Introduction to Groups

1.1: Basic Axioms and Examples

Exercises

1. (a) no: $a-(b-c)=a-b+c\neq(a-b)-c$

   (b) yes:

$$(a\star b)\star c=(a+b+ab)\star c=a+b+ab+c+(a+b+ab)c=a+b+c+ab+ac+bc+abc \tag{1}$$
$$a\star(b\star c)=a\star(b+c+bc)=a+b+c+bc+a(b+c+bc)=a+b+c+bc+ab+ac+abc \tag{2}$$

   (c) no:

$$(a\star b)\star c=\frac{a+b}{5}\star c=\frac{\frac{a+b}{5}+c}{5}=\frac{a+b+5c}{25} \tag{3}$$
$$a\star(b\star c)=a\star\frac{b+c}{5}=\frac{a+\frac{b+c}{5}}{5}=\frac{5a+b+c}{25} \tag{4}$$

   (d) yes:

$$((a,b)\star(c,d))\star(e,f)=(ad+bc,bd)\star(e,f)=((ad+bc)\cdot f+bd\cdot e,bd\cdot f)=(adf+bcf+bde,bdf) \tag{5}$$
$$(a,b)\star((c,d)\star(e,f))=(a,b)\star(cf+de,df)=(a\cdot df+b\cdot(cf+de),b\cdot df)=(adf+bcf+bde,bdf) \tag{6}$$

   (e) no:

$$(a\star b)\star c=\frac{a}{b}\star c=\frac{a}{bc} \tag{7}$$
$$a\star(b\star c)=a\star\frac{b}{c}=\frac{a}{\frac{b}{c}}=\frac{ac}{b} \tag{8}$$

2. (a) no: $a\star b=a-b\neq b-a=b\star a$

   (b) yes: $a\star b=a+b+ab=b+a+ba=b\star a$

   (c) yes: $a\star b=\frac{a+b}{5}=\frac{b+a}{5}=b\star a$

   (d) yes: $(a,b)\star(c,d)=(ad+bc,bd)=(cb+da,db)=(c,d)\star(a,b)$

   (e) no: $a\star b=\frac{a}{b}\neq\frac{b}{a}=b\star a$

3. I usually don't distinguish between a and $\bar{a}$ but here I will. This is basically just spamming modulo n (since applying it once is the same as applying it e.g. ten times), and then using the associativity of addition.

$$\begin{aligned}(\bar{a}+\bar{b})+\bar{c}&=((a+b)\bmod n+c)\bmod n &(9)\\&=((a+b)\bmod n+c\bmod n)\bmod n &(10)\\&=(a\bmod n+(b+c)\bmod n)\bmod n &(11)\\&=(a+(b+c)\bmod n)\bmod n &(12)\\&=(\bar{a}+\bar{b})+\bar{c} &(13)\end{aligned}$$

4. This is identical to the above with all $+$'s replaced with $\cdot$'s.

5. We just showed it was associative, we know that $\bar{1}$ is the identity, so we need to show that not every element has an inverse. For $n>1$, clearly $\bar{0}$ has no inverse since $\bar{0}\cdot\bar{a}=\bar{a}\cdot\bar{0}=\bar{0}\neq\bar{1}$ for all $\bar{a}$. For $n=1$, $\bar{0}=\bar{1}$ is the only element.

6. Addition on the reals is obviously associative, and all of these examples contain the additive identity 0, so we just need to check closure and inverses.

   (a) Closure: idk
   Inverse: For any $\frac{a}{2n+1}$ in this set, $\frac{(-a)}{2n+1}$ is also in the set; the two add to zero.

   (b) no closure: $\frac{1}{2}+\frac{1}{2}=1=\frac{1}{1}$

   (c) no closure: $\frac{1}{2}+\frac{1}{2}=1$ again

   (d) no closure: $-\frac{3}{2}+1=-\frac{1}{2}$ (can't reuse the same example a third time sadly)

   (e) Closure: A (reduced) rational number with a denominator of 1 can be written with a denominator of 2: $\frac{a}{1}=\frac{2a}{2}, a\in\mathbb{Z}$. A (reduced) rational number with a denominator of 2 must have an odd numerator, since if it didn't then we could divide both top and bottom by 2; so these fractions are of the form $\frac{2b+1}{2}, b\in\mathbb{Z}$. Now just following the rules of adding even and odd numbers (in the numerators) we see that this set is closed under addition: adding two reduced rational numbers with denominator 1, or adding two numbers with a denominator 2, yields a sum with denominator 1; adding a denominator 1 with a denominator 2 gives an denominator 2.
   Inverse: The inverse of $\frac{a}{1}$ is $\frac{(-a)}{1}$; likewise for denominator 2.

   (f) no closure: $\frac{1}{2}+\frac{1}{3}=\frac{5}{6}$.

7. For $x,y\in G$, $0\le x,y<1$ so $0\le x+y<2$. If $0\le x+y<1$ then $\lfloor x+y\rfloor=0$ and $x\star y=x+y$. If $1\le x+y<2$ then $\lfloor x+y\rfloor=1$ and $x\star y=x+y-1$. These two cases cover all possibilities.

