Math 451, 01, Exam #2
Answer Key

1. (25 points): If the statement is always true, circle "True" and prove it. If the statement is never true, circle "False" and prove that it can never be true. If the statement is true in some cases and false in others, circle "Possible" and give an example and a counter-example.

(a) Let G be an abelian group of order 16.
TRUE / POSSIBLE / [✓ **FALSE**]: The class equation of G is:

$$16 = 1+1+1+1+1+1+1+1+2+2+4$$

Since in an abelian group, $xy = yx$. This means that $yxy^{-1} = x$ for all y so that conjugacy classes are singleton sets. So the class equation for an abelian group is $1 + 1 + \cdots + 1$ (all ones).

(b) Let G be a non-abelian group of order 14.
[✓ **TRUE**] / POSSIBLE / FALSE: The class equation of G is:

$$14 = 1+2+2+2+7$$

As will be proved in a later problem, the only groups of order $2p$ (up to isomorphism) where p is prime are $\mathbb{Z}_{2p}$ (cyclic – thus abelian) and D_p (dihedral).

So $G \cong D_7 = \langle x, y \,|\, x^7 = 1, y^2 = 1, (xy)^2 = 1\rangle$ which has the above class equation.

In fact, for p an odd prime (or any odd number), the class equation of D_p is:

$$2p = 1 + 2 + \cdots + 2 + p$$

(c) Let G be a non-abelian simple group.
TRUE / POSSIBLE / [✓ **FALSE**]: G has a subgroup of index 4.

Quick answer: G has no subgroup of index 4 because if it did, G would act non-trivially on this subgroup's left cosets. Non-abelian simple groups cannot act non-trivially on a set of size ≤ 4 (homework problem).

Long answer: Let G be a non-abelian simple group and suppose that H is a subgroup of index 4. Then G acts on the left cosets of H (non-trivially). This actions gives a corresponding homomorphism $\varphi : G \to S_4$. The kernel of φ is a normal subgroup of G and since the action is not trivial and G is simple, we must have that the kernel is trivial. Therefore, G is isomorphic to a subgroup of S_4. But we know that subgroups of S_n are either "all even" or "half and half". The isomorphic copy of G in S_4 can't be half even, half odd since this would give a subgroup of index 2 (thus a proper non-trivial normal subgroup) contradicting the fact that this subgroup is simple. Thus we have that G must be isomorphic to a subgroup of A_4 (which has order 12). But there are no non-abelian simple groups of order ≤ 12. Thus this is impossible.

(d) Let $G = \langle x, y \,|\, R\rangle$ where R is a set of 3 relations.
TRUE / [✓ **POSSIBLE**] / FALSE: G is finite.

$G = \langle x, y \,|\, x, y, xy^{-1}\rangle$ is the trivial group (which happens to be finite). [Why? The first two relations say $x = 1$ and $y = 1$. The third relation is overkill – saying – $x = y$.]

$G = \langle x, y \,|\, xyx^{-1}y^{-1}, y, y^2\rangle$ is infinite cyclic. [Why? The first relation says that $xy = yx$. The second relation says $y = 1$. Again, the third relation is redundant.]

(e) $\boxed{\textbf{TRUE}}$ / POSSIBLE / FALSE: $\mathrm{PSL}_2(\mathbb{F}_9)$ has at least 24 elements of order 5.

The order of $G = \mathrm{PSL}_2(\mathbb{F}_9)$ is $(1/2)8(9)10 = 2^3 3^2 5$. Let the number of Sylow 5-subgroups in G be s. Then by Sylow's third theorem, we know that s divides $2^3 3^2$ and is congruent to 1 modulo 5. The divisors of $2^3 3^2 = 72$ are: 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72. Out of this list, only 1, 6, and 36 are congruent to 1 modulo 5. We know that G is simple, so 1 is impossible (else our subgroup would be normal). So we are left with the options 6 and 36. Since subgroups of order 5 can only intersect trivially (5 is prime), we get 4 new elements of order 5 from each such subgroup. Thus there are at least $4(6) = 24$ elements of order 5.

