1. **(6 × 5 = 30 points)** Write down or complete the precise definitions of the following concepts.

(a) Given a group G, define the **order** of $g \in G$.

If $\langle g \rangle$ is a finite group, we define the order of g to be the order of $\langle g \rangle$, and in this case we write $\boxed{\operatorname{ord}(g) := |\langle g \rangle|}$

If $\langle g \rangle$ is not a finite group, we say g is of infinite order.

(b) A group P is **abelian** if

A group P is abelian if $\forall\, x, y \in \cancel{G}\, P$ we have $xy = yx$.

(c) A group Q is **cyclic** if

A group Q is cyclic if there exists $x \in Q$ such that $Q = \langle x \rangle$.

(d) Define an **automorphism** of a group G.

A map $\phi : G \to G$ is an automorphism of a group G if ϕ is an isomorphism,

i.e. ϕ is bijective, and
ϕ is a homomorphism, i.e. $\forall\, x, y \in G \quad \phi(xy) = \phi(x)\phi(y)$.

(e) Given $r, s \in \mathbb{Z}^+$, define the **greatest common divisor** of r and s.

The positive generator $d \in \mathbb{Z}^+$ of the cyclic group $r\mathbb{Z} + s\mathbb{Z}$ (i.e. $\langle d \rangle = r\mathbb{Z} + s\mathbb{Z}$) is defined to be the greatest common divisor of r and s, and is denoted by $d = \gcd(r, s)$.

(f) Define the **Klein 4-group**.

The Klein 4-group, denoted by V, is defined as follows:

$V := \{e, a, b, c\}$ with bin. op. defined via the Cayley table

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

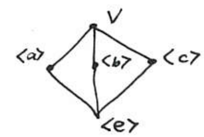
2. **(6 × 5 = 30 points)** Indicate whether the statement is true or false. Provide brief justifications for your answers. If the statement is false, it may be most efficient to give a counterexample.

(a) Every abelian group is cyclic.

#6.32(b)

☐ True

☒ False — The Klein 4-group V is abelian but not cyclic.



(b) If a is an element of a group G with $a^n = e$ for some $n \in \mathbb{Z}^+$, then $\text{ord}(a) = n$.

p.59 and #6.30, p.66

☐ True

☒ False

Consider V again.

Then $a^4 = (a^2)^2 = e^2 = e$, but $\text{ord}(a) = |\langle a \rangle| = |\{e, a\}| = 2$.

(c) $\langle 78 \rangle = \langle 42 \rangle$ in $\mathbb{Z}_{108}$.

Theorem 6.14

☒ True

☐ False

$$\left.\begin{array}{l} 108 = 2^2 \cdot 3^3 \\ 78 = 2 \cdot 3 \cdot 13 \\ 42 = 2 \cdot 3 \cdot 7 \end{array}\right\} \Rightarrow \left.\begin{array}{l} \gcd(108, 78) = 2 \cdot 3 = 6 \\ \gcd(108, 42) = 2 \cdot 3 = 6 \end{array}\right\} \xrightarrow[\text{Thm } 6.14]{} \langle 78 \rangle = \langle 42 \rangle = \langle 6 \rangle$$

(d) There exists a finite cyclic group with exactly 12 generators.

Cor 6.16

☒ True

☐ False

For p prime, $\mathbb{Z}_p$ has $p-1$ generators. $\therefore$ $\mathbb{Z}_{13}$ has 12 generators.

[can create other examples, e.g. $\mathbb{Z}_{21}$, $\mathbb{Z}_{26}$, $\mathbb{Z}_{28}$, etc.]

