NAME:

MATH 450

Final Exam

Instructions: Give a complete solution to each problem. You may use any result from class, the book, or homework **except** the statement you are asked to prove. You may also use any fact established in Calculus or Linear Algebra classes. Be sure to justify your statements.

1. **(15 points)** Show that a group of order 351 has a normal Sylow p–subgroup for some p.

   Proof: It is enough to show $n_p = |\operatorname{Syl}_p(G)| = 1$, for some $p|351$. Note $351 = 3^3 \cdot 13$. By Sylow III we know $n_{13} \equiv 1 \pmod{13}$ and $n_{13}|27$. So $n_{13} = 1$ or 27. Suppose $n_{13} = 27$. If $P, Q \in \operatorname{Syl}_{13}(G)$, then $|P| = |Q| = 13$ is prime, so $P \cap Q = \{e\}$. Thus, there are $12 \cdot 27 = 324$ elements of order 13 in G. Since there are only 27 more elements, and any Sylow 3–subgroup has order 27, we see $n_3 = 1$. Thus, either $n_{13} = 1$ or $n_3 = 1$, so for some p there is a normal Sylow p–subgroup. □

2. **(14 points)** State and prove the Lagrange's Theorem.

   Theorem: (Lagrange) If G is a finite group and H is a subgroup of G, then $|H| \,\big|\, |G|$.

   Proof: Let $a_1, a_2, \ldots, a_k$ be representatives of the distinct left cosets of H in G. If $i \neq j$, then $a_iH \cap a_jH = \emptyset$. Also, $|a_iH| = |H|$. Finally, if $g \in G$, we know $g \in gH = a_iH$ for some i. So

   $$G = a_1H \cup a_2H \cup \cdots \cup a_kH$$

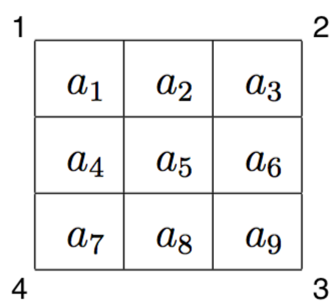
   is a disjoint union, so $|G| = k|H|$, proving the claim. □

3. **(18 points)** Consider the following 3×3 grid :

a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9

and let D_4 act on the full square. Find an expression for the number of inequivalent colorings of the grid using 4 colors.

Solution: Number the vertices of the square as shown:



We use Burnside's Theorem. We note that without considering symmetry, there are 4^9 colorings of the grid. For each $\sigma \in D_4$, we compute $|\operatorname{fix}(\sigma)|$. We note if $\sigma = 1$, then $|\operatorname{fix}(\sigma)| = 4^9$. If $\sigma = (1234)$, then the orbits of σ are $\{a_1, a_3, a_7, a_9\}, \{a_2, a_4, a_6, a_8\}$, and $\{a_5\}$ so there are 4^3 fixed colorings. Similarly, for $\sigma = (1432)$ we have $|\operatorname{fix}(\sigma)| = 4^3$. For $\sigma = (13)(24)$ we see the orbits are $\{a_1, a_9\}, \{a_2, a_8\}, \{a_3, a_7\}, \{a_4, a_6\}$, and $\{a_5\}$. So $|\operatorname{fix}(\sigma)| = 4^5$. For the reflection $(14)(23)$ the orbits are $\{a_1, a_7\}, \{a_2, a_8\}$, $\{a_3, a_9\}, \{a_4\}, \{a_5\}$, and $\{a_6\}$. So $|\operatorname{fix}(\sigma)| = 4^6$. Similarly, if $\sigma = (12)(34)$, then $|\operatorname{fix}(\sigma)| = 4^6$. For $\sigma = (24)$, we have the orbits are $\{a_2, a_4\}, \{a_3, a_7\}, \{a_6, a_8\}, \{a_1\}, \{a_5\}$, and $\{a_9\}$. So $|\operatorname{fix}(\sigma)| = 4^6$. Similarly, for $\sigma = (13)$, we have $|\operatorname{fix}(\sigma)| = 4^6$.

$$\frac{1}{8}\left(4^9 + 2 \cdot 4^3 + 4^5 + 4 \cdot 4^6\right)$$

$\square$

4. (a) **(8 points)** Give an example of a non-zero homomorphism $\varphi : R \to S$ between rings with identity so that $\varphi(1_R) \neq 1_S$, where 1_R and 1_S are identities of R and S, respectively.

   (b) **(7 points)** Show that if $\varphi : R \to S$ is a surjective homomorphism of rings with identity, then $\varphi(1_R) = 1_S$.

