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. idk how to prove something is well defined

   (a) Closure: this is so obvious I don't even know what to write
   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 $ka = \mathrm{lcm}(a, 12)$. From the relation $\mathrm{lcm}(a,b) \cdot (a,b) = ab$, we see $k = \frac{\mathrm{lcm}(a,12)}{a} = \frac{12}{(a,12)}$.

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

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

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. The easy direction first: if $|x| = 1$ then $x^1 = x = 1$, so $x^2 = 1 \cdot 1 = 1$. If $|x| = 2$ then by definition $x^2 = 1$. The other direction idk

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 $x \cdot x \cdot \ldots \cdot x = 1$ 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. $y = \left(y^{-1}\right)^{-1}$.