(e) The set $M_n(\mathbb{R})$ of all $n \times n$ matrices with real entries under matrix multiplication is a group.

ex. 4.12 p.40

☐ True

☒ False

The $n \times n$ zero matrix $O \in M_n(\mathbb{R})$ does not have a multiplicative inverse,

i.e. $\forall A \in M_n(\mathbb{R})$ $AO = OA = O \neq I_n$

(f) $\mathbb{Q}^+$ with the binary operation $a \star b := ab/3$ is a group.

variation on example 4.14 on p.40

☒ True

☐ False

closure: For $a, b \in \mathbb{Q}^+$ $a \star b = \frac{ab}{3} \in \mathbb{Q}^+$

$(\mathcal{G}_1)$ assoc: For $a, b, c \in \mathbb{Q}^+$, $(a \star b) \star c = abc/9$
$a \star (b \star c) = abc/9$

$(\mathcal{G}_2)$ identity: $3 \in \mathbb{Q}^+$ is an id. elt, since if $a \in \mathbb{Q}^+$ $a \star 3 = 3 \star a = a$

$(\mathcal{G}_3)$ inverses: For $a \in \mathbb{Q}^+$, $\frac{9}{a} \in \mathbb{Q}^+$ is the inverse elt. for a,

since $a \star \frac{9}{a} = \frac{9}{a} \star a = 3$

Thus $\langle \mathbb{Q}^+, \star \rangle$ is a group!

3. **(30 points)** Consider the group $\mathbb{Z}_{36}$.

i) • What is the order of its subgroup $\langle 24 \rangle$?

ii) • List the elements of $\langle 24 \rangle$.

iii) • Draw the subgroup diagram/lattice of $\mathbb{Z}_{36}$. *No justifications required.*

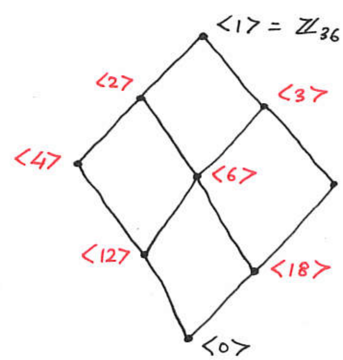
iv) • Generalize previous question to $\mathbb{Z}_{p^2q^2}$ for distinct primes p and q. *No justifications required.*

Note that $\left[\begin{array}{l} 36 = 2^2 \cdot 3^2 \\ 24 = 2^3 \cdot 3 \end{array}\right\} \longrightarrow \gcd(36, 24) = 2^2 \cdot 3 = 12$

Therefore by Theorem 6.14 we have $\left[\begin{array}{l} \boxed{|\langle 24 \rangle|} = \dfrac{36}{\gcd(36,24)} = \dfrac{36}{12} = \boxed{3} \quad \ldots \text{ i)} \\ \boxed{\langle 24 \rangle} = \langle 12 \rangle = \boxed{\{0, 12, 24\}} \quad \ldots \text{ ii)} \end{array}\right.$

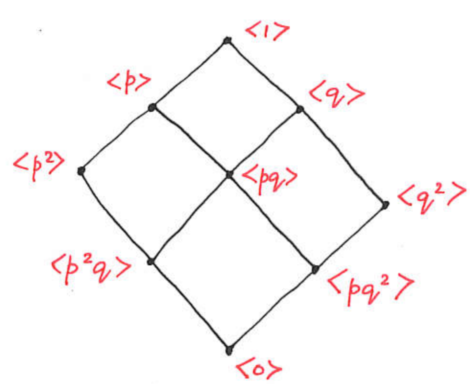
iii) The positive divisors of 36 are : 1, 2, 3, 4, 6, 9, 12, 18, 36

Thus the subgroup diagram for $\mathbb{Z}_{36}$ is :



iv) Similarly, the positive divisors of p^2q^2 are : $1, p, q, p^2, pq, q^2, p^2q, pq^2, p^2q^2$

Thus the subgroup diagram for $\mathbb{Z}_{p^2q^2}$ is :



4. **(2 × 15 = 30 points)** Prove **two** of the following results. Make your proof as precise as possible.

#4.35 (a) Let G be a group. Fix two elements a and b in G. Prove that $(ab)^2 = a^2b^2$ if and only if $ab = ba$.

#5.52 (b) Let G be a group, and $Z(G) := \{x \in G \mid xa = ax \text{ for every } a \in G\} \subseteq G$. Prove that $Z(G) \leq G$.

