Math 661 **Fall 2013**
Final Exam **Drew Armstrong**

---

1. Let G be a group and consider the group homomorphism $\varphi : G \to \text{Aut}(G)$ which sends $g \in G$ to the map $x \mapsto gxg^{-1}$ in $\text{Aut}(G)$. The orbits $\text{Orb}(x) := \{gxg^{-1} : g \in G\}$ are called **conjgacy classes** and the stabilizers $C(x) := \{g \in G : gxg^{-1} = x\}$ are called **centralizers**.

(a) For all $x \in G$ prove that the map $gxg^{-1} \mapsto gC(x)$ is well-defined and is a bijection of sets $\text{Orb}(x) \to G/C(x)$.

Proof. Fix $x \in G$. Then for all $g, h \in G$ we have

$$\begin{aligned} gxg^{-1} = hxh^{-1} &\iff h^{-1}gxg^{-1}h = x \\ &\iff (h^{-1}g)x(h^{-1}g)^{-1} = x \\ &\iff h^{-1}g \in C(x) \\ &\iff gC(x) = hC(x). \end{aligned}$$

The right arrows prove that the map is well-defined and the left arrows prove that the map is injective. The map is obviously surjective. □

(b) Define the **center** by $Z(G) := \{g \in G : gx = xg \text{ for all } x \in G\}$. If G is **finite**, prove that there exist group elements $x_i \in G$ such that

$$|G| = |Z(G)| + \sum_i |G|/|C(x_i)|.$$

[Hint: Note that $C(x) = G$ if and only if $x \in Z(G)$.]

Proof. Let G be a finite group. By part (a) and Lagrange's Theorem we know that $|\text{Orb}(x)| = |G|/|C(x)|$ for all $x \in G$. If we let $x_1, x_2, x_3, \ldots$ be representatives of the conjugacy classes then we can write G as a disjoint union:

$$\begin{aligned} G &= \sqcup_i \text{Orb}(x_i) \\ |G| &= \sum_i |\text{Orb}(x_i)| \\ |G| &= \sum_i |G|/|C(x_i)|. \end{aligned}$$

Finally, note that $|G|/|C(x)| = 1$ if and only if $x \in Z(G)$. Using this we can take the singleton conjugacy classes out of the sum to get

$$\begin{aligned} |G| &= (1 + 1 + \cdots + 1) + \sum_i |G|/|C(x_i)| \\ |G| &= |Z(G)| + \sum_i |G|/|C(x_i)|, \end{aligned}$$

where the sum on the right is now over the **nontrivial** conjugacy classes. □

(c) Now let p be **prime** and let $|G| = p^2$. Use part (b) to prove that p divides $|Z(G)|$.

Proof. Let p be prime and assume that $|G| = p^2$. Consider the Class Equation from (b). If $|G|/|C(x_i)| \neq 1$ then Lagrange says that $|G|/|C(x_i)| = p$ or p^2. In either case, p divides $|G|/|C(x_i)|$ and hence p divides the sum on the right side. Since p also divides $|G|$ we conclude that p divides $|Z(G)|$. □

(d) Use part (c) to prove that G is abelian. [Hint: Prove that $G/Z(G)$ is cyclic.]

Proof. Since p divides $|Z(G)|$ we have $|G|/|Z(G)| = 1$ or p. In either case we see that $G/Z(G)$ is cyclic, say $G/Z(G) = \langle xZ(G)\rangle$. We claim that this implies that G is abelian. Indeed, consider any $g, h \in G$. Since g and h are contained in some cosets of $Z(G)$ and every coset looks like $(xZ(G))^k = x^k Z(G)$ for some $k \in \mathbb{Z}$ we conclude that $g = x^k z$ and $h = x^\ell z'$ for some $k, \ell \in \mathbb{Z}$ and $z, z' \in Z(G)$. Finally we have

$$gh = x^k z x^\ell z' = x^k x^\ell z z' = x^{k+\ell} z' z = x^{\ell+k} z' z = x^\ell x^k z z' = x^\ell z' x^k z = hg.$$

We conclude that G is abelian. □

(e) Finally, if G is **not cyclic**, use part (d) to prove that $G \approx \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. [Hint: Choose $1 \neq x \in G$. Since $\langle x\rangle \neq G$ there exists $y \in G - \langle x\rangle$. Prove that $G = \langle x\rangle \times \langle y\rangle$ by showing $\langle x\rangle \cap \langle y\rangle = 1$, and $\langle x\rangle\langle y\rangle = G$.]

