Contact: `gwmelvin@colby.edu`

Some thoughts and advice:

- Please submit solutions to the following problems by **Wednesday, April 3rd, 1.10pm**. You can either submit your solution in class or leave it outside my office.
- You should expect to spend several hours on homework sets. A lot of practice problem-solving is essential to understand the material and skills covered in class. Be organised and do not leave problem sets until the last-minute. Instead, get a good start on the problems as soon as possible.
- When approaching a problem think about the following: *do you understand the words used to state the problem? what is the problem asking you to do? can you restate the problem in your own words? have you seen a similar problem worked out in class? is there a similar problem worked out in the textbook? what results/skills did you see in class that might be related to the problem?*

  If you are stuck for inspiration come to office hours, or send me an email. However, don't just ask for the solution - provide your thought process, the difficulties you are having, and ask a coherent question in complete English sentences.
- Form study groups - get together and work through problem sets. **This will make your life easier!** You must write your solutions *on your own* and *in your own words*.
- You **are not allowed** to use any additional resources (e.g. `stackoverflow.com`). If you are concerned then please ask.

Some Group Theory & Schur's Lemma

Unless otherwise specified, all vector spaces will have scalar field $\mathbb{C}$.

Some Definitions/Theorems:

- (First Isomorphism Theorem) *Let $f : G \to H$ be a group homomorphism. Then, $G/\ker f \simeq \operatorname{im} f$.*
- (Fundamental Theorem of Finite Abelian Groups) *Let G be a finite abelian group. Then, there exists integers $n_1, \dots, n_r$ such that*
$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$
where n_i divides n_{i+1}, for all $i = 1, \dots, r-1$.
- A representation $\rho : G \to \mathrm{GL}(V)$ is said to be **faithful** if $\ker \rho = \{e_G\}$ i.e. ρ is injective.
- The **centre of** G is $Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$.

Problems:

1. For every $g \in G$, define $c_g : G \to G\ ,\ h \mapsto ghg^{-1}$.
   (a) Prove directly that c_g is an automorphism (i.e. a bijective homomorphism) of G, for every $g \in G$.
   (b) What is the inverse c_g^{-1}?
   (c) Denote the group of all automorphisms of G by $\mathrm{Aut}(G)$. Show that
$$C : G \to \mathrm{Aut}(G)\ ,\ g \mapsto c_g$$
   is a homomorphism.
   (d) Using the previous exercise, show that $Z(G)$ is a normal subgroup of G. (*Hint: what is* $\ker C$*?*)

2. Let G be a finite subgroup of $\mathbb{C}^\times = \{z \in \mathbb{C} \mid z \neq 0\}$. Here the group operation on $\mathbb{C}^\times$ is multiplication. In particular, G is a finite abelian group. Denote $n = |G|$, the order of G.

   (a) Let $p(t) = t^n - 1 \in \mathbb{C}[t]$. Show that $p(g) = 0$, for every $g \in G$.

   (b) Let $k = \max\{o(g) \mid g \in G\}$, where $o(g) = |g|$ is the order of $g \in G$. Prove that $k = n$. (*Hint: proceed by contradiction and use the Fundamental Theorem of Finite Abelian Groups*)

   (c) Deduce the following: *any finite subgroup of $\mathbb{C}^\times$ is cyclic.* (*Hint: if $f \in \mathbb{C}[t]$ and $\deg f = r$ then f has at most r roots.*)

   Remark: There is nothing special about $\mathbb{C}$ here: the same argument shows that, for k any field, any finite subgroup of $K^\times$ is cyclic. In particular, if $k = \mathbb{Z}/p\mathbb{Z}$ then $k^\times$ is cyclic: this has important consequences for cryptography.

3. Suppose that (ρ, V) is a faithful representation of G.

   (a) Let $z \in Z(G)$. Show that $\rho_z \in \mathrm{End}_G(\rho)$.

   (b) Using the First Isomorphism Theorem, prove that $Z(G)$ is isomorphic to a finite subgroup of $\mathrm{GL}_G(\rho) = \{T \in \mathrm{End}_G(\rho) \mid T \text{ invertible}\}$.

   (c) Deduce the following: *if G admits a faithful, irreducible representation then $Z(G)$ is cyclic.*