Math 504 HW1

Rohan Mukherjee

November 17, 2023

1. Let e_1, e_2 both be identity elements of a group G. Then, $e_1 = e_1e_2 = e_2$, since we have by definition that $e_1x = xe_1 = x$ for all $x \in G$. Similarly, let $a \in G$ and b, c both be inverses of a. Then, $b = b \cdot (a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c$.

2. (a) Suppose instead that $n \nmid m$. Then write $m = bn + r$ for some $1 \leq r < n$. We thus have:

$$e = a^m = a^{bn+r}a^{bn} \cdot a^r = e^b \cdot a^r = a^r$$

But this contradicts the minimality of n.

(b) Let $G = \langle a \rangle$ be cyclic, and $H \leq G$. It follows that every element of H is of the form a^k for some $k \geq 0$ (Since $H \leq G$). Consider the set $Z = \left\{ k \in \mathbb{Z}^+ \;\middle|\; a^k \in H \right\}$. If H is the trivial subgroup then we are done, else Z is nonempty and thus has a minimal element ℓ by the well ordering principle. We claim that $H = \langle a^\ell \rangle$. Indeed, since H is closed under products, we have $(a^\ell)^n = a^{n\ell} \in H$ for any $n \geq 1$. Suppose instead that $H \not\subset \langle a^\ell \rangle$. Then there is some m not divisible by ℓ such that $a^m \in H$. Now write $m = b\ell + r$, with $1 \leq r < l$. Then we have $a^m \cdot a^{-b\ell} = a^r \in H$, but this contradicts the minimality of ℓ. Thus $H = \langle a^\ell \rangle$, which completes the proof.

(c) Write $G = \langle a \rangle$. We claim that $\mathrm{Im}\{f\} = \langle f(a) \rangle$. First notice that $\mathrm{Im}\{f\} \supset \langle f(a) \rangle$, since it contains $f(a)$ and is closed under products. Next, given an element $b \in \mathrm{Im}\{f\}$, by definition we can write $b = f(g)$ for some $g \in G$, and since $g = a^k$ for some $k \geq 0$, we have $b = f(a^k) = f(a)^k$, which shows that $b \in \langle f(a) \rangle$, completing the proof.

(d) Since $\mathbb{Z}$ is cyclic, any subgroup is also cyclic by part (b). Thus the only possible subgroups are those of the form $m\mathbb{Z} = \{ mz \mid z \in \mathbb{Z} \} = \langle m \rangle$, and since these are all subgroups, we are done.

(e) Since $\mathbb{Z}/m\mathbb{Z}$ is cyclic, all subgroups are of the form $\langle k \rangle$ for some $k \in \mathbb{Z}/m\mathbb{Z}$. We claim that $|\langle k \rangle| = m/\gcd(m,k)$. We are looking for the smallest integer n such that nk is a multiple of m. Notice that nk is also a multiple of k, so if we could find such an n $nk \geq \mathrm{lcm}(m,k) = k \cdot (m/\gcd(m,k))$. So we have that $n \geq m/\gcd(m,k)$. We see that $n = m/\gcd(m,k)$ yields a multiple of k, m since $nk = \mathrm{lcm}(m,k)$, which is a multiple of both m and k, which proves the above claim. Up to isomorphism, we just get $\mathbb{Z}/d\mathbb{Z}$ for $d \mid m$ as all the subgroups (by taking $k = m/d$).

3. (a) I claim that $\langle r^2 s\rangle \trianglelefteq \langle s, r^2\rangle \trianglelefteq D_8$, but $\langle r^2 s\rangle$ is not normal in D_8. Notice that $\langle s, r^2\rangle = \{e, s, r^2, r^2 s = sr^2 = r^{-2}s = r^2 s\}$, so $\langle s, r^2\rangle \trianglelefteq D_8$ since it is a subgroup of index 2. We also see that $\langle r^2 s\rangle = r^2 s, ((r^2)s)^2 = r^2 s, r^2 s r^2 s = r^2 s s r^{-2} = e$, which is another subgroup of index 2 so is normal in $\langle s, r^2\rangle$. However, $r(r^2 s)r^{-1} = r^3 s r^3 = s$, which is not in $\langle r^2 s\rangle$, which proves the claim.