   (a) Closure: From the above, if $0\le x+y<1$ then $x\star y=x+y$ so $0\le x\star y<1$ as required. If $1\le x+y<2$, then $x\star y=x+y-1$ or $x\star y+1=x+y$ so $1\le(x\star y+1)<2$ which means $0\le x\star y<1$ as required.
   Associativity: Follow from associativity of addition over $\mathbb{R}$.
   Identity: The additive identity of addition (zero) is in G.
   Inverse: For $x\in G$, the inverse is $x^{-1}=1-x$ since $x+x^{-1}=x+(1-x)=1\equiv 0$. The exception here is that zero is its own inverse; these two rules cover all elements of G.
   Commutativity: $x\star y=x+y-\lfloor x+y\rfloor=y+x-\lfloor y+x\rfloor=y\star x$.

8. (a) Closure: If $z_1^n=z_2^n=1$, then $(z_1z_2)^n=1$.
   Associativity: Follows from associativity of multiplication over $\mathbb{C}$.
   Identity: $1^n=1$ so $1\in G$.
   Inverse: We want to show that the obvious candidate $z^{-1}=\frac{1}{z}$ is the inverse of z where $z^n=1$. Clearly $z\cdot z^{-1}=1$, so we just need to check that $z^{-1}\in G$. This follows from $\left(z^{-1}\right)^n=\left(\frac{1}{z}\right)^n=\frac{1}{z^n}=1$.

   (b) Writing each $z\in G$ in polar form, we see that $|z|=1$. Clearly $1\in G$ for all n; but $1+1=2$ has absolute value 2 and hence is not in G, so the operation of addition is not closed.

9. (a) Closure: The addition of two generic elements is $(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$. There is no weird edge case where maybe something cancels because $\sqrt{2}\notin\mathbb{Q}$ so the two terms are guaranteed to stay separate.
   Associativity: Follows from associativity of addition for $\mathbb{Q}$.
   Identity: $a+b\sqrt{2}$ with $a,b=0$ gives the additive identity.
   Inverse: For $a+b\sqrt{2}\in G$, $(-a)+(-b)\sqrt{2}\in G$; the two add to the identity of zero.

   (b) Closure: The multiplcation of two generic elements is $(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}$. Since $a,b,c,d\in\mathbb{Q}$, $ac+2bd\in\mathbb{Q}$ and $ad+bc\in\mathbb{Q}$ so the product is still in G.
   Associativity: Follows from associativity of multiplication for $\mathbb{R}$.
   Identity: $a+b\sqrt{2}$ with $a=1,b=0$ gives the multiplicative identity.
   Inverse: For $a+b\sqrt{2}$, we can define the number $\frac{1}{a+b\sqrt{2}}$ since $0\notin G$. Now we massage:

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}+\frac{(-b)}{a^2-2b^2}\cdot\sqrt{2}\,. \tag{14}$$

   Since $a,b\in\mathbb{Q}$, both $\frac{a}{a^2-2b^2}$ and $\frac{(-b)}{a^2-2b^2}$ are also in $\mathbb{Q}$, so the inverse is in G.

10. Label the elements of G as $i_1,i_2,\ldots,i_{|G|}$, and denote the matrix of the multiplication as M (so the product $i_j\cdot i_k$ is in M_{jk}). If G is abelian then $i_ji_k=i_ki_j$ for all j,k, which means $M_{jk}=M_{kj}$ for all j,k. Likewise if $M_{jk}=M_{kj}$ for all j,k, then $i_ji_k=i_ki_j$ for all j,k.

11. This question asks to find the smallest k such that $ka \equiv 0 \bmod 12$. Then $ka = \text{lcm}(a, 12)$. From the relation $\text{lcm}(a, b) \cdot (a, b) = ab$, we see $k = \frac{\text{lcm}(a,12)}{a} = \frac{12}{(a,12)}$.

$$\begin{aligned}
\bar{0} &: \text{order } 1 \text{ (identity)} \\
\bar{1} &: \text{order } 12 \\
\bar{2} &: \text{order } 6 \\
\bar{3} &: \text{order } 4 \\
\bar{4} &: \text{order } 3 \\
\bar{5} &: \text{order } 12 \\
\bar{6} &: \text{order } 2 \\
\bar{7} &: \text{order } 12 \\
\bar{8} &: \text{order } 3 \\
\bar{9} &: \text{order } 4 \\
\bar{10} &: \text{order } 6 \\
\bar{11} &: \text{order } 12
\end{aligned}$$

12.
$$\begin{aligned}
\bar{1} &: \text{order } 1 \\
-\bar{1} &: -1 \cdot -1 = 1; \text{ order } 2 \\
\bar{5} &: 5 \cdot 5 = 25 \equiv 1; \text{ order } 2 \\
\bar{7} &: 7 \cdot 7 = 49 \equiv 1; \text{ order } 2 \\
-\bar{7} &: -7 \equiv 5; \text{ order } 2 \\
\bar{13} &: 13 \equiv 1; \text{ order } 1
\end{aligned}$$

13. Again, the order is $\frac{36}{(a,36)}$, unless of course $a = 0$.

$$\begin{aligned}
\bar{1} &: \text{order } 36 \\
\bar{2} &: \text{order } 18 \\
\bar{6} &: \text{order } 6 \\
\bar{9} &: \text{order } 4 \\
\bar{10} &: \text{order } 18 \\
\bar{12} &: \text{order } 3 \\
-\bar{1} &: -1 \equiv 35 \text{ so } (35, 36) = 1; \text{ order } 36 \\
-\bar{10} &: -10 \equiv 26 \text{ so } (26, 36) = 2; \text{ order } 18 \\
-\bar{18} &: -18 \equiv 18 \text{ so } (18, 36) = 18; \text{ order } 2
\end{aligned}$$

