Exercises on chapter 1

1. Let $G$ be a group and $H$ and $K$ be subgroups. Let $HK = \{hk \mid h \in H, k \in K\}$.
   (i) Prove that $HK$ is a subgroup of $G$ if and only if $HK = KH$.
   (ii) If either $H$ or $K$ is a normal subgroup of $G$ prove that $HK$ is a subgroup of $G$. If both $H$ and $K$ are normal subgroups of $G$, prove that $HK$ is a normal subgroup of $G$.
   (iii) Prove that $[H : H \cap K] \leq [G : K]$. (Note this makes sense even for infinite groups if we define the index $[G : K]$ to be the number of left cosets of $K$ in $G$, or $\infty$ if there are infinitely many). Moreover, if $[G : K]$ is finite, then $[H : H \cap K] = [G : K]$ if and only if $G = HK$.
   (iv) If $H, K$ are of finite index such that $[G : H]$ and $[G : K]$ are relatively prime, then $G = HK$.

2. Recall that a partially ordered set $X$ is called a complete lattice if every non-empty subset of $X$ has both a least upper bound and a greatest lower bound in $X$. Prove that the set of all normal subgroups of a group $G$ partially ordered by inclusion forms a complete lattice.

3. Let $N$ be a normal subgroup of index 2 in a finite group $G$. For example, $N = A_n$, $G = S_n$ for $n \geq 2$.
   (i) Let $X$ be a $G$-set and $x \in X$. Prove that $G \cdot x = N \cdot x$ if $G_x \not\leq N$; otherwise the $G$-orbit $G \cdot x$ splits into two $N$-orbits of the same size.
   (ii) Compute the number of conjugacy classes in the alternating group $A_6$ together with their orders.

4. Prove that any infinite group has infinitely many subgroups.

5. Compute the group $\text{Aut}(C_8)$ of automorphisms of the cyclic group $C_8$ of order 8. Is it cyclic?

6. Let $G$ be a finite group, $H \trianglelefteq G$ and $N \trianglelefteq H$.
   (i) Give a counterexample to show that it is not necessarily the case that $N \trianglelefteq G$.
   (ii) If $([N], [H : N]) = 1$, prove that $N$ is the unique subgroup of $H$ having order $|N|$. Deduce that $N \trianglelefteq G$.
   (iii) Show that $A_4$ has a unique subgroup of order 4 and that this is a normal subgroup of $S_4$.

7. A group $G$ is called metabelian if there exists a normal subgroup $N$ of $G$ with $N$ and $G/N$ both abelian. Prove that every subgroup and every quotient of a metabelian group is metabelian.

8. This is a question about the dihedral group $D_n$ of order $2n$. Recall this is the subgroup of $O(2)$ generated by two elements, $g$ of order $n$ (counterclockwise rotation through angle $2\pi/n$) and $h$ (reflection in the $x$-axis) of order 2, subject to the one relation that $hg = g^{-1}h$.
   (i) For which $n$ is the center $Z(D_n)$ trivial?
   (ii) For which $n$ do the involutions (= elements of order 2) in $D_n$ form a single conjugacy class?
(iii) Prove that the subgroup of all upper unitriangular $3 \times 3$ matrices with entries in the field $\mathbb{F}_2$ of two elements is isomorphic to $D_4$.

(iv) Is $D_6 \cong S_3 \times C_2$?

9. Suppose that $G$ is an abelian group and $g, h \in G$ are elements of orders $n = |g|$ and $k = |h|$ respectively. If $n$ and $k$ are relatively prime, i.e. their greatest common divisor $(n, k)$ is 1, show that $|gh| = nk$.

(ii) Let $G$ be a finite group of order $n$. If $G$ is cyclic prove that $G$ has a unique subgroup of order $d$ for each divisor $d$ of $n$, and moreover this subgroup is cyclic. Conversely, if $G$ has at most one cyclic subgroup of order $d$ for each divisor $d$ of $n$, prove that $G$ is cyclic.