   (b) We see that $\mathbb{Z}/6 = \langle 1\rangle$, which is obviously minimal. I claim that $\{2, 3\}$ is also minimal. First notice that $\langle 2, 3\rangle$ contains $3 - 1$ so $\mathbb{Z}/6 = \langle 1\rangle \subset \langle 2, 3\rangle$, so it is indeed a generator. However, $\langle 2\rangle = \{0, 2, 4\}$, and $\langle 3\rangle = \{0, 3\}$, neither of which are the whole group, so $\{2, 3\}$ is indeed minimal.

   (c) We see that $\mathbb{Z} \times \mathbb{Z} = \langle (1, 0), (0, 1)\rangle$.

4. If we plug $b = c = e$, we get,

$$a * d = (a \circ e) * (e \circ d) = (a * e) \circ (e * d) = a \circ d$$

Which shows they coincide. With this knowledge, if we plug in $b = e$, we get,

$$a * (c * d) = (a * c) * d$$

Finally, if we plug in $a = d = e$, we get $b * c = c * b$.

5. (a) Notice that $(0, (1, 0, 0))(0, (0, 1, 0)) = (0, (1, 0, 0) \times (0, 1, 0)) = (0, (0, 0, 1))$ while $(0, (0, 1, 0))(0, (1, 0, 0)) = (0, (0, 0, -1))$, so the operation isn't commutative. We see that

$$\begin{aligned}
&((a, u)(b, v))(c, w) = (ab - u \cdot v, av + bu + u \times v)(c, w) \\
&= (abc - c \cdot u \cdot v - (a \cdot w \cdot v + b \cdot w \cdot u + w \cdot (u \times v)), (ab - u \cdot v)w + c(av + bu + u \times v))
\end{aligned}$$

   On the other hand, we get

$$\begin{aligned}
&(a, u)((b, v)(c, w)) = (a, u)(bc - v \cdot w, bw + cv + v \times w) \\
&= (abc - a \cdot v \cdot w - (b \cdot u \cdot w + c \cdot u \cdot v + u \cdot (v \times w), a(bw + cv + v \times w) +
\end{aligned}$$

   (b) We see that if $N((a, u)) = 0$, we must have $a^2 = 0$ and $|u|^2 = 0$ which occurs iff $a = 0$ and $u = 0$. Thus, if $\alpha, \beta \neq 0$, since $N(\alpha\beta) = N(\alpha)N(\beta) \neq 0$, we have that $\alpha\beta \neq 0$. First, I claim that $(1, 0)$ is the identity. We see that $(a, u)(1, 0) = (a - u \cdot 0, 1 \cdot u + 0 \times u) = (a, u)$. I also claim that if $(a, u) \neq 0$, then the inverse of (a, u) is just $(a/(a^2 + |u|^2), -u/(a^2 + |u|^2))$. Indeed,

$$(a, u) \cdot (a/(a^2 + |u|^2), -u/(a^2 + |u|^2)) = \left(\frac{a^2}{a^2 + |u|^2} + \frac{|u|^2}{a^2 + |u|^2}, -a\frac{u}{a^2 + |u|^2} + a\frac{u}{a^2 + |u|^2}\right) = (1, 0)$$

   (c) First notice that if (a, u) and (b, v) have integer coefficients, then then $ab - u \times v$ will be the sum / difference of integers and thus also an integer, $av + bu$ will be a vector with integer coefficients, and $u \times v$ will be another vector with integer coefficients just from the formula. Now, if (a, u), (b, v) have norm 1, then the norm of their product is also 1, so this set is closed under products. It is closed under inverses by looking at the inverse formula–$(a/N(\alpha), -u/N(\alpha)) = (a, -u)$. We now consider the ways to get $N(\alpha) = 1$: either $a = \pm 1$ and $u = 0$, or $a = 0$ and $u_1 = \pm 1$, or $u_2 = \pm 1$, or $u_3 = \pm 1$, which gives 8 elements. Visually:

$$Q_8 = \left\{ (\pm 1, 0), \left(0, \begin{pmatrix} \pm 1 \\ 0 \\ 0 \end{pmatrix}\right), \left(0, \begin{pmatrix} 0 \\ \pm 1 \\ 0 \end{pmatrix}\right), \left(0, \begin{pmatrix} 0 \\ 0 \\ \pm 1 \end{pmatrix}\right) \right\}$$

