FINAL EXAM SOLUTIONS

Instructions: Justify your answers. You may use results from the homework sets, but make sure to carefully state such results. No calculators and no notes allowed. You may e.g., use part of Problem 4 to do part of Problem 1, even if you are unsuccessful with that part of Problem 4. You may use part (a) of a problem to do part (b) even if you have not solved (a), and so on.

Grading: This exam is worth 30 points. If you completed homework assignments, your homework bonus (out of 3 points) will be added to your score. You need a score of 12.5/30 or higher to pass this exam. More precisely, the following scale will be used:

A: $[26.5, 30]$, B: $[23, 26.5)$, C: $[19.5, 23)$, D: $[16, 19.5)$, E: $[12.5, 16)$, F: $[0, 12.5)$.

Problem 1. *Let S_4 be the symmetric group on $\{1, 2, 3, 4\}$.*

(a) *(2 points) Show that the quaternion group of order 8 is not a subgroup of S_4.*
(b) *(2 points) Let H be a subgroup of S_4 which contains a 3-cycle and a 4-cycle. Show that $H = S_4$.*
(c) *(2 points) Let V be the Klein 4 subgroup of S_4 given by $V := \{e, (12)(34), (14)(23), (13)(24)\}$. Show that V is normal in S_4.*
(d) *(2 points) Show that $S_4/V \cong S_3$.*

Solution. (a) A subgroup of S_4 of order 8 is a 2-Sylow subgroup. By Sylow's Theorem, all p-Sylow subgroups are conjugate. The subgroup $\langle (1234), (14)(23) \rangle$ is dihedral of order 8, because conjugating (1234) by $(14)(23)$ gives $(4321) = (1432) = (1234)^{-1}$. Therefore every subgroup of order 8 of S_4 is dihedral of order 8. Since the quaternion group of order 8 is not isomorphic to the dihedral group of order 8, the quaternion group of order 8 is not a subgroup of S_4.

(b) The subgroup A_4 of S_4 is the unique subgroup of order 12 (else, if N were another such subgroup, then $N \cap A_4$ would be a subgroup of A_4 of order 6, but A_4 has no such subgroup). The order of H is divisible by 3 and 4, hence by 12. Since a 4-cycle is odd, A_4 contains no 4-cycles. Thus H is not A_4, so $H = S_4$.

(c) A subgroup of a group G is normal if and only if it is a disjoint union of conjugacy classes of G. The subgroup V is the union of the identity and the conjugacy class of elements of type $(2, 2)$ (product of two disjoint transpositions). Hence V is normal in S_4.

(d) The quotient S_4/V has order 6. A group of order 6 is either cyclic or isomorphic to $S_3 \cong D_6$. If S_4/V were cyclic, it would have a normal subgroup of index 3, which by the isomorphism theorems would correspond to a normal subgroup of S_4 of order 8 i.e., a 2-Sylow of S_4. However, S_4 has 3 Sylow 2-subgroups.

Here is one way to see that: There are $4 \cdot 3/2 = 6$ transpositions in S_4 and the number of 4-cycles in S_4 is $4!/4 = 3! = 6$. If there were a unique 2-Sylow, it would have to contain these 12 elements of 2-power order.

Variant: The group S_4 acts transitively by conjugation on the set $\mathsf{Syl}_2(S_4)$ of its 2-Sylow subgroups. Since V is normal, it acts trivially. The action gives a permutation representation $\rho : S_4 \to S_3$. It remains to see ρ is surjective. If not, $\ker \rho$ would be a normal subgroup containing V, hence $\ker V$ would be A_4 or S_4, contradicting the transitivity of the action. Alternatively, any element of 2-power order not in V (e.g., a transposition) normalizes the unique 2-Sylow it contains and permutes the other 2-Sylows. This shows that $\mathrm{Im}(\rho)$ has even order; that the order is divisible by 3 follows from the transitivity of the action.

□

E-mail address: `wgoldring@math.su.se`.