14.
$$\begin{aligned}
\bar{1} &: \text{order } 1 \\
-\bar{1} &: -1 \cdot -1 = 1; \text{ order } 2 \\
\bar{5} &: 5^2 = 25 \to 25 \cdot 5 = 125 \equiv 17 \to 17 \cdot 5 = 85 \equiv 13 \to 13 \cdot 5 = 65 \equiv 29 \to 29 \cdot 5 = 145 \equiv 1; \text{ order } 6 \\
\bar{13} &: 13^2 = 169 \equiv 25 \to 25 \cdot 13 = 325 \equiv 1; \text{ order } 3 \\
-\bar{13} &: \text{from above, } 13^3 \equiv 1, \text{ so } (-13)^3 \equiv -1. \text{ Then } (-13)^6 \equiv -1 \cdot -1 = 1; \text{ order } 6 \\
\bar{17} &: 17^2 = 289 \equiv 1; \text{ order } 2 \text{ (thank you)}
\end{aligned}$$

15. For $n = 1$ the equality is trivial. For $n = 2$ we want the inverse of $(a_1 a_2)$. Call it x. Then

$$\begin{aligned}
(a_1 a_2)x &= 1 && (15) \\
a_2 x &= a_1^{-1} && (16) \\
x &= a_2^{-1} a_1^{-1} \; . && (17)
\end{aligned}$$

Now we want the inverse of $(a_1 \dots a_n)$, and we know the inverse of $(a_1 \dots a_{n-1})$ is $a_{n-1}^{-1} \dots a_1^{-1}$. Call the total inverse x again.

$$(a_1 \dots a_{n-1} a_n)x = 1 \tag{18}$$
$$(a_1 \dots a_{n-1})a_n x = 1 \tag{19}$$
$$a_n x = (a_1 \dots a_{n-1})^{-1} \tag{20}$$
$$a_n x = a_{n-1}^{-1} \dots a_1^{-1} \tag{21}$$
$$x = a_n^{-1} \cdot a_{n-1}^{-1} \dots a_1^{-1} \tag{22}$$

16. If $|x| = 1$ then $x^1 = x = 1$, so $x^2 = 1 \cdot 1 = 1$. If $|x| = 2$ then by definition $x^2 = 1$. For the other direction, if $x^2 = 1$, then $|x|$ is at most 2 since $|x|$ is by definition the smallest power n such that $x^n = 1$. If $|x| = 2$ then (don't hold your breath) $x^2 = 1$, if $|x| < 2$ the only option is $|x| = 1$ so $x^2 = x \cdot x \equiv 1 \cdot 1 = 1$.

17. If $n = 1$ then $x^1 = x = 1$ so trivially any power of x is the identity. For $n > 1$, expand $x^n = 1$ to get $x \cdot x \cdot \dots \cdot x = 1$ where there are a total of n factors of x. Group all but the first factor together to get $x \cdot x^{n-1} = 1$. By the uniqueness of the inverse, $x^{n-1} = x^{-1}$.

18. Start with $xy = yx$. Left multiply by y^{-1} to get $y^{-1}xy = x$. Left multiply by x^{-1} to get $x^{-1}y^{-1}xy = 1$. The other direction of implications follows from this operation being reversible since e.g. $y = \left(y^{-1}\right)^{-1}$.

19. (a) The first formula is just counting:

$$x^a x^b = \underbrace{x \dots x}_{a \text{ times}} \underbrace{x \dots x}_{b \text{ times}} = \underbrace{x \dots x x \dots x}_{a+b \text{ times}} = x^{a+b} \ . \tag{23}$$

Note that this tells us that $x^a x^a = x^{2a}$. Inductively, we get that the product of b copies of x^a is x^{ab}. More clearly, if $b = 1$ then $(x^a)^b = x^a = x^{ab}$. For $b \geq 2$ we use induction:

$$(x^a)^b = \underbrace{x^a \dots x^a}_{b \text{ times}} = x^a \underbrace{x^a \dots x^a}_{b-1 \text{ times}} = x^a \cdot x^{\overbrace{a + \dots + a}^{b-1 \text{ times}}} = x^a \cdot x^{a(b-1)} = x^{a+a(b-1)} = x^{ab} \ . \tag{24}$$

(b) The equation $(x^a)^{-1} = x^{-a}$ seems weirdly tautological so let's rephrase it as $(x^a)^{-1} = (x^{-1})^a$: multiplying a copies of the inverse of x to x^a gives the identity. Prove this inductively as well, starting with $a = 1$. Obviously multiplying 1 copy of x^{-1} to $x^1 = x$ gives the identity. Now for general $a > 1$,

$$\underbrace{x^{-1} \dots x^{-1}}_{a \text{ times}} x^a = x^{-1} \underbrace{x^{-1} \dots x^{-1}}_{a-1 \text{ times}} x^{a-1} x^1 = x^{-1} \left(\underbrace{x^{-1} \dots x^{-1}}_{a-1 \text{ times}} x^{a-1} \right) x^1 = x^{-1}(1)x^1 = x^{-1}x^1 = 1 \ . \tag{25}$$

(c) aaaaaaaaaaaaaaa

20. First we show that $\left|x^{-1}\right| \leq |x|$. If $|x| = n$, then by (25), $1 = 1^{-1} = (x^n)^{-1} = (x^{-1})^n$, so the order of x^{-1} is at most n. Now repeat the same process with x and x^{-1} switched to get that $|x| \leq \left|x^{-1}\right|$. Therefore the two must be equal.