$\boxed{a)}$ $((a,u)(b,v))(c,w) = (ab - u\cdot v,\ av + bu + u\times v)(c,w)$

$$= \Big(cab - c\,u\cdot v - w\cdot(av + bu + u\times v),$$
$$(ab - u\cdot v)w + c(av + bu + u\times v)$$
$$+ (av + bu + u\times v)\times w\Big)$$

$$= \Big(cab - c\,\vec{u}\cdot\vec{v} - a\,\vec{v}\cdot\vec{w} - b\,\vec{u}\cdot\vec{w} - \vec{w}\cdot(\vec{u}\times\vec{v}),$$
$$ab\,\vec{w} - (\vec{u}\cdot\vec{v})\vec{w} + ca\vec{v} + cb\vec{u} + c\,\vec{u}\times\vec{v}$$
$$+ a\,\vec{v}\times\vec{w} + b\,\vec{u}\times\vec{w} + (\vec{u}\times\vec{v})\times\vec{w}\Big)$$

vs. :

$$(a,u)(bc - v\cdot w,\ bw + cv + \vec{v}\times\vec{w})$$

$$= \Big(abc - a\,\vec{v}\cdot\vec{w} - \vec{u}\cdot(b\vec{w} + \vec{v} + \vec{v}\times\vec{w}),$$
$$ab\vec{w} + ac\vec{v} + a\,\vec{v}\times\vec{w} + bc\,\vec{u} - (\vec{v}\cdot\vec{w})\vec{u}$$
$$+ b\,\vec{u}\times\vec{w} + c\,\vec{u}\times\vec{v} + \vec{u}\times(\vec{v}\times\vec{w})\Big)$$

Green: $\vec{u}\cdot(\vec{v}\times\vec{w}) \stackrel{?}{=} \vec{w}\cdot(\vec{u}\times\vec{v})$ ✓

(Standard identity)

Now: Does $\vec{u} \times (\vec{v} \times \vec{w}) - (\vec{v} \cdot \vec{w})\vec{u}$

$$\overset{?}{=} (\vec{u} \times \vec{v}) \times \vec{w} - (\vec{u} \cdot \vec{v})\vec{w}$$

Recall: $\vec{u} \times (\vec{v} \times \vec{w}) = (\vec{u} \cdot \vec{w})\vec{v} - (\vec{u} \cdot \vec{v})\vec{w}$

and: $\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}$

So: $(\vec{u} \times \vec{v}) \times \vec{w} = -\vec{w}(\vec{u} \times \vec{v})$

$$= -\left((\vec{w} \cdot \vec{v}) \cdot \vec{u} - (\vec{w} \cdot \vec{u}) \cdot \vec{v}\right)$$

$$= (\vec{w} \cdot \vec{u}) \cdot \vec{v} - (\vec{w} \cdot \vec{v})\vec{u}$$

$\square$

So yes, associative.

$\boxed{b)}$ $N((a,u)(b,v)) = N((ab - u\cdot v,\ av + bu + u\times v))$

$$= (ab - u\cdot v)^2 + (av + bu + u\times v)\cdot(av + bu + u\times v)$$

$$= a^2b^2 + (u\cdot v)^2 - 2\cancel{ab(u\cdot v)} + a^2|v|^2 + b^2|u|^2 + (|u\times v|)^2 + 2a\,v\cdot(u\times v) + 2\cancel{b\,u\cdot(u\times v)} + 2\cancel{ab\,u\cdot v}$$

θ (orthogonal)

$$(u\cdot v)^2 = |u|^2|v|^2\cos^2\theta$$
$$+|u\times v|^2 = |u|^2|v|^2\sin^2\theta$$
$$= |u|^2|v|^2$$

$$= a^2b^2 + |u|^2|v|^2 + a^2|v|^2 + b^2|u|^2$$

$$N((a,u))\cdot N((b,v)) = (a^2 + |u|^2)(b^2 + |v|^2)$$
$$= a^2b^2 + a^2|v|^2 + b^2|u|^2 + |u|^2|v|^2 \checkmark$$