Algebra Qual Fall 2018

Problem 1

Statement (10 points)**.** Let G be a finite group whose order is divisible by a prime number p. Let P be a normal p-subgroup of G (so $|P| = p^c$ for some c).

(a) Show that P is contained in every Sylow p-subgroup of G.

(b) Let M be a maximal proper subgroup of G. Show that either $P \subseteq M$ or $|G/M| = p^b$ for some $b \leq c$.

Solution. **(a)** Write $|G| = mp^n$ where $p \nmid m$, with $|P| = p^k$. If $k = n$ then P is a sylow p-subgroup and its normality implies it is the unique one since all sylow p-subgroups are conjugate.

Now suppose $k < n$ and consider the quotient G/P. This has order mp^{n-k}. Since sylow subgroups always exist there is a sylow p subgroup $P' \leq G/P$ and this group has order p^{n-k} since thats the largest power of p dividing G/P. Now let $q : G \to G/P$ be the quotient. Then

$$\left|q^{-1}\left(P'\right)\right| = \left|P'\right| \cdot |P| = p^n$$

so by the lattice theorem $Q := q^{-1}\left(P'\right)$ is a sylow p-subgroup containing P. Now by normality of P

$$P = gPg^{-1} \subseteq gQg^{-1}, \text{ for all } g \in G.$$

Then since sylow subgroups are conjugate gQg^{-1} is an arbitrary sylow p-subgroup thus P is contained in the intersection of all of them.

(b) Suppose that $P \not\subseteq M$. Then as P is normal MP is a group, and M is properly contained in MP since there is a $p \in P \setminus M$ and $p \in MP$. Then by maximality of M we see that $MP = G$. Then

$$G/M = MP/M = P/M, \text{ as sets of cosets, not as quotient groups.}$$

In otherwords every coset gM has a representative in P, and $|G/M| = |P/M|$.

Now let P act on P/M by left multiplication. Note that this action is transitive since for example $p'p^{-1} \cdot pM = p'M$. Then the orbit stabilizer theorem yields

$$|P| = |P/M| \cdot |\text{Stab}\,(M)|\,.$$

Then $\text{Stab}\,(M) = P \cap M$ since $pM = M$ iff $p \in M$. Then $|P \cap M|$ is a proper subgroup of P since P is not contained in M thus $|P \cap M| = p^k$ for $k < c$ and

$$|P/M| = p^{c-k}$$

where since $k \geq 0$ we have $c - k \leq c$. □

Problem 2

Statement (10 points). **(a)** Suppose the group G acts on the set X. Show that the stabilizers of elements in the same orbit are conjugate.

(b) Let G be a finite group and let H be a proper subgroup. Show that the union of the conjugates of H is strictly smaller than G, i.e.

$$\bigcup_{g \in G} gHg^{-1} \subsetneq G.$$

(c) Suppose G is a finite group acting transitively on a set S with at least 2 elements. Show that there is an element of G with no fixed points in S.

Solution. **(a)** Suppose $x, y \in O_x$. That is there is $g \in G$ such that $g \cdot x = y$. Let $F(x)$ denote the stabilizer of x. We claim

$$gF(x)\, g^{-1} = F(y).$$

Indeed suppose $h \in F(x)$. Then

$$ghg^{-1} \cdot y = gh \cdot \left(g^{-1} \cdot y\right) = gh \cdot x = g \cdot (h \cdot x) = g \cdot x = y$$

so $gF(x)\, g^{-1} \subseteq F(y)$. Now to see the map is surjective suppose $h \in F(y)$. We claim $g^{-1}hg \in F(x)$ and thus its image under $g(\cdot)\, g^{-1}$ is precisely h. We check the same equality

$$g^{-1}hg \cdot x = g^{-1}h \cdot y = g^{-1} \cdot y = x$$

as desired.

(b) This about the size of the union of conjugate subgroups being strictly smaller then the union of cosets because they have an intersection.

Let $g_1H, \ldots, g_kH$ be the distinct cosets of H i.e. $k = [G : H]$. Then the distinct conjugate subgroups are $g_1Hg_1^{-1}, \ldots, g_kHg_k^{-1}$. Then

$$\begin{aligned}\left|\bigcup_{i=1}^{k} g_iHg_i^{-1}\right| &= \left|\{e\} \cup \bigcup_{i=1}^{k} g_iHg_i^{-1} \setminus \{e\}\right| \\ &\leq 1 + \sum_{i=1}^{k} (|H| - 1) = 1 + k\,|H| - k \\ &= |G| - k + 1\end{aligned}$$

since the identity lands in every conjugate subgroup. Since H is proper $k \geq 2$ so the above quantity is less then G.

