**M621 Overview: To help you prepare for Test 1**

Here are most of the main topics covered thus far—along with some questions about some of the topics.

1. Preliminaries:
   (a) The definition of divisibility in the integers
   (b) The Division Theorem
   (c) The GCD Theorem, which states that if $a, b$ are integers, at least one of which is non-0, then $(a, b)$ is the least positive integer in the set $\{sa+tb > 0 : \{s, t\} \subseteq \mathbb{Z}\}$. (I would expect you could prove it from the Division Theorem.)
   (d) Euclid's Lemma
   (e) A generalized version of Euclid's Lemma, which states that $a, b, c$ are integers, $a \neq 0$, and $(a, b) = 1$, then $a|bc$ implies that $a|c$.

2. Definition and fundamental properties of groups. Let $(G, *)$ be a group:
   (a) The uniqueness of identity of the identity of $G$
   (b) The uniqueness of inverses of elements
   (c) Left and right cancellation properties of groups
   (d) The order of an element of a group—be sure you know the definition of order of an element of a group.
   (e) Some basic problems; below $G = (G, *)$ is a group, and $b \in G$.
      i. Define a binary operation $\circ$ as follows: for all $u, v \in G$, $u \circ v = u * b * v$. Show that $\circ$ is an associative operation, that $(G, \circ)$ has an identity element, and show that every element $w \in G$ has an inverse in $(G, \circ)$ (find a formula for the inverse of an element $u \in (G, \circ)$).
      ii. Show that if $g \in G$, then $|gbg^{-1}| = |b|$—be sure to treat the two cases ( $|b|$ is finite and $|b|$ is infinite).
      iii. Show that if $|g| = n \in \mathbb{N}$ and $k \in \mathbb{Z}$, then $|g^k| = \frac{n}{(n,k)}$. Be able to write a clear, concise proof.

3. Subgroups and direct products.

   (a) Know the definition of a subgroup, and be able to use the subgroup tests.

   (b) Suppose that $G$ is a group, and $H$ is a finite non-empty subset of $G$. Be able to show that $H$ is a subgroup of $G$ (written $H \leq G$) if and only if $H$ is closed under the operation.

   (c) Let $A$ and $B$ be groups.

      i. What is the operation of the direct product $A \times B$?

      ii. Suppose $a \in A, b \in B$, with $|a| = m, |b| = n$, where $m, n$ are positive integers. Show that $|(a, b)| = \text{lcm}(|a|, |b|)$.

      iii. Show there is a subgroup of $A \times B$ that's isomorphic to $A$.

4. Homomorphisms and homomorphic images. Let $\Gamma : G \to K$ be a homomorphisms.

   (a) Show that $ker(\Gamma)$ is a normal subgroup of $G$.

   (b) Let $b \in K$. Prove that $\Gamma^{-1}(b)$ is a left coset of $ker(\Gamma)$.

   (c) Suppose $g \in G$ with $|g| = n \in \mathbb{N}$. Prove that $|\Gamma(g)|$ is the least positive integer $k$ such that $g^k \in N$. Then prove that $|\Gamma(g)|$ divides $|g|$.

   (d) Prove that if $N$ is a normal subgroup of $G$, then there exists a group $K$ and an onto homomorphism $\Gamma : G \to K$ such that $N = ker(\Gamma)$.

   (e) Suppose $G$ is Abelian and $\Gamma : G \to K$ is an onto homomorphism. Prove that $K$ is Abelian. Show by an example that if $\Gamma$ is not onto, then $K$ is not necessarily Abelian.

   (f) Suppose $G$ is cyclic and $\Gamma : G \to K$ is an onto homomorphism. Prove that $K$ is cyclic.

   (g) Suppose $G$ is n-generated, where $n \in \mathbb{N}$, and $\Gamma : G \to K$ is an onto homomorphism. Prove that $K$ is $n$-generated.

   (h) Suppose $H \leq G$. Prove that $N = \cap\{gHg^{-1} : g \in G\}$ is a normal subgroup of $G$. Then show that $N$ is the largest normal subgroup of $G$ contained in $H$.

5. Presentations

    (a) Be familiar and comfortable with the presentation of $D_{2n}$ given by $< r, s | r^n = e = s^2, rs = sr^{-1} >$.

    (b) Provide a presentation of $Z_3 \times Z_3$. Hint: $Z_3 \times Z_3$ is two-generated, with generators $(1,0)$ and $(0,1)$. So the presentation would look like $< a, b |$Some relations between the two generators $>$.

6. Group actions. Let $G$ act on a set $A$.

    (a) Using the axioms for group axioms, show that $\sigma_g : A \to A$, given by $\sigma_g(a) = g \cdot a$ for all $a \in A$, is a permutation of $A$. Then using those same axioms, prove that the function $\sigma : G \to S_A$ given by $\sigma(g) = \sigma_g$ for all $g \in G$, is a homomorphism. (I wouldn't hesitate to put this one on Exam 1.)

    (b) A relation is defined on $A$: For $a, b \in A$, let $a \equiv b$ if there exists $g \in G$ such that $g \cdot a = b$. Show that $\equiv$ is an equivalence relation.

    (c) The equivalence class of $a$ under the above equivalence relation (denoted $\mathcal{O}_a$) is called the *orbit* of $a$. Let $H \leq G$, and let $H$ act on $G$ as follows: $h \cdot g = hg$, for all $h \in H$ and all $g \in G$. Describe the orbits under this action; that is, for $g \in G (= A)$, describe $\mathcal{O}_g$.

    (d) Explain how the above can be used to prove Lagrange's Theorem.

7. Cyclic groups

    (a) Suppose $G =< g >$ is a cyclic subgroup generated by $g \in G$. Suppose that $|g| = n \in \mathbb{N}$.

        i. Show that $G = \{g^0, \ldots, g^{n-1}\}$, a set consisting of $n$ distinct elements.

        ii. Explain why $G \cong Z_n$: provide an isomorphism.

    (b) Theorem: Every subgroup of a cyclic group is cyclic, a main theorem. I wouldn't hesitate to ask you to prove this theorem on Test 1.

    (c) Draw the Hasse diagram of subgroups of $Z_{12}$.

    (d) Show that $A$ and $B$ both cyclic does not guarantee that $A \times B$ is cyclic.

8. $S_n$

(a) Given $\alpha \in S_n$, be able to find its representation as a product of disjoint cycles.

(b) Be able to explain why any two representations of an element $\alpha$ as a product of disjoint cycles consists of the same cycles, though perhaps given to you in different orders.

(c) Suppose $\alpha = \gamma_1 \dots \gamma_k$, where $\gamma_i$ are disjoint cycles. Show that $|\alpha| = \text{lcm}(|\gamma_i| : i = 1, \dots, k\}$.

(d) Let $(a_1 \dots a_k)$ be a k-cycle of $S_n$, and let $\beta \in S_n$. Let $\alpha = \beta(a_1 \dots a_k)\beta^{-1}$.

  i. Show that $x \in \{1, \dots, n\}$ is in $Fix(\alpha)$ if and only if $x \notin \{\beta(a_i) : i \in \{1, \dots, k\}\}$.

  ii. Show if $y \in \{1, \dots, n\}$ and $y = \beta(a_i)$ for some $i \in \{1, \dots, k\}$, then $\alpha(y) = \beta(a_{i+1})$.

  iii. Show that the above imply that $\alpha = (\beta(a_1) \dots \beta(a_k)$.

(e) Draw the Hasse diagram of the subgroup of $S_3$. Do the same for $D_8$.