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 (6 points)**.** *Let $n \geq 2$ be an integer, let S_n be the symmetric group on $\{1, 2, \ldots, n\}$ and let $\tau \in S_n$ be a transposition.*

(a) (1 point) Compute the size of the conjugacy class of τ in S_n.

(b) (3 points) Describe an isomorphism between the centralizer $\mathrm{Cent}_{S_n}(\tau)$ of τ and the direct product $\mathbf{Z}/2 \times S_{n-2}$.

(c) (1 points) For $n > 2$ show that there is no n-cycle in S_n which commutes with τ.

(d) (1 point) Give an example of $n > 2$, a transposition τ and an element of order n in S_n which commutes with τ.

Solution. (a) The conjugacy class of τ consists precisely of all transpositions. There are $n(n-1)/2$ transpositions in S_n.

(b) Let $C = \mathrm{Cent}_{S_n}(\tau)$. By definition $\langle \tau \rangle$ is contained in the center of C, so in particular is normal in C. Further, writing $\tau = (i\ j)$ for some distinct $i, j \in \{1, 2, \ldots, n\}$, let H be the subgroup of S_n which fixes both i and j. Then $H \subset C$. Since $\langle \tau \rangle$ is central in C, H is normal in the product $\langle \tau \rangle H$. Since $\langle \tau \rangle \cap H = \{e\}$, the product is direct $\langle \tau \rangle H = \langle \tau \rangle \times H$ and it is a subgroup of C of order $2(n-2)!$.

The index of C in S_n is the order of the conjugacy class of τ. By (a), the order of C is $2(n!)/n(n-1) = 2(n-2)!$. Since C and its subgroup $\langle \tau \rangle \times H$ have the same order, they are equal: $C = \langle \tau \rangle \times H$.

Any bijection between $\{1, 2, \ldots, n\} \setminus \{i, j\}$ and $\{1, 2 \ldots, n-2\}$ defines an isomorphism φ_0 from H onto S_{n-2}. Hence $\varphi : \langle \tau \rangle \times H \to \mathbf{Z}/2 \times S_{n-2}$ given by $\varphi(\tau^i, \sigma) := (i, \varphi_0(\sigma))$ defines the desired isomorphism.

(c) By (b) any element of C either fixes two elements i, j or its decomposition into disjoint cycles involves a transposition. Neither is true of an n-cycle.

(d) Let $n = 6$ and $\tau = (12)$ and $\sigma = (12)(345)$ Then $\sigma\tau = \tau\sigma$ and σ has order $\mathrm{lcm}\{2, 3\} = 6$. □

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

Problem 2 (5 points)**.** *Assume N and M are two subgroups of a group G.*

(a) (2 points) Suppose N is normal in G. Show that NM is a subgroup of G.

(b) (1 points) Now assume that both N and M are normal in G. Show that NM is normal in G.

(c) (2 points) Finally, suppose that both N and M are normal in G, that $NM = G$ and that $N \cap M = \{e\}$. Show that $G \cong N \times M$.

Solution. (a) Let n_1m_1 and n_2m_2 be two elements of NM. Then

$$n_1m_1n_2m_2 = n_1(m_1n_2m_1^{-1})m_1m_2$$

belongs to NM since $m_1n_2m_1^{-1} \in N$ by normality of N. Similarly, if $nm \in NM$, then

$$(nm)^{-1} = m^{-1}n^{-1} = (m^{-1}n^{-1}m)m^{-1}$$

is again in NM by normality of N. Hence NM is a subgroup of G.

(b) If both N and M are normal, then for all $g \in G$ and all $nm \in NM$ one has

$$gnmg^{-1} = (gng^{-1})(gmg^{-1}) \in NM,$$

where the first grouped term is in N since N is normal and the second grouped term is in M since M is normal in G.

(c) Since both N and M are normal in G,

$$nmn^{-1}m^{-1} \in N \cap M$$

for all $n \in N$ and $m \in M$. Since $N \cap M = \{e\}$, we conclude that $nm = mn$ for all $n \in N$ and $m \in M$. This shows that the map $\varphi : NM \to N \times M$ given by $\varphi(nm) = (n, m)$ is a well-defined group isomorphism. □

Problem 3 (9 points)**.** *Let G be a finite group.*

(a) (3 points) Assume $|G| = 33$. Show G is cyclic.

(b) (3 points) Assume $|G| = 5^3 \cdot 31$. Show that G has a nontrivial, normal p-Sylow subgroup for some prime p.

(c) (3 points) Assume $|G| = 165$ and that G has a normal 5-Sylow subgroup. Show that G is abelian.

Solution. (a) Since 3 does not divide $11 - 1 = 10$, Sylow's theorems imply that G has a normal 3-Sylow subgroup P and a normal 11-Sylow subgroup Q. Since $(3, 11) = 1$, by Lagrange's theorem the intersection $P \cap Q = \{e\}$ and the product $PQ = G$. Since P and Q are both normal, we conclude $G = P \times Q$. If a is a generator of P and b is a generator of Q, then again $(3, 11) = 1$ implies that the product ab generates G.