Solution:

(a) Let $\varphi : \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}$ be defined by $\varphi(n) = (n, 0)$. Then φ is a homomorphism and $\varphi(1) = (1, 0)$ is not the identity of $\mathbb{Z} \oplus \mathbb{Z}$.

(b) Let $s \in S$. By surjectivity, we have $s = \varphi(r)$, for some $r \in R$. Then

$$s \cdot \varphi(1_R) = \varphi(r)\varphi(1_R) = \varphi(r \cdot 1_R) = \varphi(r) = s$$

and

$$\varphi(1_R) \cdot s = \varphi(1_R) \cdot \varphi(r) = \varphi(1_R \cdot r)\varphi(r) = s.$$

Since $s \cdot \varphi(1_R) = s = \varphi(1_R) \cdot s$ for any $s \in S$, we see $\varphi(1_R) = 1_S$, by the uniqueness of the identity in S. $\square$

5. **(20 points)** State and prove the First Homomorphism Theorem for rings.

First Homomorphism Theorem: Let $\varphi : R \to S$ be a homomorphism of rings with kernel K. Then $\varphi(R) \simeq R/K$.

Proof: Let $\psi : R/K \to \varphi(R)$ be defined by $\psi(a+K) = \varphi(a)$. By the First Isomorphism Theorem for groups, we know this is an isomorphism of the additive groups R/K and $\varphi(R)$. Thus, we only need to prove

$$\psi((a+K)(b+K)) = \psi(a+K)\psi(b+K).$$

But

$$\psi((a+K)(b+K)) = \psi(ab+K) = \varphi(ab)\varphi(a)\varphi(b) = \psi(a+K)\psi(b+K).$$

Thus, ψ is also a ring homomorphism, and hence is a ring isomorphism. $\square$

6. Let F be a field and suppose $f(x) \in F[x]$ is a polynomial of degree $n \geq 1$.
   (a) **(9 points)** If $g(x) \in F[x]$, let $\overline{g(x)}$ be the element $g(x)+(f(x)) \in F[x]/(f(x))$. Prove that for each $\overline{g(x)} \in F[x]/(f(x))$ there is a unique polynomial $g_0(x)$ of degree at most $n-1$ so that $\overline{g_0(x)} = \overline{g(x)}$.
   (b) **(6 points)** Suppose F is a field with q elements. Show $F[x]/(f(x))$ has q^n elements.

Solution:

(a) By the Division Algorithm, for each $g(x) \in F[x]$ there are $q(x), r(x) \in F[x]$ with $g(x) = q(x)f(x) + r(x)$, and $\deg r(x) < \deg f(x) = n$. So takking $g_0(x) = r(x)$, we have $(g - g_0)(x) = q(x)f(x) \in (f(x))$, so $\overline{g(x)} = \overline{g_0(x)}$. This shows there is a representative g_0 of degree at most $n-1$. To see it is unique, suppose $\overline{g_0(x)} = \overline{g_1(x)}$ and $\deg g_0, \deg g_1 < n$. Then $(g_0 - g_1)(x) \in (f(x))$ and so $(g_0 - g_1)(x) = q(x)f(x)$ for some $q(x)$. If $q(x) \neq 0$, then $\deg(g_0 - g_1) = \deg(fq) = \deg f + \deg q$, which is a contradiction, since $\deg(g_0 - g_1) < n$. Thus, $q(x) = 0$, so $g_0(x) = g_1(x)$, and thus the representative is unique.

(b) By (a), each coset is represented by an element $g_0(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, and each n–tuple, $(a_0, a_1, \ldots, a_{n-1})$ of coefficients gives a unique coset in $F[x]/(f(x))$. Since there are q choices for each a_i, we see there are q^n disctinct cosets. $\square$

7. **True/False (5 points each).** Determine whether each of the following statements is true or false. If true, give a proof. If false, give a concrete counterexample.
   (a) If G is a group, H is a subgroup of G, and Ha and Hb are distinct right cosets, then aH and bH are distinct left cosets.
   (b) If R is a commutative ring with identity, and P and Q are maximal ideals of R then $P \cap Q$ is a maximal ideal.
   (c) If R is a ring, F is a field, and $\varphi : R \to F$ is a non-zero homomorphism, then $\ker \varphi$ is a maximal ideal.
   (d) $\mathbb{Z} \times \mathbb{Z}$ is a cyclic group.
   (e) If G has a unique subgroup H of a given order, then H is normal in G.

