Algebra

Math 211 Midterm
November 11, 2003
Ali Nesin

1. *How many abelian groups are there up to isomorphism of order* 67500? (5 pts.)

Answer: Since $67500 = 675 \times 10^2 = 25 \times 27 \times 10^2 = 2^2 \times 3^3 \times 5^4$, the answer is $2 \times 3 \times 5 = 30$.

For the 2-part of the group we have two choices: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$.

For the 3-part of the group we have three choices:

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$

$\mathbb{Z}/27\mathbb{Z}$

For the 5-part of the group we have five choices:

$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$,

$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,

$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$,

$\mathbb{Z}/625\mathbb{Z}$,

$\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$

2. *Let* $\mathbb{Z}(p^\infty)$ *be the Prüfer p-group. Prove or disprove*: $\mathbb{Z}(p^\infty) \approx \mathbb{Z}(p^\infty) \oplus \mathbb{Z}(p^\infty)$. (5 pts.)

Disproof: The first one has $p - 1$ elements of order p, the second one has $p^2 - 1$ elements of order p, so that these two groups cannot be isomorphic.

3. *Show that a subgroup of index* 2 *of a group is necessarily normal*. (5 pts.)

Proof: Let H be a subgroup of index 2 of G. Let $a \in G \setminus H$. Then $G = H \sqcup Ha = H \sqcup aH$, so that $aH = G \setminus H = Ha$, hence $aH = Ha$. If $a \in H$, $aH = Ha$ as well. So $aH = Ha$ all $a \in G$ and $H \lhd G$.

4. *Show that* $\mathbb{Q}^* \approx (\mathbb{Z}/2\mathbb{Z}) \oplus (\oplus_\omega \mathbb{Z})$. (5 pts.)

Proof: Let $q \in \mathbb{Q}^*$. Then $q = a/b$ for some $a, b \in \mathbb{Z} \setminus \{0\}$. Decomposing a and b into their prime factorization, we can write q as a ±product of (negative or positive) powers of prime numbers. Set,

$$q = \varepsilon(q)\prod_{p \text{ prime}} p^{\mathrm{val}_p(q)}$$

where $\mathrm{val}_p(q) \in \mathbb{Z}$ and $\varepsilon(q) = \pm 1$ depending on the sign of q. Note that all the $\mathrm{val}_p(q)$ are 0 except for a finite number of them. Let $\varphi : \mathbb{Q}^* \to (\mathbb{Z}/2\mathbb{Z}) \oplus (\oplus_\omega \mathbb{Z})$ be defined by

$$\varphi(q) = (\varepsilon(q), \mathrm{val}_2(q), \mathrm{val}_3(q), \mathrm{val}_5(q), \ldots)$$

It is clear that φ is an isomorphism of groups. (Here we view $\mathbb{Z}/2\mathbb{Z}$ as the multiplicative group $\{1, -1\}$).

5. *Find* $|\mathrm{Aut}(\mathbb{Z}/p^n\mathbb{Z})|$. (10 pts.)

Answer. The group $\mathbb{Z}/p^n\mathbb{Z}$ being cyclic (generated by $\underline{1}$, the image of 1), any endomorphism φ of $\mathbb{Z}/p^n\mathbb{Z}$ is determined by $\varphi(\underline{1})$. Then $\varphi(\underline{x}) = x\varphi(\underline{1})$ for all $x \in \mathbb{Z}$. Conversely any $\underline{a} \in \mathbb{Z}/p^n\mathbb{Z}$ gives rise to a homomorphism φ_a via $\varphi_a(\underline{x}) = x\underline{a}$. In other words $\mathrm{End}(\mathbb{Z}/p^n\mathbb{Z}) \approx \mathbb{Z}/p^n\mathbb{Z}$ via $\varphi \mapsto \varphi(1)$ as rings with identity. Thus $\mathrm{Aut}(\mathbb{Z}/p^n\mathbb{Z}) = \mathrm{End}(\mathbb{Z}/p^n\mathbb{Z})^* \approx (\mathbb{Z}/p^n\mathbb{Z})^* = \{\underline{a} : a \text{ prime to } p\} = \{\underline{a} : a \text{ not divisible by } p\} = \mathbb{Z}/p^n\mathbb{Z} \setminus p\mathbb{Z}/p^n\mathbb{Z}$ and has $p^n - p^{n-1}$ elements.

6. *What is* $\mathrm{Hom}(\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/6\mathbb{Z})$? *More generally, what is* $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$? *How many elements does it have*? (15 pts.)