Remark. To formalize

$$(\#\text{conjugate subgroups of } H) \leq (\#\text{cosets of } H)$$

show that the map $gH \mapsto gHg^{-1}$ is well defined. It obviously surjective so we get the right inequality.

(c) This is straight from burnsides lemma. Recall $|S/G|$ is the number of orbits under the action of G. Then we have

$$1 = |S/G| = \frac{1}{|G|} \sum_{g \in G} |S^g|.$$

Then $|G| = \sum_{g \in G} |S^g|$. Now note that $S^e = S$ so we may write

$$|G| = |S| + \sum_{g \neq e} |S^g| \geq |S| + |G| - 1$$

so $|S| \leq 1$ a contradiction. □

Problem 3

Statement (10 points)**.** Let $F \subset K \subset L$ be finite degree field extensions. For each of the following assertions, give a proof or a counterexample.

(a) If L/F is Galois, then so is K/F.

(b) If L/F is Galois, then so is L/K.

(c) If K/F and L/K are both Galois, then so is L/F.

Solution. **(a)** False for example if L is the splitting field for $x^4 - 5$ (which is irred over $\mathbb{Q}$ by eisensteins with $p = 5$) then $\mathbb{Q}\left(5^{1/4}\right)$ is a subfield, but it is not Galois since it is not normal. It contains one root of $x^4 - 5$ but not all.

(b) This is true. Let $f(x) \in K[x]$ be the minimal polynomial of some $\alpha \in L$. Then since L/F is Galois (algebraic since the extension is finite) there is a minimal polynomial over F say $g(x) \in F[x]$. Now $g(x)$ is still an annihilating polynomial in $K[x]$ so by minimality $f(x) \mid g(x)$. Then since $g(x)$ splits in L so does $f(x)$, and since $g(x)$ has distinct roots in L so does $f(x)$.

(c) No. Consider the extensions

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt[4]{2}\right).$$

$\mathbb{Q}\left(\sqrt{2}\right)$ is Galois over $\mathbb{Q}$ since its the splitting for the irreducible poly $x^2 - 2 \in \mathbb{Q}[x]$. Also $\mathbb{Q}\left(\sqrt[4]{2}\right)$ is Galois over $\mathbb{Q}\left(\sqrt{2}\right)$ since it is the splitting field for $\left(x^2 - \sqrt{2}\right) \in \mathbb{Q}\left(\sqrt{2}\right)[x]$, but $\mathbb{Q}\left(\sqrt[4]{2}\right)$ is not Galois over $\mathbb{Q}$ because it isn't normal. It contains one root of $x^4 - 2$, but not all. □

Problem 4

Statement (10 points)**.** Let V be a finite dimensional vector space over a field (the field is not necessarily algebraically closed). Let $\phi : V \to V$ be a linear transformation. Prove that there exists a decomposition of V as $V = U \oplus W$, where U and W are ϕ-invariant subspaces of V, $\phi|_U$ is nilpotent, and $\phi|_W$ is nonsingular.

Solution.

Attempt

Consider the exact sequence

$$0 \to \ker \phi \to V \xrightarrow{\phi} \operatorname{im} \phi \to 0.$$

Since $\operatorname{im}\phi$ is vector space it is a free module so there exists a splitting map $h : \operatorname{im}\phi \to V$ such that $\phi \circ h = \mathrm{id}_{\operatorname{im}\phi}$ i.e. the restriction of ϕ to $\operatorname{im} h$ is surjective onto $\operatorname{im}\phi$. Now since there is a splitting map we get that

$$V = \ker\phi \oplus \operatorname{im} h$$

so $\ker\phi$ and $\operatorname{im} h$ are disjoint and thus $\phi \upharpoonright \operatorname{im} h$ is in fact an isomorphism so must be non-singular. Of course $\phi \upharpoonright \ker\phi$ is the zero map so nilpotent in a trivial sense.

Problem: The subspaces above might not be invariant.