(c) Answer the following pair of questions:

#4.32 (i) Let G be a group with the property that every element in G is equal to its own inverse. Prove G is abelian.

In $\mathbb{Z}_6$, 1 and 5 are inverses of each other. (ii) Prove or disprove the converse: If a group is abelian, then every element is its own inverse.

(d) Recall that $\mathrm{GL}(2,\mathbb{R})$ is the group of 2×2 matrices with real entries that have non-zero determinant, with the operation of matrix multiplication. Define $\mathrm{SL}(2,\mathbb{R})$ to be the set of 2×2 matrices with real entries whose determinant is one. Show $\mathrm{SL}(2,\mathbb{R}) \leq \mathrm{GL}(2,\mathbb{R})$.

example 5.16 on p.53

4.(d) alternate proof using homomorphisms

Lemma [Given a homomorphism bt. groups $\phi: G \to G'$, then $\ker(\phi) \leq G$.] ... ⓐ

pf: left to you! $\ker(\phi) := \{x \in G \mid \phi(x) = e'\}$

Check that the map [$\det : GL(n,\mathbb{R}) \to \mathbb{R}^*$ is a homomorphism] ... ⓑ

Now use ⓐ and ⓑ to conclude that $SL(n,\mathbb{R}) \leq GL(n,\mathbb{R})$.

we will soon learn that kernels of homomorphisms are a special kind of subgroup called NORMAL subgroups!

we denote this as $SL(n,\mathbb{R}) \trianglelefteq GL(n,\mathbb{R})$.

5. **(30 points)** Prove **one** of the following results. Make your proof as precise as possible.

Theorem 6.6 → (a) Prove that every subgroup of a cyclic group is cyclic.

(b) Prove that the groups $\mathbb{C}^*$ and $\mathbb{R}^*$ (of all non-zero complex numbers and all non-zero real numbers, respectively, both under the operation of standard multiplication) are not isomorphic.

(c) Let G be a finite cyclic group of order n generated by $a \in G$, i.e. $G = \langle a \rangle$ and $|G| = n$. For any $s \in \mathbb{Z}^+$, prove that $\langle a^s \rangle = \langle a^{\gcd(n,\,s)} \rangle$.

(d) Let $\mathbb{R}^*$ be the group of non-zero real numbers under the operation of standard multiplication. For any subgroup $D \leq \mathbb{R}^*$, define $M(D) := \{A \in \mathrm{GL}(2,\mathbb{R}) \mid \det(A) \in D\}$. Prove that $M(D) \leq \mathrm{GL}(2,\mathbb{R})$.

5.(b) Study [example 3.16 on p.33] and [#3.31 on p.36]

5.(c) Theorem 6.14 in Fraleigh or my $\boxed{\text{Theorem 6.14 (a) Redux}}$ in handout

5.(d) Let $D \leq \mathbb{R}^*$. Recall $M(D) := \{A \in GL(2,\mathbb{R}) \mid \det(A) \in D\} \subseteq GL(2,\mathbb{R})$.

Closure Let $A, B \in M(D)$, and let $a := \det(A)$ and $b := \det(B)$.

Then $a, b \in D$ by def. of $M(D)$ and since $D \leq \mathbb{R}^*$ we have $ab \in D$.

Therefore $\det(AB) = \det(A)\det(B) = ab \in D$ and so $AB \in M(D)$.

Identity $I_2 \in GL(2,\mathbb{R})$ and $\det(I_2) = 1 \in D$ since $D \leq \mathbb{R}^*$ and must contain the id. elt of $\mathbb{R}^*$ (which is 1). Thus $I_2 \in M(D)$.

Closed under inverses Let $A \in M(D)$ and let $a := \det(A) \in D$.

Note that $a^{-1} = \frac{1}{a} \in D$ since $D \leq \mathbb{R}^*$ and closed under inverses.

Also notice that $\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{a} \in D$ and so $A^{-1} \in M(D)$.

Since we have checked that the criteria / hypotheses of Theorem 5.14 are satisfied, it follows that $M(D) \leq GL(n,\mathbb{R})$.