(iii) Explain why the equation $x^n = 1$ has at most $n$ solutions in a field $K$.

(iv) Now let $G$ be a finite subgroup of the group $K^\times$ of units of some field $K$. Prove that $G$ is cyclic.

10. A commutator in a group $G$ is an element of the form $[g, h] = ghg^{-1}h^{-1}$ for $g, h \in G$. Prove that $G'$ is the smallest normal subgroup of $G$ such that $G/G'$ is abelian.

(ii) Explain how to define a functor (“abelianization”) from the category groups to the category ab so that an object $G$ maps to $G^{ab} := G/G'$.

(iii) Let $G$ be a group and $H$ be an abelian group. Show that the sets $\text{Hom}_{\text{groups}}(G, H)$ and $\text{Hom}_{\text{ab}}(G^{ab}, H)$ have the same size.

(iv) Compute $G^{ab}$ for each of the groups $G = S_n (n \geq 1)$, $A_n (n \geq 2)$, $C_n (n \geq 1)$ and $D_n (n \geq 1)$.

11. Recall that the direct product $H \times K$ of two groups is just the Cartesian product with coordinatewise multiplication. It is sometimes called the “external” direct product since we have built a completely new group out of the two groups we started with. This is different from the notion of an “internal” direct product. A group $G$ is said to be the internal direct product of $H$ and $K$ if $H$ and $K$ are subgroups of $G$ and the map $H \times K \to G,(h,k) \mapsto hk$ is an isomorphism.

(i) Prove that $G$ is the internal direct product of $H$ and $K$ if and only if $H \leq G$, $K \leq G$, $G = HK$ and $H \cap K = \{1\}$.

(ii) For which $n$ is the dihedral group $D_n$ an internal direct product of two proper subgroups?

12. Suppose that $K$ is a finite field with $q$ elements.

(i) Explain why $|GL_n(K)|$ is equal to the number of distinct ordered bases $(v_1, \ldots, v_n)$ for the vector space $K^n$. Hence compute $|GL_n(K)|$ and $|SL_n(K)|$.

(ii) Suppose for the remainder of the question that $V$ is a $2n$-dimensional vector space over $K$ equipped with a non-degenerate skew-symmetric bilinear form. Explain why there are $\frac{(q^{2n} - 1)(q^{2n} - q^{2n-1})}{(q^2 - q)}$ different non-degenerate 2-dimensional subspaces of $V$.

(iii) Recall that $Sp(V) \cong Sp_{2n}(K)$ is the group of all linear maps from $V$ to $V$ preserving the given non-degenerate skew-symmetric form. Prove that the stabilizer in $Sp(V)$ of a non-degenerate 2-dimensional subspace is isomorphic to $Sp_{2n-2}(K) \times Sp_2(K)$. Hence deduce that $|Sp_{2n}(K)| = q^{n^2}(q^{2n} - 1)(q^{2n-2} - 1) \cdots (q^2 - 1)$.

(iv) How many different non-degenerate skew-symmetric bilinear forms are there on the vector space $V$?

13. Prove that there is no simple group of order 120.
14. Suppose that $G$ is a group of order $p^3q$ for distinct primes $p, q$ and that $G$ has no normal Sylow subgroups. Compute $|G|$. Give an example of such a group.

15. Let $p, q, r$ be distinct primes. Prove that there are no simple groups of order $pqr$.

16. Suppose that $G$ is a non-abelian simple group with $|G| < 200$. Prove that $|G| = 60$ or $|G| = 168$. To make life easier – though you can solve this without it – you may assume without proof the following consequence of Burnside’s $p^aq^b$ theorem which we will discuss later in the course: there is no simple group of order $p^aq^b$ for $p, q$ distinct primes.