Proof. Again suppose that $|G| = p^2$ and assume that G is not cyclic. Then there exists $1 \neq x \in G$ such that $\langle x\rangle \neq G$. Choosing $y \in G - \langle x\rangle$ gives us two cyclic subgroups $\langle x\rangle$ and $\langle y\rangle$. Note that $|\langle x\rangle| = |\langle y\rangle| = p$ by Lagrange because neither is trivial or equal to the full group. Hence $\langle x\rangle \approx \langle y\rangle \approx \mathbb{Z}/p\mathbb{Z}$. We claim that $G = \langle x\rangle \times \langle y\rangle$. Indeed, by Lagrange the intersection has size 1 or p. If $|\langle x\rangle \cap \langle y\rangle| = p$ then we have $\langle x\rangle = \langle x\rangle \cap \langle y\rangle = \langle y\rangle$, contradiction. Finally, note that $G = \langle x\rangle\langle y\rangle$. This follows, for example, because $\langle x\rangle\langle y\rangle$ **properly** contains $\langle x\rangle$. Since $|\langle x\rangle\langle y\rangle|$ divides p^2 and is strictly greater than p we have $|\langle x\rangle\langle y\rangle| = p^2$. □

2. Consider the general linear group $G = GL(n, K)$ over a field K. Let P be the **subset**

$$P := \left\{ \left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array} \right) \right\} \subseteq G$$

where A is $r \times r$ and B is $(n-r) \times (n-r)$.

(a) Prove that P is a **subgroup** of G. [Hint: Find the inverse of an element of P.]

Proof. Consider the general element of P. Since it is invertible the left r columns must be independent, hence $A \in GL(r, K)$. Similarly, the bottom $n-r$ rows must be independent, hence $B \in GL(n-r, K)$. [Remark: You didn't need to check this.] To show that P is a subgroup of G we first note that it is closed under multiplication:

$$\left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array} \right) \left(\begin{array}{c|c} A' & C' \\ \hline 0 & B' \end{array} \right) = \left(\begin{array}{c|c} AA' & AC' + CB' \\ \hline 0 & BB' \end{array} \right)$$

Then solving the previous equation for $AA' = I$, $BB' = I$ and $AC' + CB' = 0$ shows us that $A' = A^{-1}$, $B' = B^{-1}$, and $AC' = -CB' \Rightarrow C' = A^{-1}CB^{-1}$. Hence P is closed under inversion:

$$\left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array} \right)^{-1} = \left(\begin{array}{c|c} A^{-1} & -A^{-1}CB^{-1} \\ \hline 0 & B^{-1} \end{array} \right).$$

□

(b) Let L be the **subset**

$$L := \left\{ \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) \right\} \subseteq P.$$

Prove that L is a **subgroup** of P isomorphic to $GL(r, K) \times GL(n-r, K)$.

Proof. We can identify $GL(r, K)$ and $GL(n-k, K)$ with the subgroups

$$G_r := \left\{ \left(\begin{array}{c|c} A & 0 \\ \hline 0 & I \end{array} \right) \right\} \qquad \text{and} \qquad G_{n-r} := \left\{ \left(\begin{array}{c|c} I & 0 \\ \hline 0 & B \end{array} \right) \right\}.$$

We clearly have $G_r \cap G_{n-r} = 1$. Next note that $L = G_r G_{n-r}$ because

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & I \end{array} \right) \left(\begin{array}{c|c} I & 0 \\ \hline 0 & B \end{array} \right)$$

and finally note that $G_r G_{n-r} = G_r G_{n-r}$ because

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & I \end{array} \right) \left(\begin{array}{c|c} I & 0 \\ \hline 0 & B \end{array} \right) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & B \end{array} \right) \left(\begin{array}{c|c} A & 0 \\ \hline 0 & I \end{array} \right).$$

We conclude that $L = G_r \times G_{n-r}$. ◻

(c) Prove that the map $\varphi : P \to L$ defined by

$$\left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array} \right) \mapsto \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right)$$

is a group homomorphism. Let $U \lhd P$ denote the kernel of φ.

Proof. The map is a homomorphism because

$$\begin{aligned}
\varphi\left(\left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array} \right) \left(\begin{array}{c|c} A' & C' \\ \hline 0 & B' \end{array} \right) \right) &= \varphi\left(\left(\begin{array}{c|c} AA' & AC' + CB' \\ \hline 0 & BB' \end{array} \right) \right) \\
&= \left(\begin{array}{c|c} AA' & 0 \\ \hline 0 & BB' \end{array} \right) \\
&= \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) \left(\begin{array}{c|c} A' & 0 \\ \hline 0 & B' \end{array} \right) \\
&= \varphi\left(\left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array} \right) \right) \varphi\left(\left(\begin{array}{c|c} A' & C' \\ \hline 0 & B' \end{array} \right) \right)
\end{aligned}$$

◻

(d) Prove that U is isomorphic to the **additive** group $\mathrm{Mat}_{r,n-r}(K)$ of $r \times (n-r)$ matrices.

