# Math 306 Topics in Algebra, Spring 2013
# Takehome final exam solutions

(1) (10 pts) Suppose $G$ is a finite group and $H$ a subgroup such that $|H| \nmid [G : H]!$. Prove that $H$ contains a nontrivial normal subgroup of $G$. (Hint: Define an action of $G$ on the set of cosets of $H$ in $G$ and look at the kernel of the associated permutation representation.)

*Solution:* Let $[G : H] = n$ and let $S$ be the set of cosets of $H$ in $G$. Thus $|S| = n$ and we have

$$|G| = |H| \cdot [G : H] = |H| \cdot n.$$

Now let $G$ act on $S$ by translation, namely define an action

$$\begin{aligned} G \times S &\longrightarrow S \\ (g, g'H) &\longmapsto g(g'H) = (gg')H. \end{aligned}$$

One then has the associated homomorphism

$$\begin{aligned} \phi\colon G &\longrightarrow \mathrm{Sym}(S) \cong S_n \\ g &\longmapsto \phi(g)(g'S) = (gg')H. \end{aligned}$$

(So $\phi$ simply permutes the conjugacy classes.)

Now $\ker \phi \subset H$ since if $\phi(g) = H$ (i.e. $\phi$ sends $g$ to the identity), then $\phi(g)(g'S) = (gg')H = H$ for all $g' \in G$ and in particular for $g' = 1$, in which case we must have $gH = H$. In other words, $g \in H$.

Since $\ker \phi$ is a normal subgroup, it now suffices to show that $\ker \phi$ is nontrivial. Since $\mathrm{im}\, \phi$ is a subgroup of $S_n$, we have that $|\mathrm{im}\, \phi|$ divides $|S_n| = n!$. We also know by the First Isomorphism Theorem that $|G|/|\ker \phi| = |\mathrm{im}\, \phi|$. But $|G| = n \cdot |H|$ so

$$n \cdot |H|/|\ker \phi| \,|\, n!$$

If kernel were trivial, the above would become $n \cdot |H||n!$ or $|H| \,|\, (n-1)!$. Further, this means that $|H|$ divides any multiple of $(n-1)!$ and in particular $|H|$ must divide $n!$. Since $n = [G : H]$, we then get

$$|H| \,|\, n! = [G : H]!,$$

which contradicts the hypothesis. Thus $\ker \phi$ must be nontrivial.

(2) (10 pts) Let $G$ be a group of order $pq$ where $p, q$ are primes with $p < q$ and $q \not\equiv 1 \pmod{p}$. Use representation theory to show that $G$ is abelian. (Hint: Use the fact that the number of one-dimensional representations of $G$ divides $|G|$.)

*Solution:* Let $d_1, ..., d_s$ be degrees of the irreducible representations of $G$. We know that $d_i$ divide $|G|$. From this, along with $p < q$ and

$$pq = |G| = d_1^2 + \cdots + d_s^2,$$

it follows that $d_i$is 1 or $p$ for all $i$. Let $n$ be the number of degree $p$ representations and let $m$ be the number of degree 1 representations. Then $pq = m + np^2$. Since $m$ divides $|G|$ (by the hint), $m \geq 1$ (there is at least the trivial representation), and $p|m$, we must have that $m = p$ or $m = pq$. If $m = p$, then $q = 1 + np$, contradicting that $q \not\equiv 1 \pmod{p}$. Therefore $m = pq$ and so all the irreducible representations of $G$ have degree one. Thus $G$ is abelian.

(Note: Using Sylow Theory, one can show that $G$ is in fact cyclic.)

(3) The following is the character table of a certain group $G$ of order 60. The numbers in brackets are the numbers of elements in the conjugacy classes of representatives $g_i \in G$, $\chi_i$ is the character of an irreducible representation

$\phi_i$, $\alpha = (1+\sqrt{5})/2$, and $\beta = (1-\sqrt{5})/2$:

| | $g_1 = e$ [1] | $g_2$ [20] | $g_3$ [15] | $g_4$ [12] | $g_5$ [12] |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 5 | $-1$ | 1 | 0 | 0 |
| $\chi_3$ | 4 | 1 | 0 | $-1$ | $-1$ |
| $\chi_4$ | 3 | 0 | $-1$ | $\alpha$ | $\beta$ |
| $\chi_5$ | $a$ | $b$ | $c$ | $d$ | $e$ |

(a) (3 pts) Determine the dimension of the representation $\phi_5$.
(b) (6 pts) Determine $\chi_5$.
(c) (6 pts) Show that $G$ is a simple group.