21. If the order of x is odd then $1 = x^{2k-1}$ for some $k \geq 1$. Multiplying both sides by x, we see that

$$x = x \cdot x^{2k-1} = x^{2k} = (x^2)^k \tag{26}$$

where the second equality is by (23) and the third equality is by (24).

22. We want to find $\left|g^{-1}xg\right|$. Start multiplying it by itself to see the pattern:

$$\left(g^{-1}xg\right)^1 = g^{-1}xg \tag{27}$$
$$\left(g^{-1}xg\right)^2 = g^{-1}xgg^{-1}xg = g^{-1}x1xg = g^{-1}x^2g \tag{28}$$

so it looks like $\left(g^{-1}xg\right)^n = g^{-1}x^n g$. Prove this inductively:

$$\begin{aligned}
\left(g^{-1}xg\right)^n &= g^{-1}xg \cdot \left(g^{-1}xg\right)^{n-1} && (29)\\
&= g^{-1}xg \cdot g^{-1}x^{n-1}g && (30)\\
&= g^{-1}x(1)x^{n-1}g && (31)\\
&= g^{-1}x^n g && (32)
\end{aligned}$$

Now we first show that $|x| = n \implies \left|g^{-1}xg\right| = n$. Using $x^n = 1$ and manipulating,

$$\left(g^{-1}xg\right)^n = g^{-1}x^n g = g^{-1}(1)g = g^{-1}g = 1 \ . \tag{33}$$

Now we do the implication the other way: $\left|g^{-1}xg\right| = n \implies |x| = n$. This is just more manipulation:

$$\begin{aligned}
1 &= \left(g^{-1}xg\right)^n && (34)\\
&= g^{-1}x^n g && (35)\\
g &= gg^{-1}x^n g && (36)\\
g &= x^n g && (37)\\
gg^{-1} &= x^n gg^{-1} && (38)\\
1 &= x^n && (39)
\end{aligned}$$

23. If $1 = x^n = x^{st}$, from (24) we have $1 = (x^s)^t$ so $|x^s| = t$.

24. For $n = 0$ this is brainless: $(ab)^0 = 1 = 1 \cdot 1 = a^0 b^0$. Just as brainless for $n = 1$: $(ab)^1 = ab = a^1 b^1$. Now prove inductively for $n > 1$, assuming $(ab)^{n-1} = a^{n-1}b^{n-1}$:

$$(ab)^n = (ab)(ab)^{n-1} = (ab)a^{n-1}b^{n-1} \ . \tag{40}$$

Now we want to show that $ba^{n-1} = a^{n-1}b$ which requires induction again. For $n = 2$ we have $ba = ab$, which is true by the definition of commutativity. Then for $n > 2$,

$$ba^{n-1} = ba^{n-2} \cdot a = a^{n-2}b \cdot a = a^{n-2} \cdot ba = a^{n-2} \cdot ab = a^{n-1}b \tag{41}$$

where, if we're being pedantic, we used (23). Continuing from (40),

$$(ab)^n = (ab)a^{n-1}b^{n-1} = a(ba^{n-1})b^{n-1} = a(a^{n-1}b)b^{n-1} = a^n b^n \tag{42}$$

again using (23). Now we want to prove this for $n < 0$. More explicitly, since

$$(ab)^{-n} = ((ab)^n)^{-1} = (a^n b^n)^{-1} \tag{43}$$

(we used (25) in the first equality), we want to show that $a^{-n}b^{-n}$ is the inverse of $a^n b^n$. Multiplying the two looks like

$$1 =^? a^{-n}b^{-n} \cdot a^n b^n \ . \tag{44}$$

If we can show that b^{-n} and a^n commute then we're done since we get $1 = a^{-n}a^n \cdot b^{-n}b^n = 1 \cdot 1$. We have to show this inductively (wow!), first do it for $n = 1$:

$$ab = ba \implies b^{-1}ab = b^{-1}ba = a \implies b^{-1}abb^{-1} = ab^{-1} \implies b^{-1}a = ab^{-1} \ . \tag{45}$$

Now inductively we assume that $b^{-(n-1)}a^{(n-1)} = a^{(n-1)}b^{-(n-1)}$ for $n > 1$. Then

$$b^{-n}a^n = b^{-1}\left(b^{-(n-1)}a^{(n-1)}\right)a = b^{-1}\left(a^{(n-1)}b^{-(n-1)}\right)a \ . \tag{46}$$

We need to show that we can commute b^{-1} with powers of a, and vice versa. Luckily we already did this in (41) and (42); e.g. we can just rename $b^{-1} \to b$ since the only fact that was used was that these two elements commute. Finally we have

$$b^{-n}a^n = b^{-1}a^{(n-1)}b^{-(n-1)}a = a^{(n-1)}b^{-1}b^{-(n-1)}a = a^{(n-1)}b^{-n}a = a^{(n-1)}ab^{-n} = a^n b^{-n} \tag{47}$$

(using (23) twice) as required.

25. If $x^2 = 1$ for all $x \in G$, then picking any two elements x and y, their product squares to the identity: $1 = (xy)^2 = xyxy$. Then

$$xy = x(1)y = x(xyxy)y = (xx)yx(yy) = (1)yx(1) = yx \ . \tag{48}$$

26. Closure: We are told that for all $h, k \in H$, $hk \in H$.
Associativity: This is inherited from the associativity of G since all elements in H are also in G.
Inverse: We are given that for all $h \in H$, $h^{-1} \in H$.
Identity: If $h \in H$, then $h^{-1} \in H$, and $hh^{-1} = 1 \in H$.