(b) If G has a unique 31-Sylow, it is normal by Sylow's theorems and we are done. Otherwise, since the number of 31-Sylows is $\equiv 1 \pmod{31}$ and divides 5^3, the number of 31-Sylows must be 5^3. Since two distinct 31-Sylows intersect in the identity, and each contains 30 non-identity elements, all of order 31, the 5^3 Sylow 31-subgroups account for $30 \cdot 5^3$ elements of order 31. This leaves 5^3 elements of order $\neq 31$, which must make up the one and only 5-Sylow of G. Hence G has a normal 5-Sylow.

(c) One has $165 = 3 \cdot 5 \cdot 11$. By Sylow's theorems, G has a unique, hence normal 11-Sylow P. By assumption G has a normal 5-Sylow, call it Q. Let R be a 3=Sylow of G. Since P is normal in G, it is normalized by R. Hence PR is a subgroup of order 33; it is cyclic by (a). Hence reciprocally also R is normalized by P. The index of the normalizer $N_G(R)$ in G is the number of 3-Sylow subgroups. Since P normalizes R, the normalizer $N_G(R)$ contains the subgroup PR of order 33. So the number of 3-Sylow subgroups of G divides $165/33 = 5$. Since it is also 1 mod 3, we conclude that R is the unique 3-Sylow of G, hence it too is normal in G. As in (a), one has $G = P \times Q \times R$ since $3, 5, 11$ are pairwise relatively prime and if a, b, c are generators of P, Q, R respectively, then the product abc generates $PQR = G$.

□

Problem 4 (3 points)**.** *Let $\varphi : R \to S$ be a homomorphism between commutative rings with* 1*.*

(a) (1 point) Show that the inverse image of a prime ideal in S is a prime ideal in R.
(b) (1 point) Show that every maximal ideal of S is a prime ideal of S.
(c) (1 point) Show by example that the inverse image of a maximal ideal in S need not be maximal in R.

Solution. (a) Let Q be a prime ideal in S and set P to be the inverse image of Q in R. The inverse image of a subgroup under a group homomorphism is a subgroup, so P is a subgroup of R under $+$. If $r \in R$ and $a \in P$, then $\varphi(a) \in Q$, so $\varphi(ra) = \varphi(r)\varphi(a) \in Q$ since Q is an ideal. Hence ra is in P, which shows P is an ideal. If $a_1a_2 \in P$ for some $a_1, a_2 \in R$, then $\varphi(a_1a_2) = \varphi(a_1)\varphi(a_2) \in Q$, so $\varphi(a_1) \in Q$ or $\varphi(a_2) \in Q$ since Q is prime. If $\varphi(a_i) \in Q$ then $a_i \in P$ for $i = 1, 2$. Hence $a_1 \in P$ or $a_2 \in P$. So P is a prime ideal in R.

(b) Assume $\mathfrak{m}$ is a maximal ideal in S and that $ab \in \mathfrak{m}$ for some $a, b \in S$. If $a \in \mathfrak{m}$, we are done. Otherwise, $(\mathfrak{m}, a)$ is an ideal which properly contains $\mathfrak{m}$; so $(\mathfrak{m}, a) = S$ since $\mathfrak{m}$ is maximal. In particular, there exists $m \in \mathfrak{m}$ and $s \in S$ such that $1 = m + sa$. Multiplying by b gives $b = mb + sab$. The two summands on the right belong to $\mathfrak{m}$, so $b \in \mathfrak{m}$.

(c) Let $\varphi : \mathbf{Z} \to \mathbf{Q}$ be the inclusion. The zero ideal (0) is maximal in $\mathbf{Q}$ because $\mathbf{Q}$ is a field. Its inverse image in $\mathbf{Z}$ is again (0) and (0) is not maximal in $\mathbf{Z}$ as it is properly contained in (n) for every $n > 1$. □

Problem 5 (7 points). *Let $f(x) \in \mathbf{Z}[x]$.*

(a) (1 point) Assume $f(x) = x^3 - 2x + 14$. Show that $f(x)$ is irreducible in $\mathbf{Q}[x]$ but reducible in $\mathbf{R}[x]$.

(b) (1 point) Assume that f is monic and that for some prime p, the reduction of f modulo p is irreducible in $\mathbf{F}_p[x]$. Show that $f(x)$ is irreducible in $\mathbf{Z}[x]$.

(c) (1 point) Assume f is irreducible in $\mathbf{Q}[x]$. Is f necessarily irreducible in $\mathbf{Z}[x]$? Explain.

(d) (1 point) Assume $f(x) = x^4 + ax^2 + b$ for some $a, b \in \mathbf{Z}$. Show that the roots of f in $\mathbf{C}$ have the form $\pm\alpha, \pm\beta$ for some $\alpha, \beta \in \mathbf{C}$ and that $(\alpha\beta)^2 \in \mathbf{Z}$.