Proof

Consider the chains

$$\ker\phi \subseteq \ker\phi^2 \subseteq \cdots$$
$$\operatorname{im}\phi \supseteq \operatorname{im}\phi^2 \supseteq \cdots$$

since the space is finite dimensional these chains must converge. Pick k large enough so that both chains converge. That $\operatorname{im}\phi^k = \operatorname{im}\phi^{k+1}$ and $\ker\phi^k = \ker\phi^{k+1}$. We claim that $\operatorname{im}\phi^k \cap \ker\phi^k = \{e\}$. Indeed suppose $v \in \operatorname{im}\phi^k \cap \ker\phi^k$. Then $v = \phi^k(u)$ and since $\phi^k(v) = 0$ we see that

$$\phi^k(v) = \phi^{2k}(u) = 0$$

thus $u \in \ker\phi^{2k} = \ker\phi^k$ so that $\phi^k(u) = v = 0$. Then we have a direct sum

$$\operatorname{im}\phi^k \oplus \ker\phi^k \subseteq V$$

thus by rank nullity

$$\dim\left(\operatorname{im}\phi^k \oplus \ker\phi^k\right) = \dim\operatorname{im}\phi^k + \dim\ker\phi^k = \dim V$$

so the direct sum is the entire space as desired.

Now since the chains have converged both of these are invariant subspaces for ϕ. That is

$$\phi\left(\operatorname{im}\phi^k\right) = \operatorname{im}\phi^{k+1} = \operatorname{im}\phi^k$$

and if $v \in \ker\phi^k$ then $\phi(v) \in \ker\phi^k$ since $\phi^k(\phi(v)) = \phi\left(\phi^k(v)\right) = \phi(0) = 0$.

Then $\phi \upharpoonright \operatorname{im}\phi^k$ is an isomorphism since it is surjective and disjoint from the kernel of ϕ^k which contains the kernel of ϕ.

$\phi \upharpoonright \ker\phi^k$ is nilpotent since ϕ^k is zero on the subspace.

Remark. For the argument about chains note that the containments are proper iff the dimension actually drops since if the dimension doesn't drop then the subspace contains a basis for the original space so they must be equal. Alternatively there is a more general theory of Artinian modules and vector spaces are that. That ϕ is an isomorphism can also be justified from the fact that any surjective operator on a finite dimensional space must be injective. This is because rank nullity yields the dimension of the kernel must be 0.

□

Problem 5

Statement (10 points)**.** Let A be an $n \times n$ matrix.

(a) Suppose that v is a column vector such that the set $\left\{v, Av, \ldots, A^{n-1}v\right\}$ is linearly independent. Show that any matrix B that commutes with A is a polynomial in A.

(b) Show that there exists a column vector v such that the set $\left\{v, Av, \ldots, A^{n-1}v\right\}$ is linearly independent if and only if the characteristic polynomial of A equals the minimal polynomial of A.

Solution. **(a)** Since $\{v, Av, \ldots, A^{n-1}v\}$ is linearly independent and has n elements, it's a basis for F^n, i.e.

$$F^n = \operatorname{span}\{v, Av, \ldots, A^{n-1}v\}.$$

Suppose $AB = BA$. Let $u \in F^n$ be arbitrary and write $u = \sum_{i=0}^{n-1} a_i A^i v$. Then

$$B(u) = B\left(\sum_{i=0}^{n-1} a_i A^i v\right) = \sum_{i=0}^{n-1} a_i A^i (Bv).$$

Say $Bv = \sum_{j=0}^{n-1} b_j A^j v$. Then

$$\begin{aligned} B(u) &= \sum_{i=0}^{n-1} a_i A^i \left(\sum_{j=0}^{n-1} b_j A^j v\right) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_i b_j A^i A^j v \\ &= \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} b_j A^j (a_i A^i v) = \sum_{j=0}^{n-1} b_j A^j u. \end{aligned}$$

So if $f(x) = \sum_{j=0}^{n-1} b_j x^j$, then $B = f(A)$.

(b) For the converse ($\implies$ direction) also consider the contrapositive. Suppose $m_A \neq \chi_A$. Then since $m_A \mid \chi_A$ and they are both monic this can only happen if $\deg m_A < \deg \chi_A$. Then $\deg m_A \leq n-1$ so we may write $m_A(x) = \sum_{i=0}^{n-1} m_i x^i$. Now $m_A(A) = 0$ so for any $v \in F^n$ we have

$$m_A(A)\, v = m_0 v + m_1 Av + \cdots + m_{n-1} A^{n-1} v = 0$$

so $\mathcal{B}_v$ is not independent for any v.