27. In the language of the previous exercise, let $H(x) = \{x^n \mid n \in \mathbb{Z}\}$. We want to show that for all $h, k \in H(x)$, we have $hk \in H(x)$ and $h^{-1} \in H(x)$. From the form of H we have $h = x^m$ and $k = x^n$ for some $m, n \in \mathbb{Z}$. Then $hk = x^m x^n = x^{m+n} \in H(x)$ by (23) and $h^{-1} = (x^m)^{-1} = x^{-m} \in H(x)$ by (25).

28. Given the groups $(A, \star)$ and $(B, \diamond)$, for the group $A \times B$ we have

    (a) Associativity: follows from algebra bashing using the associativity of A and B in the third equality

$$\begin{aligned}
(a_1, b_1)\left[(a_2, b_2)(a_3, b_3)\right] &= (a_1, b_1)\left[(a_2 \star a_3, b_2 \diamond b_3)\right] && (49)\\
&= (a_1 \star (a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3)) && (50)\\
&= ((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3) && (51)\\
&= \left[a_1 \star a_2, b_1 \diamond b_2\right](a_3, b_3) && (52)\\
&= \left[(a_1, b_1)(a_2, b_2)\right](a_3, b_3) && (53)
\end{aligned}$$

    (b) Identity: We want to show that $ae = ea = a$ for all $a \in A \times B$, with $e = (1_A, 1_B)$:

$$\begin{aligned}
(a, b)(1_A, 1_B) &= (a \star 1_A, b \diamond 1_B) = (a, b) && (54)\\
(1_A, 1_B)(a, b) &= (1_A \star a, 1_B \diamond b) = (a, b) && (55)
\end{aligned}$$

    (c) Inverse: We want to show that $(a, b)^{-1} = (a^{-1}, b^{-1})$:

$$(a^{-1}, b^{-1})(a, b) = (a^{-1} \star a, b^{-1} \diamond b) = (1_A, 1_B) = 1 \tag{56}$$

    Since $a^{-1} \in A$ and $b^{-1} \in B$, (a^{-1}, b^{-1}) is in $A \times B$ and this is well-defined.

29. Use the same notation from the previous exercise. For arbitrary (a, b) and $(c, d) \in A \times B$,

$$(a, b)(c, d) = (a \star c, b \diamond d) \ . \tag{57}$$

If $A \times B$ is abelian, then we also have

$$(a, b)(c, d) = (c, d)(a, b) = (c \star a, d \diamond b) \tag{58}$$

which tells us that $a \star c = c \star a$ (for arbitrary $a, c \in A$) meaning A is abelian. The same can be said for B. This works in the other direction: if A and B are both abelian then

$$(a, b)(c, d) = (a \star c, b \diamond d) = (c \star a, d \diamond b) = (c, d)(a, b) \ . \tag{59}$$

30. Proving $(a, 1_B)$ and $(1_A, b)$ commute is trivial:

$$(a, 1_B)(1_A, b) = (a \star 1_A, 1_B \diamond b) = (a, b) = (1_A \star a, b \diamond 1_B) = (1_A, b)(a, 1_B) \ . \tag{60}$$

Then, using the result from exercise 24 to split apart the product group (please don't make me prove the last equality),

$$(a, b)^n = ((a, 1_B)(1_A, b))^n = (a, 1_B)^n (1_A, b)^n = (a^n, 1_B)(1_A, b^n) \ . \tag{61}$$

If we want $|(a, b)| = n$ then we must have both $a^n = 1_A$ and $b^n = 1_B$. The smallest positive n that satisfies this condition is the least common multiple of $|a|$ and $|b|$.

31. Following the hint, let $t(G)$ be the set of all elements in G that are not their own inverse. From exercise 32 we know that, since G is a finite group, the order of all $x \in G$ is finite. Choose an arbitrary element x and call its order n, then
$$1 = x^n = x \cdot x^{n-1} \implies x^{-1} = x^{n-1} \; . \tag{62}$$
If $n > 2$, then $x \neq x^{n-1}$, so we have found two elements that are not their own inverse: x and x^{-1}. Add these to $t(G)$. Continuing like this and finding all such pairs in G (double-counting is fine; we just care that they come in pairs), we end up with an even number of elements in $t(G)$. Clearly, $1 \notin t(G)$ since the identity is its own inverse. That means the set $t(G) \cup 1$ has an odd number of elements in it, and contains all $x \in G$ such that $|x| = 1$ or $|x| > 2$. Then $G - (t(G) \cup 1)$, assuming it is nonempty, contains all elements of order 2. If $|G|$ is even, then this set must contain an odd (i.e. nonzero) number of elements, hence there is at least one element of order 2.

32. Prove the contrapositive. Suppose that $1, x, x^2, \ldots, x^{n-1}$ are not all distinct, i.e. there exist $a, b \in \mathbb{Z}$ with $0 \leq a < b \leq n-1$ such that $x^a = x^b$. Then, multiplying both sides by x^{-a} and using (23) we see
$$1 = x^{-a}x^a = x^{-a}x^b = x^{b-a} \tag{63}$$
so $|x| = b - a < n$. Then it cannot be the case that $|x| = n$.
Since there are $|G|$ distinct elements in G (duh), by the sequence of $|G|+1$ elements $1, x, x^2, \ldots, x^{|G|}$ cannot contain $|G|+1$ distinct elements. Following the above argument, we see that $|x| < |G| + 1$ meaning $|x| \leq |G|$.