17. Suppose that $G$ is a simple group of order 60. Prove that $G \cong A_5$.

18. Recall a permutation group $G$ acting on a set $X$ is transitive if for each $x, y \in X$ there exists $g \in G$ with $gx = y$. Instead, $G$ is called 2-transitive if for each $x_1 \neq x_2$ and $y_1 \neq y_2$ from $X$ there exists $g \in G$ with $gx_1 = y_1, gx_2 = y_2$.
   (i) Show that $A_n$ is a 2-transitive permutation group on $\{1, \ldots, n\}$ for $n \geq 4$.
   (ii) If $G$ is a 2-transitive permutation group on $X$ and $1 < K \leq G$, prove that $K$ is transitive on $X$.

19. The goal of this problem is to prove that the group $G = GL_3(\mathbb{F}_2)$ of $3 \times 3$ invertible matrices over the field with two elements is a simple group.
   (i) What is the order $|G|$?
   (ii) Let $V = (\mathbb{F}_2)^3$ be the vector space that $G$ acts on naturally. Prove that $G$ acts 2-transitively on $V - \{0\}$.
   (iii) Hence by question 18 if $1 < K \leq G$ then $K$ is transitive on $V - \{0\}$. Deduce that $7||K|$. (iv) Now let $n_7$ denote the number of Sylow 7-subgroups of $K$, so $n_7 = 1$ or $n_7 = 8$. If $n_7 = 8$ and $K \neq G$ prove that $K$ has a unique Sylow 2-subgroup. Why does this imply that $G$ itself has a unique Sylow 2-subgroup too? Obtain a contradiction by exhibiting more than one Sylow 2-subgroup in $G$ explicitly.
   (v) If $n_7 = 1$ then $G$ has just 6 elements of order 7. Obtain a contradiction. Hence $G$ is simple.

20. For any field $k$, prove that $GL_n(k)$ is a semidirect product of $SL_n(k)$ by $k^\times$.

21. Let $G$ be the subgroup of $GL_2(\mathbb{C})$ generated by the matrices
   \[
   \begin{pmatrix}
   \omega & 0 \\
   0 & \omega^2
   \end{pmatrix}, \quad \begin{pmatrix}
   0 & i \\
   i & 0
   \end{pmatrix}
   \]
   where $\omega = e^{2\pi i/3}$ is a primitive cube root of unity. Prove that $G$ is a group of order 12 that is not isomorphic to $A_4$ or $D_6$.

22. Recall that the quaternions $\mathbb{H}$ are defined to be the real vector space of dimension 4 with basis $1, i, j, k$ with associative, bilinear multiplication (making it into a ring or more precisely an $\mathbb{R}$-algebra with identity element 1) defined on the basis elements by $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i$ and $ki = j$.
   (i) Prove that every non-zero quaternion is a unit with inverse
   \[\frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk)\]
   Hence $\mathbb{H}$ is a division algebra (a non-commutative field).
   (ii) Define the norm $N : \mathbb{H}^\times \to \mathbb{R}^+$ by $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$. Check that this is a group homomorphism and moreover every $h \in \mathbb{H}^\times$ has a polar decomposition $h = rs$ where $r \in \mathbb{R}^+$ and $s \in \ker N$ (which is the sphere $S^3$).
(iii) Let $A$ be the set of all matrices of the form \[
\begin{pmatrix}
z & w \\
-\bar{w} & \bar{z}
\end{pmatrix}
\] where $z$ and $w$ are complex numbers and $z \mapsto \bar{z}$ denotes complex conjugation. Prove that $A$ is a subring of the ring $M_2(\mathbb{C})$ of $2 \times 2$ complex matrices and that $A \cong \mathbb{H}$.

(iv) Using your answer to (iii), prove that the normal subgroup $\ker N$ of $\mathbb{H}^\times$ is isomorphic to the group $SU(2)$ – the special unitary group consisting of all $2 \times 2$ complex matrices \[
\begin{pmatrix}
p & q \\
r & s
\end{pmatrix}
\] of determinant 1 such that $pq + rs = 0$ and $pr + qs = 1 = q\bar{q} + s\bar{s}$.

(v) Deduce that $\mathbb{H}^\times = SU(2) \rtimes \mathbb{R}^+$.

