Exercises 5

14. (a) No. $f(x)=3$ & $g(x)=-3$ are both elements of $\tilde{F}$, but $(f+g)(x)=0$ so $f+g \notin \tilde{F}$. Thus $\tilde{F}$ is not closed.
(b) Yes. A gp is always a subgp of itself.

28. $\langle c \rangle = \{e, c\}$

29. $\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = \zeta_6^2$, where $\zeta_6 = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6}$.

$\langle \zeta_6^2 \rangle = \langle 1, \zeta_6^2, \zeta_6^4 \rangle = \langle 1, \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}, \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} \rangle$

46. Let G be a cyclic gp, & suppose $\exists\, a \in G$ s.t. $\langle a \rangle = G$. Then $\langle a^{-1} \rangle = G$ as well (this is because $\{a^n \mid n \in \mathbb{Z}\} = \{(a^{-1})^n \mid n \in \mathbb{Z}\}$. Since G has only one generator, $a = a^{-1}$, & so $a^2 = e$.
Thus $G = \langle a \rangle = \{e, a\}$, & G has 2 elements, if $a \neq e$, and one element if $a = e$.

47. Let $H = \{x \in G \mid x^2 = e\}$.
- H is closed: Let $x, y \in H$. Then we need to show $(xy)^2 = e$.
$(xy)^2 = xyxy = xxyy = x^2y^2 = e \cdot e = e$ ✓
because G is abelian.
- $e \in H$: $e^2 = e$ ✓
- Let $x \in H$. We need to show $(x^{-1})^2 = e$.
$(x^{-1})^2 = x^{-1}x^{-1} = (xx)^{-1} = (x^2)^{-1} = e^{-1} = e$ ✓

Therefore, $H \leq G$.

51. $H_a = \{x \in G \mid xa = ax\}$
- H_a is closed: Let $x, y \in H_a$.
Then $xya = xay$ $(y \in H_a)$
$= axy$ ✓ $(x \in H_a)$
- $e \in H_a$: $ea = a = ae$ ✓
- Let $x \in H_a$. Then $ax^{-1} = x^{-1}xax^{-1}$
$= x^{-1}axx^{-1}$
$= x^{-1}a$, so $x^{-1} \in H$ ✓

Therefore, $H_a \leq G$.

52. (a) $H_S = \{x \in G \mid xs = sx \ \forall s \in S\}$
(same pf as 51 works, just add $\forall a \in S$ to each line)
(b) Let $H_G = \{x \in G \mid xg = gx \ \forall g \in G\}$, & let $x, y \in H_G$.
Then $xy = yx$, because x commutes with every element of G, in particular x commutes with y.

53. • reflexive: let $a \in G$. Then $aa^{-1} = e \in H$, b/c H is a subgp. $\Rightarrow a \sim a$ ✓
• symmetric: let $a, b \in G$ s.t. $a \sim b$. Then $ab^{-1} \in H$, so $ba^{-1} = (ab^{-1})^{-1} \in H$, since H is a subgp $\Rightarrow b \sim a$. ✓
• transitive: let $a, b, c \in G$ s.t. $a \sim b$ & $b \sim c$. Then $ab^{-1} \in H$ & $bc^{-1} \in H$, so $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$, since H is a subgp $\Rightarrow a \sim c$. ✓

Therefore, $\sim$ is an equivalence relation.

57. Let G be a gp & suppose G has no non-trivial proper subgps.
If $G=\{e\}$, then $G=\langle e\rangle$, so G is cyclic.
If $G\neq\{e\}$, then $\exists g\in G$ s.t. $g\neq e$. Consider $\langle g\rangle\leq G$. Since $g\neq e$, $\langle g\rangle$ is not trivial. Since G has no proper subgps, $\langle g\rangle = G$. Thus G is cyclic.

Exercises 6:

33. D_4

34. $(\mathbb{R},+)$

35. $\mathbb{Z}_2$

36. No example exists: Let G be an infinite cyclic gp, with generator a. Suppose $b\in G$ generates G. Then $a=b^k$ for some $k\in\mathbb{Z}$, & $b=a^m$ for some $m\in\mathbb{Z}$. Thus $a=b^k=(a^m)^k=a^{mk}$, and so $mk=1$.
The only pairs of integers satisfying $mk=1$ are $m=1$ & $k=1$, or $m=-1$ & $k=-1$.
Therefore $b=a$ or $b=-a$ (plugging in $m=\pm1$ to $b=a^m$), so an infinite cyclic gp can have at most 2 generators.

37. $\mathbb{Z}_{10}=\langle 1\rangle=\langle 3\rangle=\langle 7\rangle=\langle 9\rangle$, because 1,3,7,9 are exactly the elements of $\mathbb{Z}_{10}$ that are relatively prime to 10.

49. The klein 4 group (V) is not cyclic, but every proper subgp is. (you can check by checking $\langle g\rangle\neq V$ for any of the 4 elements $g\in V$; we did this in class.)

50. $\langle a\rangle=\{e,a\}$, & $\langle x\rangle\neq\{e,x\}$ for all $x\in G$ with $x\neq a$.