*Solution:*

(a) The dimensions must satisfy $|G| = 10 = 1^2 + 5^2 + 4^2 + 3^2 + a^2$ from which it follows that $a = 3$.
(b) Using orthogonality relations gives

$$3 + 20b + 15c + 12d + 12e = 0$$
$$5 \cdot 3 = 2 - b + 15c = 0$$
$$4 \cdot 3 + 20b - 12d - 21e = 0$$
$$5 \cdot 3 - 15c + 12\alpha d + 12\beta e = 0.$$

Solving this system gives $b = 0$, $c = -1$, $d = 1 - \alpha = \beta$, and $e = 1 - \beta = \alpha$.

(c) For no character (other than the identity) is it true that there is a conjugacy class such that the value of the character on that class is the same as the value of the identity on that class. Hence $|G|$ has no proper normal subgroups and is hence simple.

(4) (7 pts/part) Let $G$ be a finite group, let $g \in G$, and let $\chi$ be a character of $G$ associated to an $n$-dimensional representation $\phi$. Prove the following:
(a) If $g$ has order 2, then $\chi(g) \in \mathbb{Z}$ and $\chi(g) \equiv \chi(e) \pmod 2$.
(b) If $g$ has order 4 and $g$ is conjugate to $g^{-1}$, then $\chi(g) \in \mathbb{Z}$.

*Solution:*

(a) We can replace the matrix representing $\phi_g$ by a diagonal matrix with eigenvalues $\lambda_i$ of $\phi_g$ on the diagonal (there was a homework problem showing that this can be done). Since $g^2 = e$, the diagonal matrix also has to have order two and we thus have that $\lambda_i = \pm 1$ for all $i$. Thus

$$\chi(g) = \sum_{i=1}^{n} \lambda_i = \sum_{i=1}^{n} \pm 1 \in \mathbb{Z}.$$

Furthermore, $\lambda_i \pm 1 \equiv 1 \pmod 2$, so

$$\chi(g) = \sum_{i=1}^{n} \lambda_i = \sum_{i=1}^{n} \pm 1 \equiv \sum_{i=1}^{n} 1 \pmod 2 \equiv n \pmod 2 = \chi(e) \pmod 2.$$

(b) Now we have $\lambda_i^4 = 1$ and so $\lambda_i = \pm 1, \pm i$. Since $g$ and $g^{-1}$ are conjugate, we have $\chi(g) = \chi(g^{-1}) = \overline{\chi(g)}$, where $\overline{\chi(g)}$ means the complex conjugate of $\chi(g)$ (we showed the last equality on a homework). Thus $\chi(g)$ equals its complex conjugate, which means $\chi(g) \in \mathbb{R}$.
Thus in $\chi(g) = \sum_{i=1}^{n} \lambda_i$, for every $\lambda_i = \pm i$, there must be a $\lambda_j = \mp i$ and the two cancel out. Therefore $\sum_{i=1}^{n} \lambda_i$ is really a sum of $\pm 1$'s, and is hence an integer.

(5) (5 pts/part) Section 10.1, problem 8 (p. 344). (Note: In part (a), you can assume $R$ is commutative since that is a part of the definition of an integral domain.)

*Solution:*

(a) Suppose $R$ is an integral domain. It suffices to show that $\mathrm{Tor}(M)$ is nonempty and that $x+ry \in \mathrm{Tor}(M)$ for all $x, y \in \mathrm{Tor}(M)$ and $r \in R$. Since $r \cdot 0 = 0$ for any $r$, $0 \in \mathrm{Tor}(M)$ so $\mathrm{Tor}(M)$ is nonempty. Now let $x, y \in \mathrm{Tor}(M)$, $r \in R$. Since $x, y$ are torsion elements, there exist $s, t \in R$ such that $sx = ty = 0$. Then

$$\begin{aligned}(st)(x+ry) &= (st)x + ((st)r)y \\ &= (ts)x + ((sr)t)y \\ &= t(sx) + (sr(ty) \\ &= t \cdot 0 + (sr) \cdot 0 \\ &= 0\end{aligned}$$

Because $R$ is an integral domain and $s, t$ are nonzero, $st$ is nonzero. Thus $(st)(x+ry) = 0$ for a nonzero element $st \in R$. Thus $x + ry$ is a torsion element.

(b) Take $R = M = \mathbb{Z}/6\mathbb{Z}$. Then 2 and 3 are torsion elements (since $3 \cdot 2 = 2 \cdot 3 = 6 = 0$). However, $2 + 3 = 5 \notin \mathrm{Tor}(M)$ so $\mathrm{Tor}(M)$ is not closed under addition.

(c) Suppose $s$ and $r$ are zero divisors in $R$ such that $sr = 0$. Then, for any nonzero module $M$ with a nonzero element $m$, either $rm = 0$ or $rm \neq 0$. In the first case, $m \in \mathrm{Tor}(M)$ since $m$ is nonzero. In the second case, we get that $rm \in \mathrm{Tor}(M)$ since $s(rm) = (sr)m = 0 \cdot m = 0$. In either case, there exists a nonzero element of $M$ that is in $\mathrm{Tor}(M)$.