Solutions:

(a) **False:** Let $G = S_3$, $H = \{1, (12)\}$, $a = (123)$ and $b = (23)$. Since $b \notin Ha = \{(123), (13)\}$, we have $Ha \neq Hb$. But $aH = bH = \{(123), (23)\}$.

(b) **False:** Let $R = \mathbb{Z}$. Take maximal ideals $P = 2\mathbb{Z}$ and $Q = 3\mathbb{Z}$. Then $P \cap Q = 6\mathbb{Z}$ is not maximal.

(c) **False:** Let $R = \mathbb{Z}$, $F = \mathbb{Q}$, and $\varphi(n) = n$. This is a homomorphisms whose kernel is (0) which is not maximal.

(d) **False:** Suppose $\mathbb{Z} \times \mathbb{Z} = \langle (a, b) \rangle$, for some (a, b). Then $(2, 3) = (ca, cb)$, for some $c \in \mathbb{Z}$. But $\gcd(2, 3) = 1$, so $c = \pm 1$, and so $(a, b) = \pm(2, 3)$. But then $(1, 0) \notin \langle (2, 3) \rangle$, contradicting our choice of (a, b). Thus, $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

(e) **True:** For each $g \in G$, we have $|gHg^{-1}| = |H|$, so by uniqueness, $gHg^{-1} = H$, so $H \triangleleft G$.

8. Let G be a group. For $g \in G$, define $\sigma_g : G \to G$ by $\sigma_g(x) = gxg^{-1}$.

   (a) **(9 points)** Show σ_g is an automorphism of G.

   (b) **(9 points)** Let $\mathrm{Aut}(G)$ be the group of all automorphisms of G (You need not prove $\mathrm{Aut}(G)$ is a group.) Let $\psi : G \to \mathrm{Aut}(G)$ be given by $\psi(g) = \sigma_g$. Show ψ is a homomorphism.

   (c) **(5 points)** Find the kernel of ψ.

   Solutions:

   (a) Let $x, y \in G$. Then $\sigma_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \sigma_g(x)\sigma_g(y)$. So σ_g is a homomorphism. If $\sigma_g(x) = \sigma_g(y)$ then $gxg^{-1} = gyg^{-1}$, so $x = y$, and thus σ_g is one-to-one. If $y \in G$, then $y = \sigma_g(g^{-1}yg)$, so σ_g is onto. Hence σ_g is an isomorphism from G to G,i.e., an automorphism.

   (b) Note, for $g, h \in G$ we have $\psi(gh) = \sigma_{gh}$, and

   $$\sigma_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = \sigma_g(\sigma_h(x)) = \sigma_g\sigma_h(x).$$

   So, $\sigma_{gh} = \sigma_g\sigma_h$, and so $\psi(gh) = \psi(g)\psi(h)$. Thus, ψ is a homomorphism.

   (c) Note $g \in \ker\psi$ if and only if $\psi(g) = 1_G$, where $1_G(x) = x$, for all $x \in G$. Thus, $g \in \ker\psi$ if and only if $\sigma_G(x) = x$ for all x. Which holds if and only if $gxg^{-1} = x$ for all x. Which holds if and only if $gx = xg$ for all x. so $\ker\psi = Z(G)$, the center of G. □

9. **(13 points)** Let G be a group of permutations on a set X. For $x \in X$ we let

   $$\mathrm{Stab}_G(x) = \{\sigma \in G | \sigma(x) = x\}.$$

   Prove $\mathrm{Stab}_G(x)$ is a subgroup of G.

   Proof: Note, the identity $1_X : X \to X$ satisfies $1_X(y) = y$, for all $y \in X$, and so we know $1_X \in \mathrm{Stab}_G(x)$, so $\mathrm{Stab}_G\, x) \neq \emptyset$. Let $\sigma, \tau \in \mathrm{Stab}_G(x)$. Then $\sigma\tau(x)$ $s(\tau(x)) = \sigma(x) = x$, so $\sigma\tau \in \mathrm{Stab}_G(x)$. Thus, $\mathrm{Stab}_G(x)$ is closed under group multiplication. Also, $\sigma(x) = x$ implies $\sigma^{-1}(\sigma(x)) = \sigma^{-1}(x)$, so $\sigma^{-1}(x) = x$, so

$\sigma^{-1} \in \mathrm{Stab}_G(x)$. Tghus, $\mathrm{Stab}_G(x)$ is also closed under inversion, and hence is a subgroup. $\square$

10. **(18 points)** Let $n \geq 3$. Recall $A_n \subset S_n$ is the subgroup of even permutations of $\{1, 2, \ldots, n\}$. Prove that A_n contains a subgroup which is isomorphic to S_{n-2}. (Hint: Try to construct an explicit monomorphism $\varphi : S_{n-2} \to S_n$, whose image is in A_n.