For the $\impliedby$ direction view F^n as an $F[x]$-module via $x \cdot w := Aw$; call this module (F^n, A). By the structure theorem for finitely generated torsion modules over the PID $F[x]$, there is an invariant factor decomposition

$$(F^n, A) \cong \bigoplus_{i=1}^{m} \frac{F[x]}{(d_i(x))}$$

with $d_1(x) \mid d_2(x) \mid \cdots \mid d_m(x)$, where the largest invariant factor $d_m(x)$ is the minimal polynomial $m_A(x)$, and the product $d_1(x) \cdots d_m(x)$ is the characteristic polynomial $\chi_A(x)$.

Suppose $m_A = \chi_A$. Comparing degrees in the product $d_1 \cdots d_m = \chi_A = m_A = d_m$ forces $m = 1$: there is only one invariant factor. So

$$(F^n, A) \cong \frac{F[x]}{(d(x))}, \quad d(x) = m_A(x) = \chi_A(x), \quad \deg d = n.$$

Let $\phi : F[x]/(d(x)) \to F^n$ be this $F[x]$-module isomorphism. As an F-vector space, $F[x]/(d(x))$ has basis $\left\{1, x, \ldots, x^{n-1}\right\}$ since $\deg d = n$.

Let $v = \phi(1)$. Since ϕ is an $F[x]$-module map and the module structure on F^n is given by A, we have $\phi\left(x^i\right) = x^i \cdot \phi(1) = A^i v$. So

$$\phi(1), \phi(x), \ldots, \phi\left(x^{n-1}\right) = v, Av, \ldots, A^{n-1}v,$$

and since ϕ is an isomorphism it carries the basis $\left\{1, x, \ldots, x^{n-1}\right\}$ to a basis $\left\{v, Av, \ldots, A^{n-1}v\right\}$ of F^n. In particular this set is independent, as desired.

Alternate proof of $\implies$ direction: Consider again F^n as a $F[x]$-module

$$(F^n, A) \cong \bigoplus_{i=1}^{m} \frac{F[x]}{(d_i(x))}$$

with isomorphism $\phi : (F^n, A) \to F^n$. Then suppose

$$\left\{v, Av, \ldots, A^{n-1}v\right\}$$

is a basis for F^n. Then $\phi^{-1}(v)$ generates F^n as a $F[x]$-module i.e. it is cyclic isomorphic to $F[x]/\langle d(x)\rangle$ for some d. Then we can't have more then one invariant factor $m = 1$ and $\chi_A = M_A$. □

Problem 6

Statement (10 points)**.** Let R be a commutative ring, and let M be an R-module. An R-submodule N of M is maximal if there is no R-module P with $N \subsetneq P \subsetneq M$.

(a) Show that an R-submodule N of M is maximal iff M/N is a simple R-module: i.e., M/N is nonzero and has no proper, nonzero R-submodules.

(b) Let M be a $\mathbb{Z}$-module. Show that a $\mathbb{Z}$-submodule N of M is maximal iff $\#M/N$ is a prime number.

(c) Let M be the $\mathbb{Z}$-module of all roots of unity in $\mathbb{C}$ under multiplication. Show that there is no maximal $\mathbb{Z}$-submodule of M.

Solution. **(a)** Recall the lattice theorem for modules. That is submodules of M/N correspond bijectively to submodules of M containing N. Then if N is maximal there are no proper submodules of M containing it so there are no proper submodules of M/N. Similarly if M/N is simple then there must not be any proper submodules of M containing N so N must be maximal.

(b) By part (a) N is maximal iff M/N is simple. Then it suffices to show that the non-zero simple $\mathbb{Z}$-modules are precisely C_p for some prime p. Then suppose M is a non-zero simple $\mathbb{Z}$-module. Then it has a nonzero element $v \in M$ and $\langle v\rangle \subseteq M$ is a submodule. Since M is simple this submodule is not-proper and $\langle v\rangle = M$. Now suppose M is infinite. Then v has infinite order so $\langle 2v\rangle$ is a proper submodule. Then M must be finite, and thus is a finite cyclic group of order say $m = |M|$. Then for any $d \mid m$ we know $\left\langle \frac{m}{d} v\right\rangle$ is a proper submodule. Then M is simple iff it has no proper non-trivial divisors i.e. if m is prime.