Answer: Since $\mathbb{Z}/n\mathbb{Z}$ is cyclic and generated by $\underline{1}$ (the image of 1 in $\mathbb{Z}/n\mathbb{Z}$), any element φ of $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ is determined $\varphi(\underline{1}) \in \mathbb{Z}/m\mathbb{Z}$. Let

$$\mathrm{val}_1 : \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

be the map determined by $\mathrm{val}_1(\varphi) = \varphi(\underline{1})$. This is a homomorphism of (additive) groups. Furthermore it is one to one. However val_1 is not onto as in Question 5, because not all $\underline{\underline{a}} \in \mathbb{Z}/m\mathbb{Z}$ gives rise to a well-defined function $\underline{x} \mapsto x\underline{\underline{a}}$.

Claim: *An element* $\underline{\underline{a}} \in \mathbb{Z}/m\mathbb{Z}$ *gives rise to a well-defined function* $\underline{x} \mapsto x\underline{\underline{a}}$ *if and only if* m/d *divides* a *where* $d = \gcd(m, n)$.

Proof of the Claim: Assume m/d divides a where $d = \gcd(m, n)$. We want to show that the map $\underline{x} \mapsto x\underline{\underline{a}}$ from $\mathbb{Z}/n\mathbb{Z}$ into $\mathbb{Z}/m\mathbb{Z}$ is well-defined. Indeed assume $\underline{x} = \underline{y}$. Then n divides $x - y$. So na divides $xa - ya$. By hypothesis, it follows that nm/d divides $xa - ya$. Since $nm/d = \mathrm{lcm}(m, n)$, we get that $\mathrm{lcm}(m, n)$ divides $xa - ya$. Hence m divides $xa - ya$. It follows that $x\underline{\underline{a}} = y\underline{\underline{a}}$.

Conversely, assume that the function $\underline{x} \mapsto x\underline{\underline{a}}$ from $\mathbb{Z}/n\mathbb{Z}$ into $\mathbb{Z}/m\mathbb{Z}$ is well-defined. Then $n\underline{\underline{a}} = 0\underline{\underline{a}} = \underline{\underline{0}}$ and m divides na. Hence m/d divides $(n/d)a$. Since n/d and m/d are prime to each other we get that m/d divides a. This proves the claim.

Now we continue with the solution of our problem. The claim shows that the homomorphism

$$\mathrm{val}_1 : \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \longrightarrow (m/d)\mathbb{Z}/m\mathbb{Z}$$

is an isomorphism. We can go further and prove that $(m/d)\mathbb{Z}/m\mathbb{Z} \approx \mathbb{Z}/d\mathbb{Z}$.

Claim: *If* $n = mp$ *then* $m\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}/p\mathbb{Z}$.

Proof of the Claim: Let $\varphi : \mathbb{Z} \longrightarrow m\mathbb{Z}/n\mathbb{Z}$ be defined by $\varphi(x) = \underline{mx}$. Clearly φ is a homomorphism and onto. Its kernel is $\{x \in \mathbb{Z} : n \text{ divides } mx\} = \{x \in \mathbb{Z} : mp \text{ divides } mx\} = \{x \in \mathbb{Z} : p \text{ divides } x\} = p\mathbb{Z}$. So $\mathbb{Z}/p\mathbb{Z} \approx m\mathbb{Z}/n\mathbb{Z}$.

Thus $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \approx \mathbb{Z}/d\mathbb{Z}$ where $d = \gcd(m, n)$ and

$$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \{\underline{x} \mapsto k(m/d)\underline{\underline{x}} : k \in \mathbb{Z}\}.$$

For the specifique question: $\mathrm{Hom}(\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}) = \{\underline{x} \mapsto \underline{\underline{0}}, \underline{x} \mapsto 3\underline{\underline{x}}\} \approx \{\underline{\underline{0}}, \underline{\underline{3}}\}^+$.

7. *Let* p *be a prime*, A *a finite* p*-group and* $\varphi \in \mathrm{Aut}(A)$ *an automorphism of order* p^n *for some* n. *Show that* $\varphi(a) = a$ *for some* $a \in A^\#$. (10 pts.)