Proof: Let $\gamma = (n-1\, n) \in S_n$. Note $\sigma\gamma = \gamma\sigma$ for any $\sigma \in S_{n-2}$, since the two permutations are disjoint. Now let $\varphi : S_{n-2} \to S_n$ be given by

$$\varphi(\sigma) = \begin{cases} \sigma & \text{if } \sigma \text{ is even;} \\ \sigma\gamma & \text{if } \sigma \text{ is odd.} \end{cases}$$

Note $\varphi(\sigma) \in A_n$ for each σ. Also, if σ, τ are both even, then $\varphi(\sigma\tau) = \sigma\tau = \varphi(\sigma)\varphi(\tau)$. If both σ, τ are odd, then $\sigma\tau$ is even and $\varphi(\sigma\tau) = \sigma\tau = (\sigma\gamma)(\tau\gamma) = \varphi(\sigma)\varphi(\tau)$. Now if one of σ, τ is even, and the other odd,then $\sigma\tau$ is odd,so $\varphi(\sigma\tau) = \sigma\tau\gamma = \sigma(\tau\gamma) = (\sigma\gamma)\tau = \varphi(\sigma)\varphi(\tau)$, no matter which is odd. Thus, φ is a homomorphism. Clearly, $\varphi(\sigma) = 1$ only if $\sigma = 1$, so φ is a monomorphism. Thus, $\varphi(S_{n-2}) \subset A_n$ is the desired subgroup. $\square$

11. Let R be a ring. An element $a \in R$ is *nilpotent* if there is some $n > 0$ with $a^n = 0$.
    (a) **(10 points)** Prove that if R is commutative a, b are nilpotent, then so is $a+b$.
    (b) **(8 points)** Show that if R is a commutative ring with identity, then the set, N, of all nilpotent elements of R forms an ideal.
    (c) **(6 points)** Show R/N is a ring with no non-zero nilpotent elements.

Solutions:

(a) Let $m \geq n > 0$, with $a^n = b^m = 0$. Note if $k \geq m$ then $a^k = b^k = 0$. Now note

$$(*) \qquad (a+b)^{2m} = \sum_{k=0}^{2m} \binom{2m}{k} a^k b^{2m-k}.$$

Note, if $k < m$, then $2m - k > m$, so for each term in the sum, either $a^k = 0$ or $b^{2m-k} = 0$. Thus, the sum (*) is zero, and $(a+b)^{2m} = 0$, which shows $a+b$ is nilpotent.

(b) By (a) N is closed under addition. Also, if $a \in N$, and $a^n = 0$, then $(-a)^n = (-1)^n a^n = 0$, so $-a \in N$. Thus, N is a subgroup of the additive group R. Let $r \in R$ and $a \in N$. Suppose $n > 0$ with $a^n = 0$. Then $(ra)^n = r^n a^n = r^n \cdot 0 = 0$, so $ra \in N$. Thus, N is an ideal.

(c) Suppose $a \in R$ and $\bar{a} = a + N$ is a nilpotent element in R/N. Then, for some $n > 0$, we have $\bar{a}^n = \bar{0}$, the zero element of R/N. Since N is the zero element of R/N, we have $\bar{a}^n = \overline{a^n} = N$, so $a^n \in N$. But then, for some $m > 0$, we have $(a^n)^m = 0$, so $a \in N$, i.e., $\bar{a} = \bar{0}$. Thus, zero is the only nilpotent element in R/N. $\square$

Extra Credit: (10 points) Prove the following are equivalent for a ring R:

i) R has no non-zero nilpotent elements

ii) If $a \in R$ and $a^2 = 0$, then $a = 0$.

Proof: Suppose (i) holds. If $a^2 = 0$, then by definition, a is nilpotent, hence $a = 0$. So (ii) holds. Now suppose (ii) holds. Let $a \in R$ be nilpotent. Then, for some $n > 0$, we have $a^n = 0$. If $a = 1$, then $a = 0$. If $n = 2$, then by assumption (ii) $a = 0$. Suppose $n \geq 3$, and n is the smallest positive integer with $a^n = 0$, i.e., assume $a^{n-1} \neq 0$. Then $2(n-1) = 2n - 2 > n$, since $n > 2$. So $a^{2n-2} = (a^{n-1})^2 ==$, so by (ii) we have $a^{n-1} = 0$, contradicting our choice of n. Thus, if a is nilpotent, $a = 0$. $\square$