33. If $x^n = 1$ for some n then, for some given power x^a,
$$(x^i)^{-1} = x^{-i} = 1 \cdot x^{-i} = x^n x^{-i} = x^{n-i} \tag{64}$$
using (25) and (23), so if we want the two equal we require $i = n - i$ (more technically, both sides are modulo n), so $n = 2i$.

    (a) If n is odd then there is no i such that $n = 2i$, so the above is impossible.

    (b) If n is even, then there is only one solution for i (modulo n), and we have $n = 2i$.

34. Prove the contrapositive. Suppose that the elements $x^n, n \in \mathbb{Z}$ are not all distinct. That means there exist $a, b \in \mathbb{Z}$ such that $x^a = x^b$. Then, multiplying both sides by x^{-a} and using (23) we see
$$1 = x^{-a}x^a = x^{-a}x^b = x^{b-a} \tag{65}$$
so we see $|x| = b - a$, so x does not have infinite order.

35. Suppose $|x| = n$ for some finite (duh) integer $n > 0$, so $x^n = 1 = 1^{-1} = x^{-n}$. Consider an arbitrary power x^a. By the division algorithm, we can write $a = qn + r$ for some $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then
$$x^a = x^{qn+r} = x^{qn}x^r = (x^n)^q x^r = 1^q x^r = 1x^r = x^r \tag{66}$$
where the second equality is by (23) and the third equality is by (24). We see that $x^a = x^{a \bmod n}$.

36. not sure how to do this using the hint about cancellation rules, the only way I could do this was extremely ugly and trial and error; it'd be easier if I could use the fact that no element has order 3 but we're not there yet

1.2: Dihedral Groups

Page 25 – D_{2n} Relations

Given an regular n-gon with its vertices labeled 0 through $n-1$, denote the set of all vertices $S = \{0, 1, \ldots, n-1\}$. This makes modular arithmetic much easier, and is equivalent to the textbook formulation; just add 1 to every label. Then any element $g \in D_{2n}$ sends each vertex to some (possibly the same) vertex, so we have a corresponding function $\sigma_g : S \to S$. We want to describe r and s in terms of their corresponding functions in order to understand arbitrary compositions of them. We (the textbook authors) have already established what σ_r is:
$$\sigma_r(i) = \begin{cases} i+1 \; , & 0 \leq i < n-1 \\ 0 \; , & i = n-1 \end{cases} \tag{67}$$

which can be written in the succinct form (this is why I labeled them 0 to $n-1$)

$$\sigma_r(i) = (i+1) \bmod n \ . \tag{68}$$

For σ_s we go vertex-by-vertex. Since the axis of reflection goes through vertex 0, clearly this is a fixed point with $\sigma_s(0) = 0$. The two adjacent vertices, labeled by 1 and $n-1$, swap under the action of s. The two vertices after, 2 and $n-2$ also switch. This goes all the way around the polygon, so the total description is

$$\sigma_s(i) = \begin{cases} n-i \ , & 0 < i \leq n-1 \\ 0 \ , & i = 0 \end{cases} \tag{69}$$

and, since $n - 0 = n \equiv 0$ when considered modulo n, we can combine the two cases into

$$\sigma_s(i) = (n-i) \bmod n = -i \bmod n \ . \tag{70}$$

1. Given σ_r, the action of σ_{r^2} is easy:

   $$\sigma_{r^2}(i) = \sigma_r(\sigma_r(i)) = \sigma_r((i+1) \bmod n) = (((i+1) \bmod n) + 1) \bmod n = ((i+1)+1) \bmod n = (i+2) \bmod n \ . \tag{71}$$

   Inductively,

   $$\sigma_{r^k}(i) = \sigma_r(\sigma_{r^{k-1}}(i)) = \sigma_r\left((i+k-1) \bmod n\right) = (((i+k-1) \bmod n) + 1) \bmod n = (i+k) \bmod n \ . \tag{72}$$

   The easiest way to show that r^k and r^l ($0 \leq k, l < n$ and $k \neq l$) are different transformations is to show that there exists an i such that $\sigma_{r^k}(i) \neq \sigma_{r^l}(i)$. This is easily verified by choosing $i = 0$: $\sigma_{r^k}(0) = k$ and $\sigma_{r^l}(0) = l$, so these cannot be the same function and hence r^k and r^l are not the same transformation. Showing that $r^n = 1$ is just as straightforward:

   $$\sigma_{r^n}(i) = (i+n) \bmod n = i \bmod n = i \tag{73}$$

   where the last equality is because $0 \leq i < n$. Since σ_{r^n} is the identity map on all of S, r^n is the identity element of D_{2n}.

2. We know what σ_s is so we just compose it twice:

   $$\sigma_{s^2}(i) = \sigma_s(\sigma_s(i)) = \sigma_s(-i \bmod n) = -(-i \bmod n) \bmod n = -(-i) \bmod n = i \bmod n = i \tag{74}$$

   where, again, the last equation is because $0 \leq i < n$. Just as in the above example, this shows that $s^2 = 1$. Obviously $s \neq 1$ so we see $|s| = 2$.