(e) (2 points) Let $f(x)$ be as in (d). Show that f is irreducible over $\mathbf{Q}$ if and only if none of $\alpha^2, \alpha - \beta, \alpha + \beta$ lie in $\mathbf{Q}$. Hint: *Compute also $\alpha^2 + \beta^2$.*

(f) (1 point) As a concrete example of (d)-(e), factor $f(x) = x^4 + 4$ into irreducibles over $\mathbf{Q}$.

Solution. (a) By the rational root test, any root in $\mathbf{Q}$ must be an integer dividing 14. By plugging in, we check that none of $\pm 1, \pm 2, \pm 7, \pm 14$ are roots of f. So f has no root in $\mathbf{Q}$. Since its degree is ≤ 3, f is irreducible over $\mathbf{Q}$.

(b) Assume f factors in $\mathbf{Z}[x]$ as $f = gh$. Since also $f = (-g)(-h)$, we may assume g, h are both monic. Now $\bar{f} = \bar{g}\bar{h}$ in $\mathbf{F}_p[x]$ where bar denotes reduction mod p. Since g, h are both monic and $\bar{f}$ is irreducible in $\mathbf{F}_p[x]$ we must have $g = 1$ or $h - 1$.

(c) No. Example: $f(x) = 2x$ is irreducible in $\mathbf{Q}[x]$ but reducible in $\mathbf{Z}[x]$ since 2 is not a unit in $\mathbf{Z}$.

(d) One has $f(x) = g(x^2)$, where $g(y) = y^2 + ay + b$. Solving for y using the quadratic formula gives that the roots of f are

$$\pm\sqrt{\frac{-a \pm \sqrt{a^2 - 4b}}{2}}.$$

So the roots have the form $\pm\alpha$ and $\pm\beta$ if we set $\alpha = \sqrt{\frac{-a+\sqrt{a^2-4b}}{2}}$ and $\beta = \alpha = \sqrt{\frac{-a-\sqrt{a^2-4b}}{2}}$. Then

$$(\alpha\beta)^2 = \left(\frac{-a + \sqrt{a^2 - 4b}}{2}\right)\left(\frac{-a - \sqrt{a^2 - 4b}}{2}\right) = \frac{a^2 - (a^2 - 4b)}{4} = b \in \mathbf{Q}.$$

(e) First note that $\alpha^2 + \beta^2 = -a \in \mathbf{Q}$. So if either $\alpha - \beta$ or $\alpha + \beta$ is in $\mathbf{Q}$, then using $(\alpha \pm \beta)^2 = \alpha^2 + \beta^2 \pm 2\alpha\beta$ shows that $\alpha\beta \in \mathbf{Q}$.

If $\alpha^2 \in \mathbf{Q}$ (resp. $\alpha - \beta \in \mathbf{Q}$, $\alpha + \beta \in \mathbf{Q}$, then $(x - \alpha)(x + \alpha) = x^2 - \alpha^2$ (resp. $(x + \alpha)(x - \beta)$, $(x + \alpha)(x + \beta)$) is a factor of f over $\mathbf{Q}$, so that f is reducible.

Conversely, assume none of $\alpha^2, \alpha + \beta, \alpha - \beta$ are in $\mathbf{Q}$. Then $\alpha \notin \mathbf{Q}$. Further $(\alpha\beta)^2 \in \mathbf{Q}$ shows that β^2 and thus also β does not belong to $\mathbf{Q}$. Hence f has no roots in $\mathbf{Q}$. So the only way for f to be reducible would be to factor as a product $q_1 q_2$ of two quadratic polynomials $q_1, q_2 \in \mathbf{Q}[x]$. But the roots of q_1 are among $\pm\alpha, \pm\beta$, so either the coefficient of x in q_1 would be $\pm(\alpha \pm \beta)$ or the constant term of q_1 would be $-\alpha^2$ or $-\beta^2$, contradicting that none of these lie in $\mathbf{Q}$.

(f) Specializing (d) with $a = 0$ and $b = 4$, we are led to let $\alpha = \sqrt{2i}$ and $\beta = \sqrt{-2i}$. The square-root of i and $-i$ is only determined up to sign; let us fix $\sqrt{i} = e^{2\pi i/8}$ and $\sqrt{-i} = i\sqrt{i} = e^{6\pi i/8}$ in $\mathbf{C}$. Then

$$\sqrt{i} = \cos(2\pi/8) + i\sin(2\pi/8) = \frac{\sqrt{2}(1 + i)}{2}.$$

Similarly, $\sqrt{-i} = \sqrt{2}(-1 + i)/2$. So $\alpha = 1 + i$ and $\beta = -1 + i$. Thus $\alpha - \beta = 2 \in \mathbf{Q}$ and $\alpha\beta = -2 \in \mathbf{Q}$. Following (e) we find

$$f(x) = [(x + \alpha)(x - \beta)][(x - \alpha)(x + \beta)] = (x^2 + 2x + 2)(x^2 - 2x + 2).$$

Variant: Here is a less conceptual and more elementary way, using the trick "complete the square, hope for a difference of squares":

$$x^4 + 4 = (x^4 + 4x^2 + 4) - 4x^2 = (x^2 + 2)^2 - (2x)^2 = (x^2 + 2x + 2)(x^2 - 2x + 2).$$

□