + de), bdf) \end{aligned}$$

which are equal.

(e) No. $(8/4)/2 = 1$, but $8/(4/2) = 4$.

1.1.6. Most of these sets are not closed under addition.

(a) Yes. Suppose that b and d are odd. Then when we write $a/b + c/d = (ad + bc)/(bd)$ in lowest terms, the denominator will divide bd , hence will be odd. Thus the set is closed under addition. Addition in \mathbb{Q} is associative. The additive identity 0 is in the set by hypothesis. If a/b is in lowest terms with b odd then its additive inverse $(-a)/b$ is still in lowest terms.

(b) No. $1/6 + 1/6 = 2/6 = 1/3$.

(c) No. $1/2 + 1/2 = 1$.

(d) No. $3/2 + (-1) = 1/2$.

(e) Yes. Every element of this set can be written uniquely as $n/2$, where $n \in \mathbb{Z}$. The set is closed under addition because \mathbb{Z} is: $m/2 + n/2 = (m + n)/2$. Addition in \mathbb{Q} is associative. The additive identity $0 = 0/2$ is in the set. If $n/2$ is in the set then so is its additive inverse $(-n)/2$.

(f) No. $1/2 + 1/3 = 5/6$.

1.2.2. An arbitrary element $x \in D_{2n}$ can be written in terms of the generators as $x = s^{k_1} r^{i_1} s^{k_2} r^{i_2} \dots s^{k_m} r^{i_m}$ where the powers $k_1, k_2, \dots, k_m, i_1, i_2, \dots, i_m \in \mathbb{Z}$. Since $rs = sr^{-1}$, we can move all the s 's to the left and r 's to the right, so $x = s^k r^i$ with $k, i \in \mathbb{Z}$. Since $s^2 = 1$, we have $x = r^i$ or $x = sr^i$. If x is not a power of r then $rx = rsr^i = sr^{-1}r^i = sr^i r^{-1} = xr^{-1}$.