3. This is easily shown by looking at the image of 0 and 1. The action of s has $\sigma_s(0) = 0$ and $\sigma_s(1) = n-1$. If we want a power of r that recreates $0 \mapsto 0$ then we want $\sigma_{r^k}(0) = (0+k) \bmod n = k \bmod n = 0$ so we have k is a multiple of n, write it $k = an$. But then $r^k = r^{an} = (r^n)^a = 1^a = 1$ so we must have $\sigma_{r^k}(1) = 1$. The only way this can agree with σ_s is if $n = 2$, but then we don't even have a polygon to begin with.

4. We want to show that $sr^k \neq sr^l$ (again for $0 \leq k, l < n$ and $k \neq l$). Again, this just requires showing that there is one element $i \in S$ such that $\sigma_{sr^k}(i) \neq \sigma_{sr^l}(i)$. Choose $i = 0$ again; the left-hand side is

   $$\sigma_{sr^k}(0) = \sigma_s(\sigma_{r^k}(0)) = \sigma_s(k \bmod n) = -(k \bmod n) \bmod n = -k \bmod n \tag{75}$$

   and likewise the right-hand side is $-l \bmod n$. Since $k \neq l$, $n - k \neq n - l$ so $-k$ and $-l$ are different equivalence classes modulo n.

5. We can show this for all $i \in S$, but first we need to establish what $\sigma_{r^{-1}}$ is. Since $r^n = 1$, we immediately have $r^{-1} = r^{n-1}$ which means

   $$\sigma_{r^{-1}}(i) = \sigma_{r^{n-1}}(i) = (i+n-1) \bmod n = (i-1) \bmod n \tag{76}$$

   as expected. Now to show $rs = sr^{-1}$ by showing $\sigma_r \circ \sigma_s = \sigma_s \circ \sigma_{r^{-1}}$. The left-hand side is

   $$\sigma_r(\sigma_s(i)) = \sigma_r(-i \bmod n) = ((-i \bmod n) + 1) \bmod n = (-i+1) \bmod n \ . \tag{77}$$

   The right-hand side is

   $$\sigma_s(\sigma_{r^{-1}}(i)) = \sigma_s((i-1) \bmod n) = -((i-1) \bmod n) \bmod n = -(i-1) \bmod n = (-i+1) \bmod n \ . \tag{78}$$

6. We have already shown equality for $k = 1$. Now inductively commute all but one power of r, then do the last by itself:

   $$r^k s = r(r^{k-1}s) = r(sr^{-(k-1)}) = (rs)r^{-(k-1)} = (sr^{-1})r^{-(k-1)} = s(r^{-1}r^{-(k-1)}) = sr^{-k} \ . \tag{79}$$

Page 27 – "it is easy to see"

not sure, following the discussion for X_{2n} I just get $r = r$ lol

Exercises

1. The elements of D_{2n} are $\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$. A lot of these have the same answers: consider sr^k for some $k \geq 1$. Squaring it gives
$$(sr^k)^2 = (sr^k)(sr^k) = s(r^k s)r^k = s(sr^{-k})r^k = s^2 r^{-k} r^k = s^2 = 1 \tag{80}$$
so every element of this form has order 2. We also know $s^2 = 1$, and we made no reference to k being positive, so this is in fact true for all integer k.

   (a) for D_6, $n = 3$:
   $$\begin{aligned} 1 &: 1 \\ r &: 3 \\ r^2 &: r^6 = (r^2)^3 = 1 \text{ so order is 3; note this is } \tfrac{\operatorname{lcm}(2,3)}{2} \text{ which is equivalent to } \tfrac{3}{(2,3)} \text{ (c.f. exercise 1.1.11)} \\ s &: 2 \\ sr &: 2 \\ sr^2 &: 2 \end{aligned}$$

   (b) for D_8, $n = 4$:
   $$\begin{aligned} 1 &: 1 \\ r &: 4 \\ r^2 &: \tfrac{4}{(2,4)} = 2 \\ r^3 &: \tfrac{4}{(3,4)} = 4 \\ s &: 2 \\ sr &: 2 \\ sr^2 &: 2 \\ sr^3 &: 2 \end{aligned}$$

   (c) for D_{10}, $n = 5$:
   $$\begin{aligned} 1 &: 1 \\ r &: 5 \\ r^2 &: \tfrac{5}{(2,5)} = 5 \\ r^3 &: \tfrac{5}{(3,5)} = 5 \\ r^4 &: \tfrac{5}{(4,5)} = 5 \\ s &: 2 \\ sr &: 2 \\ sr^2 &: 2 \\ sr^3 &: 2 \\ sr^4 &: 2 \end{aligned}$$

2. If x is not a power of r, then we can write it in the form sr^k. Now do the algebra bash:
$$rx = r(sr^k) = (rs)r^k = (sr^{-1})r^k = sr^{k-1} = (sr^k)r^{-1} = xr^{-1} \ . \tag{81}$$

3. See (80). D_{2n} is generated by $\{r, s\}$, but we can write $r = s \cdot sr$, so we can also generate the group with $\{sr, s\}$. We already knew $s^2 = 1$; we have shown $(sr)^2 = 1$.