23. Recall that the quaternion group $Q_4$ is the subgroup $\{\pm 1, \pm i, \pm j, \pm k\}$ of $\mathbb{H}^\times$.

(i) Prove that $Q_3$ is isomorphic to the group $\langle x, y \mid x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle$.

(ii) Prove that $Q_3$ is not isomorphic to the semidirect product $C_4 \rtimes C_2$ of a cyclic group of order 4 by a cyclic group of order 2. Deduce that $Q_3 \not\cong D_4$.

24. Let $G$ be a finite group, $N \leq G$ and $P$ be a Sylow $p$-subgroup of $G$ for some prime $p$. Prove that $PN/N$ is a Sylow $p$-subgroup of $G/N$ and $P \cap N$ is a Sylow $p$-subgroup of $N$.

25. Prove that all of the following groups are abelian:

(i) A group $G$ all of whose elements are of order 1 or 2.

(ii) A group $G$ with $|\text{Aut}(G)| = 1$.

(iii) A group $G$ of order $p^2$ ($p$ prime).

26. Let $p$ be a prime. How many subgroups does the group $C_p \times C_p$ have? (Don’t forget the trivial ones!)

27. How many different groups of order 18 are there up to isomorphism? (There are only two groups of order 9, namely, $C_9$ and $C_3 \times C_3$.)

28. We will prove in class that $PSL_2(\mathbb{F}_5)$, the quotient of the special linear group $SL_n(\mathbb{F}_5)$ by its center $\{\pm I_2\}$, is a simple group of order 60. Hence it is isomorphic to the group $A_5$. Prove that $SL_2(\mathbb{F}_5)$ is a non-split extension of $C_2$ by $A_5$.

29. Suppose that $G$ and $H$ are finite groups with $|G|, |H| = 1$. Is it true that every subgroup of $G \times H$ is of the form $G' \times H'$ for $G' \leq G$ and $H' \leq H$?

30. Let $1 < m < n - 1$, and $G$ be the symmetric group $S_n$ acting on the set $X$ of $m$-element subsets of $\{1, \ldots, n\}$.

(i) Show that $G$ is not 2-transitive on $X$.

(ii) What is the stabilizer of a point?

(iii) Using your answer to (ii) determine for which $m$ the action of $G$ on $X$ is primitive.

31. This exercise is concerned with a useful counterexample! Let $p$ be a prime and define the group $C_{p^\infty}$ to be the subgroup of $\mathbb{C}^\times$ consisting of all $p^n$-th roots of 1 for all $n \geq 0$. Note that $C_{p^\infty}$ is an example of an infinite $p$-group: all its elements are of order a power of $p$.

(i) Let $C_p$ denote the subgroup of $C_{p^\infty}$ consisting of all $p$-th roots of 1. By considering the map $z \mapsto z^p$, prove that $C_{p^\infty}/C_p \cong C_{p^\infty}$.

(ii) Prove that every finitely generated subgroup of $C_{p^\infty}$ is cyclic, but $C_{p^\infty}$ is not cyclic itself.

(iii) (An alternative definition.) By considering the map $q \mapsto e^{2\pi i q}$, prove that $C_{p^\infty}$ is isomorphic to the subgroup $\{[\frac{\alpha}{p^n}] \mid \alpha \in \mathbb{Z}, n \geq 0\}$ of the quotient group $\mathbb{Q}/\mathbb{Z}$ (rational numbers modulo 1).
32. Determine which of the following groups are solvable and/or nilpotent.
   (i) The alternating groups $A_n$ for $n \geq 3$.
   (ii) The symmetric groups $S_n$ for $n \geq 2$.
   (iii) The dihedral groups $D_n$ for $n \geq 4$. (Hint: what is the center of $D_n$?)
   (iv) The group of upper unitriangular $n \times n$ matrices over a field $F$.
   (v) The group of invertible upper triangular $n \times n$ matrices over a field $F$.
   (vi) A group of order $pq$ where $p \neq q$ are primes.