Note: Consider the case $s = 6$. Then if H is a Sylow 5-subgroup, we have that $N_G(H)$ (the normalizer of H in G) has index 6. This implies (by part (d) above) that G is isomorphic to a subgroup of A_6. But A_6 has order $6!/2 = 360$ (which is the order of G). So that $G \cong A_6$. The elements of order 5 in A_6 are precisely the 5 cycles. Therefore, A_6 has $\binom{6}{5} \cdot (5-1)! = 144$ elements of order 5 (contradicting the choice $s = 6$). Therefore, $s = 36$ and thus there are (exactly) $36(4) = 144$ elements of order 5 in G.

2. (20 points): Let p be a prime and k a positive integer.

(a) Show that a group of order p^k has a non-trivial center. Then explain why a group of order p^k is simple if and only if $k = 1$.

Let G be a group of order p^k. The class equation of G is $p^k = 1 + \sum_i k_i$ (where each k_i divides p^k and the "1" comes from the conjugacy class of the identity element).

Now suppose that G has a trivial center. We know that the center of a group is equal to the union of all of the singleton conjugacy classes. Therefore, since the center is trivial, we must have that $k_i > 1$. But the k_i's divide p^k. Thus $k_i = p^{m_i}$ for some $m_i > 0$. Now reduce the class equation modulo p and get $0 \equiv p^k = 1 + \sum_i k_i \equiv 1$ modulo p (contradiction). Therefore, $Z(G)$ is non-trivial.

Now we consider the simplicity of G. Since $Z(G)$ is non-trivial. We have a non-trivial normal subgroup. If $Z(G)$ is proper, then G is not simple. So consider the case when $Z(G) = G$ — that is — G is abelian. Take any $g \in G$, $g \neq 1$. Then $|g| = p^\ell$ some $\ell > 0$. This implies that $x = g^{p^{\ell-1}}$ is an element of order p. Recall that G is abelian so that every subgroup is normal. Thus $\langle x \rangle$ is a normal subgroup of order p. Thus if G is to be simple we must have $G = \langle x \rangle$. Finally, any group of prime order is cyclic and simple.

To sum up, a group of order p^k is simple if and only if $k = 1$ in which case it is cyclic.

(b) Show that groups of order p^2 are abelian. Then classify the groups of order p^2.

Let G be a group of order p^2 and suppose that G is not abelian. We know (by part (a)) that $Z(G)$ is non-trivial. Thus since $G \neq Z(G)$, we must have that $|Z(G)| = p$. Consider $x \in G$ such that $x \notin Z(G)$. Notice that the centralizer of x contains x itself as well as the whole center. That is $Z(G) \cup \{x\} \subset Z(x) = \{g \in G \,|\, xg = gx\}$. Thus $|Z(x)| > p$ so its order must be p^2 (since it is a subgroup thus its order divides the order of G). But then $Z(x) = G$ which implies that everything in G commutes with x so that $x \in Z(G)$ (contradiction). Therefore, G is abelian.

Now that we know G is abelian, consider the following two cases:

- G has an element of order p^2. Therefore, G is cyclic.

- G has no elements of order p^2. So every non-identity element has order p. Let x be some element of order p. The order of $H = \langle x \rangle$ is p. Let $y \in G - H$ (y in G but not in H). Since H has order p, $|G - H| = p^2 - p > 0$ so such a y exists. Also, the identity is in H so that y has order p. Let $K = \langle y \rangle$. Notice that if $g \in H \cap K$ then $g = x^i = y^j$ some $0 \leq i, j < p$. If $i > 0$, then the g.c.d. of i and p is 1. Thus there exists a, b such that $ai + bp = 1$ so that $g^a = x^{ai} = x^{ai+bp} = x \in H \cap K$. Thus $H \subset H \cap K$ and so $H = K$ (contradicting the fact that y is not in H). So $i = 0$ and similarly $j = 0$. Thus $H \cap K = \{1\}$ which gives us that $|HK| = |H \times K| = p^2$ so that $G = HK$. Notice since G is abelian, both H and K are normal in G. Putting all this together we get that $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Thus G is either cyclic of order p^2 or the direct product of two cyclic groups of order p.

3. (20 points): Classify.

(a) Classify the groups of order $2p$ where p is an odd prime.