Problem 2. *Let G be a group. A subgroup K of G is said to be characteristic in G if K is stable under all automorphisms of G i.e., $\varphi(K) = K$ for all $\varphi \in \mathrm{Aut}(G)$.*

(a) (1 points) Show that a characteristic subgroup of G is normal in G.
(b) (2 points) Assume N is a normal subgroup of G and K is a characteristic subgroup of N. Show that K is normal in G.
(c) (2 points) Let p be a prime. Assume G is finite and that P is a p-Sylow subgroup of G. Show that the normalizer $N_G(P)$ of P in G is self-normalizing i.e. $N_G(N_G(P)) = N_G(P)$.
(d) (2 point) Assume G is finite and that P, Q are two distinct p-Sylow subgroups of G of order p^2. If $P \cap Q \neq \{e\}$, show that $N_G(P \cap Q)$ contains at least $p + 1$ Sylow p-subgroups of G.

Solution. (a) By definition, a subgroup is normal if and only if it is stable under all inner automorphisms; hence a subgroup stable under all automorphisms is normal.

(b) Let $\mathrm{Int}_x : G \to G$ denote the inner automorphism given by conjugation by $x \in G$; thus $\mathrm{Int}_x(g) = xgx^{-1}$. Since N is normal in G, the inner automorphism Int_x leaves N stable, so its restriction $\mathrm{Int}_x|_N$ to N gives an automorphism of N (not necessarily inner as automorphism of N). Since K is characteristic in N, it is stable under the automorphism $\mathrm{Int}_x|_N$. Since K is stable under all inner automorphisms of G, K is normal in G.

(c) Every subgroup H of G is normal in its normalizer; in fact the normalizer $N_G(H)$ is characterized as the largest subgroup of G in which H is normal. Hence P is normal in $N_G(P)$. Since P is a p-Sylow of G, it is also a p-Sylow in $N_G(P)$. By Sylow's Theorems, P is the unique p-Sylow of $N_G(P)$.

If φ is an automorphism of G, then φ maps a subgroup H to a subgroup of the same order as H. Hence φ maps a p-Sylow to another p-Sylow.

Hence P is characteristic in $N_G(P)$. Since $N_G(P)$ is normal in $N_G(N_G(P))$, by (b) we get that P is normal in $N_G(N_G(P))$. Hence $N_G(N_G(P))$ is contained in $N_G(P)$. Since the reverse inclusion is trivial, the two normalizers are equal.

(d) Since every group of order p^2 is abelian, The p-Sylows P, Q are both contained in $N_G(P \cap Q)$. Hence P, Q are two distinct p-Sylow subgroups of $N_G(P \cap Q)$. By Sylow's Theorems, the number of p-Sylows is $\equiv 1 \pmod p$. Since it is ≥ 2, it must be at least $p + 1$.

$\square$

Problem 3. *Let R be a commutative ring with 1.*

(a) *(1 point) Assume R is an integral domain. Show that the polynomial $x^2 - 1 \in R[x]$ has at most two distinct roots in R.*

(b) *(1 point) Give an example of an integral domain R where $x^2 - 1 \in R[x]$ has just one distinct root in R.*

(c) *(1 point) Let p be a prime and $k \geq 2$ an integer. Show that $\mathbf{Z}/p^k\mathbf{Z}$ contains nonzero nilpotent elements and a unique maximal ideal.*

(d) *(1 point) Give an example where R has a unique maximal ideal and where $x^2 - 1 \in R[x]$ has strictly more than 2 distinct roots in R.*

(e) *(1 point) Give an example where R has no nonzero nilpotent elements and where $x^2 - 1 \in R[x]$ has strictly more than 2 distinct roots in R.*

Solution. (a) One has $a^2 - 1 = (a-1)(a+1)$ in R. If a is a root of $x^2 - 1$ in R, then $(a-1)(a+1) = 0$ in R. Since R is an integral domain, $a = 1$ or $a = -1$ (and these two possibilities are the same if R has characteristic 2 i.e., if $1 + 1 = 0$ in R).

(b) In $R = \mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ there is a unique solution $x = 1$, since $1 = -1$ in $\mathbf{F}_2$.