4. If $n = 2k$, then $1 = r^n = r^{2k} = (r^k)^2$ so r^k has order 2 (and is its own inverse). Any element of D_{2n} is either r^l for some l, or sr^l. Commutation is obvious in the first case since $r^k r^l = r^{k+l} = r^{l+k} = r^l r^k$ (I guess I showed it anyway). In the second case, we can use (81) to inductively show that $r^l x = xr^{-l}$:
$$r^l x = r(r^{l-1}x) = r(xr^{1-l}) = (rx)r^{1-l} = xr^{-1}r^{1-l} = xr^{-l} \ . \tag{82}$$
We see that r^l commutes with any and all of these x elements exactly when $r^l = r^{-l} = r^{n-l}$. For $0 \leq l < n$, the only solutions are the identity (trivial), and $n = 2l$. We see that r^k is the only element (other than the identity) that commutes with everything.

5. This follows from my solution of the previous exercise; there is no solution to $n = 2l$ if n is odd, so there is no second element that commutes with everything.

6. If x and y are order two then $x = x^{-1}$ and $y = y^{-1}$. Then $t^{-1} = (xy)^{-1} = y^{-1}x^{-1} = yx$ so

$$tx = (xy)x = x(yx) = xt^{-1} \ . \tag{83}$$

7. Two of the relations follow trivially since $a = s$ and $ab = ssr = r$:

$$s^2 = 1 \iff a^2 = 1 \tag{84}$$
$$(ab)^n = 1 \iff r^n = 1 \tag{85}$$

The last relation is also pretty easy:

$$b^2 = 1 \iff b = b^{-1} \iff sr = (sr)^{-1} \iff sr = r^{-1}s^{-1} = r^{-1}s \iff r = sr^{-1}s \iff rs = sr^{-1} \tag{86}$$

8. The order is n... this seems so easy I think I have to be interpreting it incorrectly... we showed in (72) and (73) that $1, r, r^2, \ldots r^{n-1}$ are all distinct, and $r^n = 1$.

9. These problems seem intimidating but have a straightforward solution. If we orient the solid such that one face is on "the bottom", and specify the rotation of this face, we have fixed the entire solid. The rotational symmetry group of the face is $\mathbb{Z}/3\mathbb{Z}$ so it has three elements. There are four possible faces we can choose to be on the bottom, so the total number of automorphisms of the vertices of a tetrahedron is $4 \cdot 3 = 12$.

10. Likewise, the cube has six faces, each of which has 4 vertices, so $6 \cdot 4 = 24$.

11. Eight faces, three vertices on a face, $8 \cdot 3 = 24$.

12. Twelve faces, five vertices on a face, $12 \cdot 5 = 60$.

13. Twenty faces, three vertices on a face, $20 \cdot 3 = 60$.

14. Wasn't this given as an example? $\mathbb{Z} = \langle\, 1 \,\rangle$.

15. We can reach every element of $\mathbb{Z}/n\mathbb{Z}$ by repeatedly adding 1 to itself. The only condition is that $n = 0$ so

$$\mathbb{Z}/n\mathbb{Z} = \langle\, 1 \mid n(1) = 0 \,\rangle \ . \tag{87}$$

16. Take exercise 7 and set $n = 2$.

17. We already know that $|X_{2n}| \leq 6$, and $x^3 = 1$ for any n. That means $x^2 = x^{-1}$ and the relation $xy = yx^2$ can be rewritten $xy = yx^{-1}$, which is the same as the relation for D_{2n} with y taking the role of s and x taking the role of r. The other relations are $y^2 = 1$, which is identical to $s^2 = 1$, and $x^n = 1$.

    (a) If $n = 3k$, then $1 = x^n = x^{3k} = (x^3)^k = 1^k$ and the condition that $x^n = 1$ is the same as the condition that $x^3 = 1$. We have $x^3 = y^2 = 1$ and $xy = yx^{-1}$, which is the presentation for D_6. The elements are $1, x, x^2, y, yx, yx^2$.

    (b) If $(3, n) = 1$ then there exist integers a, b such that $3a + nb = 1$. Then

    $$x = x^1 = x^{3a+nb} = x^{3a}x^{nb} = (x^3)^a(x^n)^b = 1^a1^b = 1 \tag{88}$$

    and the only elements of the group are 1 and y.

18. The presentation is $Y = \langle\, u, v \mid u^4 = v^3 = 1, uv = v^2u^2 \,\rangle$.

    (a) This is so easy that I used it without comment in the previous exercise. Take $v^3 = 1$ and apply v^{-1} to both sides to get $v^2 = v^{-1}$.

    (b) Lots of algebra bashing:

    $$vu^3 = vu1u^2 = vuv^3u^2 = v(uv)(v^2u^2) = v(v^2u^2)(uv) = v^3u^3v = u^3v \ . \tag{89}$$

(c) Since $u^4 = 1$, $u = (u^4)^2 u = u^8 u = u^9$. Then

$$vu = vu^9 = vu^3u^3u^3 = u^3vu^3u^3 = u^3u^3vu^3 = u^3u^3u^3v = u^9v = uv \ . \tag{90}$$

(d) Now that we know we can arbitrarily commute u and v, the last relation becomes

$$uv = v^2u^2 = uvuv = (uv)^2 \implies 1 = uv \ . \tag{91}$$

(e) Use $u^4 = v^3 = 1$:

$$1 = 1 \cdot 1 = u^4v^3 = uvuvuvu = (uv)^3u = 1^3u = u \ , \tag{92}$$

then since $uv = 1$ we see that we also have $v = 1$. Since Y is generated by $u = 1$ and $v = 1$, and arbitrary products of 1 still equal to 1, we find that the only element of Y is the identity.