Note: We all ready took care of $p = 2$ in the previous problem.

Let G be a group of order $2p$ and let s_i be the number of Sylow i-subgroups of G ($i = 2$ and p). Then by Sylow's third theorem, s_2 must divide p (thus it must be 1 or p) and s_p must divide 2 and be congruent to 1 modulo p (thus $s_p = 1$).

Let H be the Sylow p-subgroup and let K be a Sylow 2-subgroup. H and K are cyclic (since they're of prime order). Let $H = \langle x \rangle$ and let $K = \langle y \rangle$. Notice that $H \cap K = \{1\}$ since the order $H \cap K$ must divide both p and 2 (so its order is 1). This implies that $|HK| = |H \times K| = 2p$. Therefore, $G = HK$ (G is generated by $\{x, y\}$). Finally, notice that since $s_p = 1$, we have that H is a normal subgroup of G.

Since H is normal, $yxy^{-1} \in H = \langle x \rangle$. Thus $yxy^{-1} = x^i$ for some $0 < i < p$ (if $i = 0$, then we would have that $x = 1$). Recall that $y^2 = 1$, so that $x = y^2xy^{-2} = yx^iy^{-1} = x^{i^2}$. Now the order of x is p, therefore, $i^2 \equiv 1 \bmod p$. That is — p divides $i^2 - 1 = (i-1)(i+1)$. By Euclid's lemma, p divides either $i - 1$ or $i + 1$.

- Case: p divides $i - 1$. In this case, notice that $i - 1 < p$, so we must have that $i - 1 = 0$ (i.e. $i = 1$). Thus $yxy^{-1} = x$ so that $xy = yx$. Thus G is abelian and so K is normal (i.e. $s_2 = 1$). It then follows that $G = HK \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$ (the last isomorphism is due to the fact that 2 and p are relatively prime).
- Case: p divides $i + 1$. In this case, $1 < i + 1 \leq p$. Therefore, $i + 1 = p$ (i.e. $i = p - 1$). This means that $yxy^{-1} = x^{p-1} = x^{-1}$. Therefore, $(xy)^2 = 1$ so that $G = \langle x, y \,|\, x^p = 1, y^2 = 1, (xy)^2 = 1 \rangle \cong D_{2p}$.

Thus G is either cyclic or dihedral.

(b) Classify the groups of order 99.

Let G be a group of order $99 = 3^2 \cdot 11$ and let s_i be the number of Sylow i-subgroups of G.

We know that s_3 divides 11 and is congruent to 1 modulo 3. Since 11 is not congruent to 1 modulo 3, we must have that $s_3 = 1$. Let H be the Sylow 3-subgroup (since $s_3 = 1$, H is normal).

Next, we know that s_{11} divides 9 and is congruent to 1 modulo 11. Since 3 and 9 are not congruent to 1 modulo 11, we must have that $s_{11} = 1$. Let K be the Sylow 11-subgroup (since $s_{11} = 1$, K is normal).

Note that $H \cap K = \{1\}$ since the orders of H and K are relatively prime. Thus $|HK| = |H \times K| = 99$ Keeping in mind that both H and K are normal, we conclude that $G = HK \cong H \times K$.

Now H is a group of order $9 = 3^2$. By a previous problem, we know that $H \cong \mathbb{Z}_9$ or $H \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. K has order 11, so $K \cong \mathbb{Z}_{11}$.

Remember that we can combine cyclic groups whose orders are relatively prime, so that G is isomorphic to either $\mathbb{Z}_{99}$ or $\mathbb{Z}_3 \times \mathbb{Z}_{33}$.

4. (25 points): William Wallace would be proud.

(a) State the universal property of a free group F generated by the set X equipped with mapping $i : X \to F$.