Consider the element xax^{-1}.
Then
$$\begin{aligned}(xax^{-1})^2 &= xax^{-1}xax^{-1}\\ &= xaax^{-1}\\ &= xa^2x^{-1}\\ &= xex^{-1}\\ &= xx^{-1}\\ &= e.\end{aligned}$$
Therefore, $\langle xax^{-1}\rangle=\{e,xax^{-1}\}$, & so $xax^{-1}=a$, by assumption. But then $xa=ax$, as desired. ■

55. $\mathbb{Z}_p$ is a cyclic group, & so all subgroups are cyclic. Let $1\leq i<p$. then $\langle i\rangle=\mathbb{Z}_p$, because $\gcd(i,p)=1$, as p is prime. Also, $\langle 0\rangle=\{0\}$. Therefore, all subgps of $\mathbb{Z}_p$ are improper or trivial.

Additional exercises:

1. The order of such a gp must be prime: Let $|G|=n$. Since G is cyclic, it is a thm in the reading that for every $d\in\mathbb{Z}^+$ s.t. $d\mid n$, there is a subgp $H\leq G$ with $|H|=d$. Since every subgp of G is either proper or trivial, the only factors of n are 1 & n. Thus n is prime.

2. (a) $L = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix} \middle| \, a,b,c \in \mathbb{R} \right\}$

- Closure: $\begin{pmatrix} 1 & 0 & 0 \\ a_1 & 1 & 0 \\ b_1 & c_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ a_2 & 1 & 0 \\ b_2 & c_2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ a_1+a_2 & 1 & 0 \\ b_1+c_1a_2+b_2 & c_1+c_2 & 1 \end{pmatrix} \in L$ ✓
- The identity matrix $I \in L$ ✓
- The inverse of $\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix}$ is $\begin{pmatrix} 1 & 0 & 0 \\ -a & 1 & 0 \\ ca-b & -c & 0 \end{pmatrix} \in L$ ✓

(b) All cyclic groups are abelian, so I will find 2 cyclic subgps of L. The easiest way to show they are not isomorphic is to find 2 subgps of different cardinalities.

There are lots of choices!

<u>Ex</u>:

- $\left\langle \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ n & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, n \in \mathbb{Z} \right\}$ is countable (and infinite)
- $\left\langle \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\rangle$ has order 2
- $\left\langle \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle$ has order 3

A non-cyclic example:

$\left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & c & c \end{pmatrix} \middle| \, a,b,c \in \mathbb{R}^* \right\}$ is a subgp, uncountable, & abelian.

3.

$$\begin{tikzcd}
 & & D_4 \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] & & \\
\{e,\tau,\rho^2\tau,\rho^2\} \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \langle \rho \rangle \arrow[d, dash] & & \{e,\rho\tau,\rho^3\tau,\rho^2\} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \\
\langle \tau \rangle \arrow[drr, dash] & \langle \rho^2\tau \rangle \arrow[dr, dash] & \langle \rho^2 \rangle \arrow[d, dash] & \langle \rho\tau \rangle \arrow[dl, dash] & \langle \rho^3\tau \rangle \arrow[dll, dash] \\
 & & \langle e \rangle & &
\end{tikzcd}$$

4. (a) Let $\frac{a}{b} \in \mathbb{Q}^+$, & let $a = p_1 \cdots p_k$, $b = p_1' \cdots p_{k'}'$ be the prime factorizations of a & b.

Then
$$\frac{a}{b} = \frac{p_1 \cdots p_k}{p_1' \cdots p_{k'}'} = \frac{1}{p_1'} \cdot \cdots \cdot \frac{1}{p_{k'}'} \cdot p_1 \cdots p_k$$
$$= \left(\frac{1}{p_1'}\right) \cdot \cdots \cdot \left(\frac{1}{p_{k'}'}\right) \cdot \left(\frac{1}{p_1}\right)^{-1} \cdot \cdots \cdot \left(\frac{1}{p_k}\right)^{-1}$$

Since each $\frac{1}{p_i}, \frac{1}{p_i'} \in S = \{\frac{1}{p} \mid p \text{ prime}\}$, we have shown that $\frac{a}{b} \in \langle S \rangle$. Since $\frac{a}{b} \in \mathbb{Q}^+$ was arbitrary, $\mathbb{Q}^+ = \langle S \rangle$.

* Note: When we say a gp G is generated by a set S, this means (by definition) that every elt in G can be written as a product of powers of elts in S <u>and</u> their inverses.

(b) Suppose a set $S = \{\frac{a_1}{b_1}, \ldots, \frac{a_m}{b_m}\}$ generates $\mathbb{Q}^+$. Then there are only finitely many primes $p_1, \ldots, p_k$ that appear in the prime factorizations of any a_i or b_i. Let $q \in \mathbb{Z}$ be a prime larger than any p_i. Since $q \in \mathbb{Q}^+$, q can be written as a product of elts of S & their inverses. Thus q can be expressed as a product of primes (none of which are $= q$), which contradicts the fact that q is prime. Therefore S does not generate $\mathbb{Q}^+$. Since S was an arbitrary finite set, $\mathbb{Q}^+$ cannot be generated by any finite set.