(c) One has $p \neq 0$ since $k \geq 2$ and $p^k = 0$ in $\mathbf{Z}/p^k\mathbf{Z}$. Hence p is a nonzero nilpotent element. If I is an ideal in $\mathbf{Z}/p^k\mathbf{Z}$, then $\pi^{-1}I$ is an ideal in $\mathbf{Z}$, where $\pi : \mathbf{Z} \to \mathbf{Z}/p^k\mathbf{Z}$ is the projection. Since $\mathbf{Z}$ is a PID, $\pi^{-1}I = (a)$ for some integer (a); thus $I = \pi(a)$ is also principal. By the Isomorphism Theorems, ideals of $\mathbf{Z}/p^k$ correspond to ideals of $\mathbf{Z}$ containing (p^k) via $I \to \pi^{-1}(I)$. Therefore, if I is maximal in $\mathbf{Z}/p^k$, then $\pi^{-1}I$ is maximal in $\mathbf{Z}$ and if J is maximal in $\mathbf{Z}$ then either $\pi(J)$ is maximal in $\mathbf{Z}/p^k$ or $\pi(J) = \mathbf{Z}/p^k$. It follows that the one and only maximal ideal of $\mathbf{Z}/p^k$ is (p) (if q is a prime different from p, then $\pi((q)) = \mathbf{Z}/p^k$ since $\pi(q)$ is a unit in $\mathbf{Z}/p^k$).

(d) In $\mathbf{Z}/8\mathbf{Z}$, the unique maximal ideal is (2) by (c) and $1, 3, 5, 7$ are four distinct roots of $x^2 - 1$.

(e) The ring $\mathbf{Z}/15\mathbf{Z}$ has no nonzero nilpotent elements, since for an integer a, if a^n is divisible by 15, then a is already divisible by 15 (consider the factorizations of a and a^n into primes). By contrast, $\mathbf{Z}/15$ does have zero divisors *e.g.*, $3 \cdot 5 = 0$ in $\mathbf{Z}/15$.

The elements $1, -1, 4, -4$ are distinct roots of $x^2 - 1$ in $\mathbf{Z}/15\mathbf{Z}$ (under the Chinese Remainder isomorphism $\mathbf{Z}/15 \cong \mathbf{Z}/5 \times \mathbf{Z}/3$, these correspond to $(1, 1)$, $(-1, -1)$, $(-1, 1)$ and $(1, -1)$ respectively). □

Problem 4. *Let p be an odd prime and let $n \geq 1$ be an integer.*

(a) (2 points) Show that a group of order $2p$ which is not abelian is isomorphic to the dihedral group D_{2p} of order $2p$.
(b) (1 points) Show that any group of order $2p$ is either dihedral or cyclic.
(c) (2 points) Let G be a group of order $2n$ with an element b of order n and an element a of order 2 which is not a power of b. Show that every element of G can be written uniquely in the form $a^i b^j$ with $0 \leq i \leq 1$ and $0 \leq j \leq n-1$.
(d) (2 points) Give an example of a group of order 16 which is neither abelian nor dihedral but which is an example of (c) i.e., G has an element b of order 8 and an element a of order 2 which is not a power of b. Justify your answer.

Solution. (a) Let G be a group of order $2p$. By Sylow's Theorems, G has a unique, normal p-Sylow subgroup; call it N. Let b be a generator of N. Let a be an element of order 2 in G. Then a and b together must generate all of G by order considerations. Thus, if a and b commute, then G is abelian.

Assume that G is not abelian. Then a and b do not commute. Since N is normal in G, one has $aba^{-1} \in N$; hence $aba^{-1} = b^j$ for some $j \in \mathbf{Z}$. A second iteration of this relation gives

$$a^2 ba^{-2} = ab^j a^{-1} = (aba^{-1})^j = b^{j^2}.$$

Since $a^2 = e$, we get $b^{j^2} = b$. So $b^{j^2-1} = e$. Since b has order p, p divides $j^2 - 1 = (j+1)(j-1)$. Hence p divides $j+1$ or p divides $j-1$. Since $ab \neq ba$ one has $j \not\equiv 1 \pmod{p}$. So we conclude that $j \equiv -1 \pmod{p}$. Therefore

$$G = \langle a, b \,| a^2 = b^p = e, \; aba^{-1} = b^{-1} \rangle$$

is a presentation of G which exhibits it as a dihedral group of order $2p$.