33. True or false? If true give a proof, if false give a counterexample...
   (i) If $G$ is a finite nilpotent group, and $m$ is a positive integer dividing $|G|$, then there exists a subgroup of $G$ of order $m$.
   (ii) If $N$ is a normal subgroup of $G$ and $N$ and $G/N$ are nilpotent, then $G$ is nilpotent.
   (iii) $S_4/V_4 \cong S_3$.
   (iv) Let $G$ be a finite group. Then $G$ is nilpotent if and only if $N_G(H) \geq H$ whenever $H \leq G$.
   (v) The group $(\mathbb{Q}, +)$ has a proper subgroup of finite index.

34. Let $G$ be a finite group.
   (i) Prove that if $G$ is solvable, then $G$ contains a non-trivial normal abelian subgroup.
   (ii) Prove that if $G$ is not solvable then it contains a normal subgroup $H$ such that $H' = H$.

35. Compute the order of the group $\langle a, b, c, d \mid bab^{-1} = a^2, bdb^{-1} = d^2, c^{-1}ac = b^2, dcd^{-1} = c^2, bd = db \rangle$.

36. Suppose that $X$ is a subset of $Y$. Let $F(X)$ be the free group on $X$ and $F(Y)$ be the free group on $Y$. Using universal properties, prove that the inclusion $X \hookrightarrow Y$ induces an injective homomorphism $F(X) \hookrightarrow F(Y)$.

37. Prove that the group with presentation $\langle a, b \mid a^6 = 1, b^2 = a^3 = (ab)^2 \rangle$ is of order 12.

38. The goal of this problem is to derive a presentation for the symmetric group $S_n$. Let $G_n$ be the group with generators $\{s_1, s_2, \ldots, s_{n-1}\}$ subject to the relations $s_i^2 = 1, s_is_j = s_js_i$ for $|i - j| > 1$ and $s_is_{i+1}s_i = s_{i+1}s_is_{i+1}$. Let $S_n$ denote the symmetric group, and $t_i$ denote the basic transposition $(i \ i + 1)$ in $S_n$.
   (i) Prove that the $t_i$ satisfy the same relations as the $s_i$.
   (ii) Embed $S_{n-1}$ into $S_n$ as the subgroup consisting of all permutations fixing $n$. Prove that $\{1, t_{n-1}, t_{n-2}t_{n-1}, \ldots, t_1t_2\ldots t_{n-1}\}$ is a set of $S_n/S_{n-1}$-coset representatives.
   (iii) By considering the subgroup $G_{n-1}$ of $G_n$ generated by $s_1, \ldots, s_{n-2}$ only and using induction, prove that $G_n \cong S_n$.

39. Let $G$ and $H$ be groups. Suppose that $G$ has the presentation $G = \langle X \mid R \rangle$ and $H$ has the presentation $H = \langle Y \mid S \rangle$. (Why does any group have at least one presentation?) The free product $G \ast H$ is the group with generators $X \sqcup Y$ (disjoint union) subject to the relations $R \sqcup S$.
   (i) There are obvious maps $G \to G \ast H$ and $H \to G \ast H$. Construct them.
   (ii) Prove that $G \ast H$ together with these maps is a coproduct of $G$ and $H$ in the category of groups.
   (iii) Deduce that the group $G \ast H$ is independent of the presentations of $G$ and $H$ chosen (up to canonical isomorphism).
(iv) Consider the matrices
\[ A = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} \quad B = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \]
in $GL_2(\mathbb{C})$. Prove that $A^2 = B^2 = 1$ but that $AB$ has infinite order.

(v) Deduce that the subgroup of $GL_2(\mathbb{C})$ generated by the matrices $A$ and $B$ is isomorphic to the free product $C_2 * C_2$.

40. Since I know you love the word “unitriangular”. Let $q$ be a power of a prime $p$.

(i) Prove that the upper unitriangular matrices are a Sylow $p$-subgroup of the group $GL_n(\mathbb{F}_q)$.

(ii) How many different Sylow $p$-subgroups are there in $GL_n(\mathbb{F}_q)$?