Proof. Note that the kernel of $\varphi : P \to L$ has the form

$$\ker \varphi =: U = \left\{ \left(\begin{array}{c|c} I & C \\ \hline 0 & I \end{array} \right) \right\}.$$

The map sending such a matrix to C is clearly a bijection between U and the set $\mathrm{Mat}_{r,n-r}(K)$ of $k \times (n-r)$ matrices. In fact this map is an isomorphism between U and $\mathrm{Mat}_{r,n-k}(K)$ as an **additive** group because

$$\left(\begin{array}{c|c} I & C \\ \hline 0 & I \end{array} \right) \left(\begin{array}{c|c} I & C' \\ \hline 0 & I \end{array} \right) = \left(\begin{array}{c|c} I & C + C' \\ \hline 0 & I \end{array} \right).$$

◻

(e) Prove that $P = L \ltimes U$. [Hint: Show that $L \cap U = 1$ and $LU = P$.]

Proof. Note that we have

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) = \left(\begin{array}{c|c} I & C \\ \hline 0 & I \end{array} \right)$$

if and only if $A = I$, $B = I$, and $C = 0$. Hence $L \cap U = 1$. Next note that

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)\left(\begin{array}{c|c} I & A^{-1}C \\ \hline 0 & I \end{array}\right) = \left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array}\right),$$

hence $LU = P$. Since U is normal (it is a kernel) we conclude that $P = L \ltimes U$. [Remark: Note that P is **not** a direct product because

$$\left(\begin{array}{c|c} I & C \\ \hline 0 & I \end{array}\right)\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)\left(\begin{array}{c|c} I & -C \\ \hline 0 & I \end{array}\right) = \left(\begin{array}{c|c} A & -AC+CB \\ \hline 0 & B \end{array}\right) \notin L.]$$

□

(f) Prove that the action of L on U by conjugation is isomorphic to the action of $GL(r,K) \times GL(n-r,K)$ on $\mathrm{Mat}_{r,n-r}(K)$ by $(A,B)\cdot C := ACB^{-1}$.

Proof. Since $P = L \ltimes U$ we know that L acts on U by conjugation. Explicitly, we have

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)\left(\begin{array}{c|c} I & C \\ \hline 0 & I \end{array}\right)\left(\begin{array}{c|c} A^{-1} & 0 \\ \hline 0 & B^{-1} \end{array}\right) = \left(\begin{array}{c|c} I & ACB^{-1} \\ \hline 0 & I \end{array}\right)$$

If we identify L with $GL(r,K) \times GL(n-r,K)$ and we identify U with $\mathrm{Mat}_{r,n-r}(K)$ then this is just our favorite action $(A,B)\cdot C = ACB^{-1}$. □

3. Let G be a group, let K be a field, and let KG be the group algebra. That is, KG is the vector space of formal K-linear combinations of group elements with an associative multiplication defined by the group operation.

(a) State the definition of a KG-module. State the definition of a KG-submodule.

Proof. The group algebra KG is in particular a ring, so we define a KG-module as an additive abelian group V together with a map $KG \times V \to V$ satisfying:
- $1u = u$,
- $r(u+v) = ru + rv$,
- $(r+s)u = ru + su$,
- $r(su) = (rs)u$,

for all $r, s \in KG$ and $u, v \in V$. Note that $1 \in KG$ is the element $1_K 1_G$. We say that $U \subseteq V$ is a KG-submodule if:
- U is an additive subgroup of V, and
- $ru \in U$ for all $r \in KG$ and $u \in U$.

□

(b) Let U and V be KG-modules and let $\varphi : U \to V$ be a function of sets. What does it mean to say that φ is a **morphism** of KG-modules?

Proof. Let U and V be KG-modules and let $\varphi : U \to V$ be a function. We say that φ is a morphism of KG-modules if:
- $\varphi : U \to V$ is a homomorphism of abelian groups, and
- for all $r \in KG$ and $u \in U$ we have $\varphi(ru) = r\varphi(u)$. That is, the following diagram commutes.

$$\begin{array}{ccc} U & \xrightarrow{\varphi} & V \\ {\scriptstyle r}\downarrow & & \downarrow{\scriptstyle r} \\ U & \xrightarrow[\varphi]{} & V \end{array}$$

□

(c) We say that a KG-module is **irreducible** if it has no nontrivial KG-submodules. If U and V are irreducible KG-modules, prove that any **nonzero** morphism $\varphi : U \to V$ must be an **isomorphism**.