The universal mapping property says: Given any group G paired with a (set) map $f : X \to G$, there exists a *unique* group homomorphism $\hat{f} : F \to G$ such that $\hat{f} \circ i = f$.

$$\begin{tikzcd}
\mathbf{F} \arrow[dr, dashed, "\hat{f}"] & \\
\mathbf{X} \arrow[u, "i"] \arrow[r, "f"] & \mathbf{G}
\end{tikzcd}$$

(b) Sketch the proof of: If F_1 and F_2 are free on X, then $F_1 \cong F_2$.

$$\begin{tikzcd}
\mathbf{F}_1 \arrow[loop above, dashed, "\mathbf{id}_1"] \arrow[dr, dashed, shift right, "\hat{i}_2"'] & \\
\mathbf{X} \arrow[u, "i_1"] \arrow[r, "i_2"] & \mathbf{F}_2 \arrow[ul, dashed, shift right, "\hat{i}_1"'] \arrow[loop right, dashed, "\mathbf{id}_2"]
\end{tikzcd}$$

Let F_j be equipped with the map $i_j : X \to F_j$. By the universal mapping property for F_1, the map $i_2 : X \to F_2$ lifts to a homomorphism $\hat{i}_2 : F_1 \to F_2$ (where $\hat{i}_2 \circ i_1 = i_2$). Likewise, by the universal mapping property for F_2, $i_1 : X \to F_1$ lifts to a homomorphism $\hat{i}_1 : F_2 \to F_2$ (where $\hat{i}_1 \circ i_2 = i_1$).

Notice that $i_j : X \to F_j$ lifts to the identity homomorphism $\mathrm{id}_{F_j} : F_j \to F_j$ ($\mathrm{id}_{F_j} \circ i_j = i_j$). But also, $\hat{i}_1 \circ \hat{i}_2 : F_1 \to F_1$ lifts the map i_1 (since $\hat{i}_1 \circ \hat{i}_2 \circ i_1 = \hat{i}_1 \circ i_2 = i_1$). By uniqueness, we must have that $\hat{i}_1 \circ \hat{i}_2 = \mathrm{id}_{F_1}$. Likewise, by uniqueness, $\hat{i}_2 \circ \hat{i}_1 = \mathrm{id}_{F_2}$. Therefore, $\hat{i}_1$ (and $\hat{i}_2$) is an invertible homomorphism (i.e. an isomorphism). Thus $F_1 \cong F_2$.

(c) Identify the free groups on 0 and 1 generator, then use the universal property to prove that F is not abelian when $|X| > 1$.

The free group on zero generators is the trivial group. The free group on 1 generator is infinite cyclic. Both of these groups are abelian.

Let X have more than 1 element and let F be free on X (with map $i : X \to F$). Suppose that F is abelian.

[Quick proof: Let $|X| > 1$. Every group generated by $|X|$ or fewer elements is isomorphic to some quotient of F. Since S_3 is non-abelian and generated by 2 elements, it must be isomorphic to some quotient of F. But quotients of abelian groups are always abelian. Thus F cannot be abelian itself.]

Since F is free, it has the universal mapping property. Consider the case when $G = S_3$ and $f : X \longrightarrow S_3$ is defined by $f(x_0) = (12)$ for some fixed $x_0 \in X$ and $f(y) = (13)$ for all $y \in X$, $y \neq x_0$. By the universal property for F, f must lift to a homomorphism $\hat{f} : F \longrightarrow S_3$ where $\hat{f} \circ i = f$. Thus $(12), (13) \in \hat{f}(F) \subseteq S_3$. But these elements generate S_3 so that $\hat{f}$ is onto. Therefore, we have an abelian group whose homomorphic image is S_3 – a non-abelian group (contradiction). Thus F must be non-abelian.

5. (15 points): Choices: Choose **one** of the following problems.

I. Use the Todd-Coxeter algorithm to find a permutation representation of the group with presentation:

$$\langle x, y \,|\, x^2, y^2, xyx^{-1}y^{-1} \rangle$$

What is the name of this group?