(6) (a) (7 pts) Section 10.2, first part of problem 4 (p. 350)
(b) (7 pts) Section 10.2, second part of problem 4 (p. 350)
(c) (5 pts) Section 10.2, problem 5 (p. 350)

*Solution:*

(a) First suppose that $\phi_a$ is a well-defined $\mathbb{Z}$-module homomorphism. In the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$, $\overline{n} = \overline{0}$. Hence, because $\phi_a$ is well-defined,

$$na = \phi_a(\overline{n}) = \phi_a(\overline{0}) = 0a = 0.$$

For the converse statement, suppose that $na = 0$ and consider the map $\psi\colon \mathbb{Z} \to A$ defined by $\psi(k) = ka$ for all $k \in \mathbb{Z}$. This is clearly a group homomorphism. Furthermore, since

$$\psi(nk) = \psi(kn) = (kn)a = k(na) = k0 = 0,$$

we have that the subgroup $n\mathbb{Z}$ is contained in the kernel of $\psi$. Thus $\psi$ descends to the quotient $\mathbb{Z}/n\mathbb{Z}$. That is, there exists a unique group homomorphism $\phi_a\colon \mathbb{Z}/n\mathbb{Z} \to A$ such that $\phi_a(\overline{k}) = \psi(k) = ka$. Moreover, since

$$\phi_a(k_1\overline{k_2}) = \phi_a(\overline{k_1k_2}) = (k_1k_2)a = k_1(k_2a) = k_1\phi_a(\overline{k_2}),$$

for all $k_1 \in \mathbb{Z}$ and $\overline{k_2} \in \mathbb{Z}/n\mathbb{Z}$, it follows that $\phi_a$ is a $\mathbb{Z}$-module homomorphism.

(b) Let $\phi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$ and let $a = \phi(1)$. For any $k \in \mathbb{Z}^+$, $\phi$ being a $\mathbb{Z}$-module homomorphism implies

$$\phi(\overline{k}) = \phi\left(\sum_{i=1}^{k} \overline{1}\right) = \sum_{i=1}^{k} \phi(\overline{1}) = \sum_{i=1}^{k} a = ka.$$

Thus $\phi = \phi_a$ with $\phi_a$ as define in the previous part. Also by the previous part, $\phi = \phi_a$ is a $\mathbb{Z}$-module homomorphism if an only if $na = 0$. Therefore the function

$$\psi\colon \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \longrightarrow A_n$$

defined by $\psi(\phi_a) = a$ is a bijection. Furthermore $\psi$ is a $\mathbb{Z}$-module homomorphism since

$$\psi(\phi_a + \phi_{a'}) = \psi(\phi_{a+a'}) = a + a' = \psi(\phi_a) + \psi(\phi_{a'})$$

and

$$\psi(k\phi_a) = \psi(\phi_{ka}) = ka = k\psi(\phi_a).$$

for all $k \in \mathbb{Z}$, and all $\phi_a, \phi_{a'} \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$. Hence $\psi$ is an isomorphism.

(c) Let $a \in \mathbb{Z}/21\mathbb{Z}$ and let $\phi_a \colon \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z}$ denote the map defined by $\phi_a(\overline{k}) = ka$. Then by the previous part, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}) \cong \{\phi_{\overline{0}}, \phi_{\overline{7}}, \phi_{\overline{14}}\}$ since $\overline{0}$, $\overline{7}$ and $\overline{14}$ are the only elements of $\mathbb{Z}/21\mathbb{Z}$ that are $\overline{0}$ when multiplied by $30$ (this can be done by brute force or by more clever number-theoretic methods).

(7) (5 pts) Suppose $M$ is an $R$-module and $f \colon M \to M$ is an $R$-module homomorphism satisfying $f \circ f = f$. Use a short exact sequence to show that $M = \ker f \oplus \operatorname{im} f$.

*Solution:* Consider the standard short exact sequence arising from $f$:

$$0 \longrightarrow \ker f \longrightarrow A \xrightarrow{f} \operatorname{im} f \longrightarrow 0$$

Given $b \in \operatorname{im} f$, there exists (by definition of image) $a \in A$ such that $f(a) = b$. Then $f(b) = f(f(a)) = f(a) = b$ since $f \circ f = f$. Thus $(f \circ f_{\operatorname{im} f})(y) = y$ and so $f \circ f_{\operatorname{im} f} = Id_{\operatorname{im} f}$. In other words, $f$ has an inverse, namely $f_{\operatorname{im} f}$, and thus the sequence is split exact. Hence (by a homework problem), $M = \ker f \oplus \operatorname{im} f$.