Proof. Let U and V be irreducible KG-modules and let $\varphi : U \to V$ be a nonzero morphism. Then $\ker \varphi \subseteq U$ is a KG-submodule of U. (Proof: For all $r \in KG$ and $u \in \ker \varphi$ we have $\varphi(ru) = r\varphi(u) = r0 = 0$, hence $ru \in \ker \varphi$.) Since U is irreducible and we assumed that $\ker \varphi \neq U$ this implies $\ker \varphi = 0$, hence φ is injective. Similarly, the image $\operatorname{im} \varphi \subseteq V$ is a KG-submodule of V. (Proof: For all $r \in KG$ and $v \in \operatorname{im} \varphi$ there exists $u \in U$ such that $rv = r\varphi(u) = \varphi(ru)$. Since $ru \in U$ we conclude that $rv \in \operatorname{im} \varphi$.) Then since V is irreducible and we assumed that $\operatorname{im} \varphi \neq 0$ we conclude that $\operatorname{im} \varphi = V$, hence φ is surjective. □

(d) If $K = \mathbb{C}$ (or any algebraically closed field) prove that the isomorphism from part (c) is a scalar multiple of the identity. [Hint: If we choose bases for U and V then φ is an invertible matrix. Since $\mathbb{C}$ is algebraically closed, φ has an eigenvalue $\lambda \in \mathbb{C}^\times$.]

Proof. Let U and V be isomorphic irreducible $\mathbb{C}G$-modules and let $\varphi : U \to V$ be an isomorphism. If we choose bases for U and V then φ becomes a square matrix and then since $\mathbb{C}$ is algebraphically closed φ has an eigenvalue $\lambda \in \mathbb{C}^\times$ (which must be nonzero because φ is invertible). Now consider the map $(\varphi - \lambda I) : U \to V$, where I is the identity matrix. This is still a morphism of $\mathbb{C}G$-modules because for all $r \in \mathbb{C}G$ and $u \in U$ we have

$$(\varphi - \lambda I)(ru) = \varphi(ru) - \lambda I(ru) = r\varphi(u) - r\lambda I(u) = r(\varphi - \lambda I)(u).$$

Since $\varphi - \lambda I$ is not injective (λ is an eigenvalue) and hence is not bijective, part (c) implies that $\varphi - \lambda I = 0$, or $\varphi = \lambda I$. □

(e) If G is **abelian**, use part (d) to prove that any irreducible $\mathbb{C}G$-module is 1-dimensional. [Hint: If V is any $\mathbb{C}G$-module, show that for all $g \in G$ the map $g : V \to V$ is a nonzero **morphism** of $\mathbb{C}G$-modules.]

Proof. Let G be abelian and let V be an irreducible $\mathbb{C}G$-module. For all $g \in G$ consider the invertible $\mathbb{C}$-linear map $g : V \to V$. For all $r = \sum_{h \in G} \alpha_h h \in KG$ and for all $v \in V$

we have

$$\begin{aligned}
g(rv) &= g\left((\sum_h \alpha_h h)v \right) \\
&= g\left(\sum_h \alpha_h (hv) \right) \\
&= \sum_h \alpha_h g(hv) \\
&= \sum_h \alpha_h (gh)v \\
&= \sum_h \alpha_h (hg)v \\
&= \sum_h \alpha_h h(gv) \\
&= (\sum_h \alpha_h h)(gv) \\
&= r(gv).
\end{aligned}$$

Thus $g : V \to V$ is an isomorphism of $\mathbb{C}G$-modules. Since g is nonzero (it is invertible) part (d) implies that $g = \lambda I$ for some $\lambda \in \mathbb{C}^\times$. We have shown that **every** element of G acts like a scalar on V. It follows that **every** vector subspace of V is a $\mathbb{C}G$-submodule. Since V is irreducible this implies that V has no nontrivial subspaces. Hence V is 1-dimensional. [I guess you could also allow that $V = 0$. Is zero irreducible? Probably not, for the same reason that 1 is not prime.] □

(f) Tell me **all** the irreducible representations of the Klein Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Let $G = \{1, a, b, ab\}$ be the Klein Vierergruppe, where $a^2 = b^2 = 1$ and $ab = ba$, and let $\varphi : G \to GL(V)$ be an irreducible $\mathbb{C}G$-module. Since G is abelian we know from part (e) that V is 1-dimensional and hence we have $\varphi : G \to \mathbb{C}^\times$. Note that the representation is determined by the numbers $\varphi(a), \varphi(b) \in \mathbb{C}^\times$ because $\varphi(ab) = \varphi(a)\varphi(b)$. Note also that we have

$$\varphi(a)^2 = \varphi(a^2) = \varphi(1) = 1$$

and hence $\varphi(a) = \pm 1$. Similarly we have $\varphi(b) = \pm 1$. This gives us a total of four possibilities. These are listed in the following ("character") table:

	1	a	b	ab
φ_1	1	1	1	1
φ_2	1	-1	1	-1
φ_3	1	1	-1	-1
φ_4	1	-1	-1	1

□