Step 1:

Relation tables:

	x	x
1		1

	y	y
1		1

	x	y	x^{-1}	y^{-1}
1				1

Step 2:

Relation tables:

	x	x
1	$\boxed{2}$	1
2	1	2

	y	y
1		1
2		2

	x	y	x^{-1}	y^{-1}
1	2			1
2	1			2

Auxiliary tables:

	x
1	2
2	1

	x^{-1}
1	2
2	1

	y
1	
2	

	y^{-1}
1	
2	

Step 3:

Relation tables:

	x	x
1	2	1
2	1	2
3		3

	y	y
1	$\boxed{3}$	1
2		2
3	1	3

	x	y	x^{-1}	y^{-1}
1	2		3	1
2	1	3		2
3		2	1	3

Auxiliary tables:

	x
1	2
2	1
3	

	x^{-1}
1	2
2	1
3	

	y
1	3
2	
3	1

	y^{-1}
1	3
2	
3	1

Step 4:

Relation tables:

	x	x
1	2	1
2	1	2
3	4	3
4	3	4

	y	y
1	3	1
2	4	2
3	1	3
4	2	4

	x	y	x^{-1}	y^{-1}
1	2	$\boxed{4}$	3	1
2	1	3	4	2
3	4	2	1	3
4	3	1	2	4

Auxiliary tables:

	x
1	2
2	1
3	4
4	3

	x^{-1}
1	2
2	1
3	4
4	3

	y
1	3
2	4
3	1
4	2

	y^{-1}
1	3
2	4
3	1
4	2

The auxiliary tables give us the following permutation representation of G: x is represented by $(12)(34)$ while y is represented by $(13)(24)$. $G = \{1, x, y, xy\} \cong \{(1), (12)(34), (13)(24), (14)(23)\} \subset S_4$. So G is (isomorphic to) the Klein 4-group (or $\mathbb{Z}_2 \times \mathbb{Z}_2$).

II. Derive the formula for the order of the group $\mathrm{PSL}_2(\mathbb{F}_q)$ where $\mathbb{F}_q$ is the finite field of order q.

Let $\mathbb{F}_q$ be the field with $q = p^k$ elements.

$\mathrm{GL}_2(q)$ is the set of all invertible 2 by 2 matrices. Any vector in $\mathbb{F}_q^2$ (which has $q \cdot q$ elements) can appear as the first column of a matrix in $\mathrm{GL}_2(q)$ with one exception – the zero vector. So we have $q^2 - 1$ choices for the first column. The second column cannot be a scalar multiple of the first column. This rules out q vectors. Therefore, we have $q^2 - q$ choices for the second column. Thus $|\mathrm{GL}_2(q)| = (q^2-1)(q^2-q) = (q-1)^2 q(q+1)$.

Next, the determinant (of 2×2 matrices) is a surjective homomorphism from $\mathrm{GL}_2(q)$ onto the multiplicative group of non-zero field elements, $\mathbb{F}_q^\times$. Since $\mathrm{SL}_2(q)$ is (basically by definition) the kernel of the determinant, we have that:

$$\frac{|\mathrm{GL}_2(q)|}{|\mathrm{SL}_2(q)|} = |\mathbb{F}_q^\times| = q - 1$$

Therefore, $|\mathrm{SL}_2(q)| = (q-1)q(q+1)$.

Finally, $\mathrm{PSL}_2(q) = \mathrm{SL}_2(q)/Z$ where $Z = Z(\mathrm{SL}_2(q))$ (the center of SL_2). We know that $Z = Z(\mathrm{GL}_2(q)) \cap \mathrm{SL}_2(q) = \{aI_2 \,|\, a \in \mathbb{F}_q^\times\} \cap \mathrm{SL}_2(q) = \{aI_2 \,|\, a^2 = 1\}$ Now a polynomial of degree n cannot have more than n roots in $\mathbb{F}_q$. Therefore, if q is odd, the only elements in Z are $\pm I_2$ (since $(\pm 1)^2 = 1$ and $-1 \neq 1$ when $\mathrm{char}(\mathbb{F}_q) \neq 2$). However, if q is even (i.e. $\mathrm{char}(\mathbb{F}_q) = 2$), then $(x-1)^2 = x^2 - 2x + 1 = x^2 - 1$ (since $2 = 0$). Therefore, by uniqueness of factorizations, the only solution of $x^2 = 1$ is $x = 1$. Therefore, Z just contains the identity matrix. Therefore:

$$|\mathrm{PSL}_2(q)| = \frac{|\mathrm{SL}_2(q)|}{|Z|} = \begin{cases} \dfrac{(q-1)q(q+1)}{2} & \text{when } q \text{ is odd} \\ (q-1)q(q+1) & \text{when } q \text{ is even} \end{cases}$$