(b) Let G have order $2p$. If G is not abelian, it is dihedral by (a). If G is abelian, then, given a of order 2 and b of order p, the product ab has order divisible by $\mathrm{lcm}(2, p) = 2p$; thus ab is a generator of G.

(c) Let $N := \langle b \rangle$ and $H := \langle a \rangle$. Then N is normal in G. So HN is a subgroup of G and $HN = G$ since the orders of H, N are coprime and their product is the order of G. Therefore every element of $G = HN$ is of the form $a^i b^j$. The expression is unique because for all $h_1, h_2 \in H$ and $n_1, n_2 \in N$, an equality $h_1 n_1 = h_2 n_2$ implies that $h_2^{-1} h_1 = n_2 n_1^{-1}$ is an element of $H \cap N = \{e\}$. Thus $h_1 = h_2$ and $n_1 = n_2$.

(d) Define

$$G = \langle a, b \mid a^2 = b^8 = e, \; aba^{-1} = b^3 \rangle.$$

Then G has order 16 and is an example of (c) because $3^2 \equiv 1 \mod 8$, so that $a^2 ba^{-2} = b^{3^2} = b$ in G.

□

Problem 5.

(a) (1 point) Show that $x^3 + 6x + 10$ is irreducible in $\mathbf{Q}[x]$ but reducible in $\mathbf{R}[x]$.
(b) (1 point) Show that $x^4 + 1$ is irreducible in $\mathbf{Q}[x]$.
(c) (1 point) Show that $x^4 + 1$ is reducible in $\mathbf{F}_3[x]$.

Solution. (a) By the rational root test, any root in $\mathbf{Q}$ must be an integer dividing 10. By plugging in such integers, one checks that $x^3 + 6x + 10$ has no roots in $\mathbf{Q}$. A polynomial of degree at most 3 is irreducible over a field if and only if it has no roots in that field. Hence $x^3 + 6x + 10$ is irreducible over $\mathbf{Q}$.

Since a polynomial is continuous on $\mathbf{R}$ and since $x^3 + 6x + 10$ tends to $+\infty$ (resp. $-\infty$ as x tends to $+\infty$ (resp. $-\infty$), by the intermediate value theorem $x^3 + 6x + 10$ has a real root.

(b) As in (a), the rational root test shows that $x^4 + 1$ has no roots. Hence, if $x^4 + 1$ is reducible, then it must factor as

$$x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

for some $a, b, c, d \in \mathbf{Q}$. Multiplying out and equating terms of each degree gives $a+c = 0$, $b+d+ac = 0$, $ad + bc = 0$ and $bd = 1$. Substituting $a = -c$ into $ad + bc = 0$ gives $c(b - d) = 0$. So $c = 0$ or $b = d$.

If $c = 0$, then $a = 0$ and $b = -d$. Thus $bd = 1$ gives $b^2 = -1$ which contradicts $b \in \mathbf{Q}$ (by the rational root test $x^2 + 1$ is irreducible over $\mathbf{Q}$).

If $b = d$, then $bd = 1$ gives $b = d = 1$ or $b = d = -1$. Then $b + d + ac = 0$ gives $a^2 = 2$ or $a^2 = -2$ and both contradict $a \in \mathbf{Q}$ (again $x^2 + 2$ and $x^2 - 2$ are both irreducible over $\mathbf{Q}$ by the rational root test).

(c) In $\mathbf{F}_3$, one has $-2 = 1$, so given (b), we are led to $a^2 = 1$. Taking $a = 1$ gives $c = -1$ (and taking $a = -1$ will symmetrically give $c = 1$). One finds $b = d = -1$ and that these values satisfy all the equations above in $\mathbf{F}_3$. Thus $x^4 + 1 = (x^2 + x - 1)(x^2 - x - 1)$ in $\mathbf{F}_3[x]$.

$\square$