Proof: Let $G = \langle\varphi\rangle$. Then $|G| = p^n$ and G acts on $A^\#$. For $a \in A^\#$, there is a bijection between the G-orbit Ga of a and the coset space G/G_a where $G_a = \{g \in G : g(a) = a\}$ given by $gG_a \mapsto ga$. Thus $|Ga| = |G/G_a|$ and

$$|A^\#| = |\sqcup_a Ga| = \Sigma_a |Ga| = \Sigma_a |G/G_a|.$$

If $G_a \neq G$ for all a, then $|G/G_a| = p^i$ for some $i \geq 1$ so that p divides $\Sigma_a |G/G_a| = |A^\#| = p^n - 1$, a contradiction. Thus $G_a \neq G$ for some a and for this a, $|Ga| = 1$, i.e. $Ga = \{a\}$ and $\varphi(a) = a$.

8. *Let G be a group and $g \in G^\#$. Show that there is a subgroup H of G maximal with respect to the property that $g \notin H$.* (10 pts.)

Proof: Let $Z = \{H \leq G : g \notin H\}$. Order Z by inclusion. Since the trivial group $1 \in Z$, $Z \neq \emptyset$. It is easy to show that if $(H_i)_I$ is an increasing chain from Z then $\cup_I H_i \in Z$. Thus Z is an inductive set. By Zorn's Lemma it has a maximal element, say H. Then H is a maximal subgroup of G not containing g.

9. *A group G is called divisible if for every $g \in G$ and $n \in \mathbb{N} \setminus \{0\}$ there is an $h \in G$ such that $h^n = g$.*

9a. *Show that a divisible group cannot have a proper subgroup of finite index.* (10 pts.)

Proof: Assume G is divisible. Let $H \leq G$ be a subgroup of finite index, say n. We first prove that G has a normal subgroup K of finite index contained in H.

Claim: *A group G that has a subgroup of index n has a normal subgroup of index dividing $n!$ and contained in H.*

Proof of the Claim. Let G act on the left coset space G/H via $g.(xH) = gxH$. This gives rise to a homomorphism φ from G into $\mathrm{Sym}(G/H)$, and the latter is isomorphic to $\mathrm{Sym}(n)$. Thus $\mathrm{Ker}(\varphi)$ is a normal subgroup and φ gives rise to an embedding of $G/\mathrm{Ker}(\varphi)$ into $\mathrm{Sym}(n)$. Thus $|G/\mathrm{Ker}(\varphi)|$ dives $n!$ and $\mathrm{Ker}(\varphi)$ is a normal subgroup of index dividing $n!$

An easy calculation shows that $\mathrm{Ker}(\varphi) = \{g \in G : g(xH) = xH \text{ all } g \in G\} = \cap_{x \in G} H^x \leq H$. This proves the claim.

Let K be the normal subgroup of index m of G. Let $a \in G$. Let $b \in G$ be such that $a = b^m$. Then $a = b^m \in K$ (because the group G/K has order m) and so $G = K$.

9b. *Conclude that a divisible abelian group cannot have a proper subgroup which is maximal with respect to being proper.* (10 pts.)

Proof: Let G be a divisible abelian group. Let $H < G$ be a maximal subgroup of G. Then G/H has no nontrivial proper subgroups. Thus G/H is generated by any of its nontrivial elements. In particular G/H is cyclic. Since G/H cannot be isomorphic to $\mathbb{Z}$ (because $\mathbb{Z}$ has proper nontrivial subgroups, like $2\mathbb{Z}$), G/H is finite. By the question above $H = G$.

10. *Let G be a group. Let $H \lhd G$.*

10a. *Assume $\mathbb{Z} \approx H$. Show that $C_G(H)$ has index 1 or 2 in G.* (10 pts.)

Proof: Any element of G gives rise to an automorphism of H (hence of $\mathbb{Z}$) by conjugation. In other words, there is a homomorphism of groups $\varphi : G \to \mathrm{Aut}(H) \approx$

$\mathrm{Aut}(\mathbb{Z})$ given by $\varphi(g)(h) = h^g$ for all $h \in G$. The kernel of φ is clearly $C_G(H)$. Thus $G/C_G(H)$ embeds in $\mathrm{Aut}(\mathbb{Z})$. But $\mathbb{Z}$ has only two generators, 1 and -1 and any automorphism of $\mathbb{Z}$ is determined by its impact on 1, which must be 1 or -1. Thus $|\mathrm{Aut}(\mathbb{Z})| = 2$. This proves it.

10b. *Assume H is finite. Show that* $C_G(H)$ *has finite index in G.* (5 pts.)

Proof: As above. φ is a homomorphism from G into the finite group $\mathrm{Aut}(H)$ and the kernel of this automorphism is $C_G(H)$.