(c) More explicitly

$$M = \{z \in \mathbb{C} : z^n = 1 \text{ for some } n \in \mathbb{N}\}.$$

Suppose N is maximal submodule so that M/N is simple. Then this has prime order p. Then every coset satisfies

$$(zN)^p = z^p N = N$$

i.e. every $z \in M$ satisfies $z^p \in N$. We will show towards contradiction that $N = M$. Indeed suppose $z = e^{2\pi ik/n}$ is an n-th root of unity. Then $w = e^{2\pi ik/pn}$ is a pn-th root of unity hence $w \in M$. Then

$$z = w^p \in N$$

as desired.

Remark. Apparently there is some theory to this question. Something about this notion of divisible modules.

Divisible group – Wikipedia

□

Problem 7

Statement (10 points)**.** Let R be a commutative ring.

(a) Let $r \in R$. Show that the map $r\bullet : R \to R$ by $x \mapsto rx$ is an R-module endomorphism of R.

(b) We say that r is a zero-divisor if $r\bullet$ is not injective. Show that if r is a zero-divisor and $r \neq 0$, then the kernel and image of R each consist of zero-divisors.

(c) Let $n \geq 2$ be an integer. Show: if R has exactly n zero-divisors, then $\#R \leq n^2$.

(d) Show that up to isomorphism there are exactly two commutative rings R with precisely 2 zero-divisors. You may use without proof the following fact: every ring of order 4 is isomorphic to exactly one of the following: $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}[t]/(t^2+t+1)$, $\mathbb{Z}/2\mathbb{Z}[t]/(t^2-t)$, $\mathbb{Z}/2\mathbb{Z}[t]/(t^2)$.

Solution. **(a)** We check it preserves addition and scaling. Denote the map instead by $m_r(x)$. Then

$$m_r(a+b) = r(a+b) = ra + rb = m_r(a) + m_r(b)$$

and if $r' \in R$ then

$$m_r(r'a) = rr'a = r'(ra) = r'm_r(a)$$

so indeed multiplication by r is an R-module endomorphism.

(b) Note that

$$\ker m_r = \{a \in R : ra = 0\}$$
$$\operatorname{im} m_r = \{ra : a \in R\}$$

Now suppose $r \neq 0$. Then if $a \in \ker m_r$ we have that

$$0 = ra = ar = m_a(r)$$

so $r \in \ker m_a$ and m_a is not injective hence a is a zero divisor. Now suppose r is not injective so there is $x \in \ker m_r$ i.e. $rx = 0$. Then if $ra \in \operatorname{im} m_r$ we see that

$$m_{ra}(x) = rax = a(rx) = a0 = 0$$

so ra is a zero divisor as well.

(c) Let $r \in R$ be a zero divisor. Then the 1st isomorphism theorem gives an isomorphism

$$R/\ker m_r \cong \operatorname{im} m_r.$$

Then since the images consists of zero divisors in R and there are at most n the image has size at most n. Then from our isomorphism this is precisely the number of distinct cosets of $\ker m_r$. Then also not that since $\ker m_r$ consists of zero divisors it also has size at most n so all the cosets are finite with size at most n. Then we may write r as a union of its distinct cosets

$$|R| = \sum_{i=1}^{n} |k_i + \ker m_r| = \sum_{i=1}^{n} |\ker m_r| \leq \sum_{i=1}^{n} n = n^2.$$

(d) Form part (c) $|R| \leq 4$ so we only need to check rings of size at most 4 and at least 2.

Every ring has 1 zero divisor namely 0 so we just need to consider when the ring has precisely 1 more.

Size 2: The ring $\{0, a\}$ where $a^2 = 2a = 0$ is a ring with precisely two zero divisors.

Size 3: Suppose $\{0, a, b\}$ is a ring. Since $a, b \neq 0$ we must have $a = -b$ so one is a zero divisor iff the other is and there are no rings of size 3 with two zero divisors.

Size 4: We consider the hint. Note that since $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ is a field $\mathbb{F}_2[x]$ is a PID hence has no zero divisors. Then $\mathbb{F}_2[x]/\langle p(x)\rangle$ has zero divisors iff p factors. Then we consider each polynomial.

- $t^2 + t + 1$. This is irred in $\mathbb{F}_2$ by checking for roots thus $\frac{\mathbb{F}_2[t]}{\langle t^2+t+1\rangle}$ is a field and has no zero divisors.
- $t^2 - t = t(t-1)$ factors into distinct factors so the quotient two zero divisors which is one to many.
- $t^2 = t \cdot t$ makes t nilpotent hence adds only one zero divisor so this is the correct ring.

□