Y3 Group Theory Practice

April 20, 2015

1. Let G and H be groups:
   (a) Show that the direct product $G \times H$ is a group under pointwise products. What is the size of $G \times H$ if G and H are finite?
   (b) Let $A \subseteq G$ and $B \subseteq H$ be subgroups.
   - Show that $A \times B$ a subgroup of $G \times H$. Are all subgroups of this form?
   - If A, B are abelian show that $A \times B$ is.
   - If A, B are finite and cyclic with coprime orders then show $A \times B$ is cyclic. Can we remove any of these conditions?

   (c) What is the centre $Z(G \times H)$? Does this support the abelian claim above?
   (d) Let A, B be normal subgroups. Show that $A \times B$ is normal and express $(G \times H)/(A \times B)$ as a direct product (with proof).
   (e) What are the conjugacy classes of $G \times H$?
   (f) Find natural subgroups of $G \times H$ that are isomorphic to G, H respectively. If $|G| = p$ and $|H| = q$ are distinct primes then show these are the only possible non-trivial subgroups.
   (g) Show that $\mathrm{Aut}(G) \times \mathrm{Aut}(H)$ can be viewed as a subgroup of $\mathrm{Aut}(G \times H)$. Is this an isomorphism?

2. In this question we will show how a group G may often be decomposed into a direct product of two subgroups M, N.
   (a) Consider the map:
   $$\rho : M \times N \longrightarrow MN$$
   $$(m, n) \longmapsto mn.$$
   Show that if M, N commute then ρ is a surjective homomorphism.
   (b) Show that the kernel of ρ is isomorphic to $M \cap N$
   (c) Suppose now that $G = MN$ (i.e. every element of G is a product of something in M with something in N). Also assume that M, N commute and that $M \cap N = \{e\}$. Then show that $G \cong M \times N$.

3. Let p be prime:

   (a) What is $|\mathrm{GL}_n(\mathbb{Z}_p)|$?

   (b) Find $Z(\mathrm{GL}_n(\mathbb{Z}_p))$ for $n = 2, 3$. Generalize this for any n.

   (c) Show that the subset of upper triangular matrices with 1's on the diagonal is a subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$. What is the order of this subgroup? Does this agree with Lagrange's theorem?

4. (a) Using Sylow's theorems show that no group of order 162 is simple.

   (b) Let $p \neq q$ be odd primes and $a, b \geq 1$. Show that a group of order $p^a q^b$ has a normal Sylow subgroup if and only if $b < \mathrm{ord}_q(p)$ or $a < \mathrm{ord}_p(q)$.
   Hence show that no group of order $199^{2868936} \times 1499^2$ can be simple.

   (c) Show that there are infinitely examples where:

   - Both $n_p = n_q = 1$.
   - $n_p = 1$ but n_q isn't necessarily 1 (and that p could be either the smallest or the largest prime).
   - Neither n_p or n_q is necessarily 1.

   Thus when trying to show that there is a normal Sylow subgroup (i.e. $n_p = 1$) you don't always choose the smallest/largest prime.

5. Let G be a group of order $7^8 \times 29$.

   (a) Using 4(b) how do you know that neither n_p, n_q is necessarily 1?

   (b) Assume $n_7 \neq 1$. By using the conjugation action of G on its Sylow 7-subgroups show that G is not simple. Would this method have worked for the Sylow 29-subgroups instead?

   (c) Let $|G| = pq^b$ with p, q distinct primes, $b \geq 1$ and $p \equiv 1 \bmod q$. Show that if $b \geq \sum_{m=1}^{b} \lfloor \frac{p}{q^m} \rfloor$ then the above method will fail to show that G is not simple.

6. Let p, q be distinct primes. Using counting methods show that no group of order pq is simple. Can a group of order p^2 be simple?

7. (a) Show that $\mathrm{Aut}(\mathbb{Z}) \cong \{\pm 1\}$ (i.e. that the only automorphisms of $\mathbb{Z}$ are multiplication by ± 1).

   (b) Show that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Hence describe $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$.

   (c) Find $\mathrm{Aut}(C_2 \times C_2)$.

   (d) Show that $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^\times) \cong (\mathbb{Z}/(p-1)\mathbb{Z})^\times$. (In general $\mathrm{Aut}((\mathbb{Z}/n\mathbb{Z})^\times) \cong (\mathbb{Z}/\phi(n)\mathbb{Z})^\times$).

   (e) Working mod 5 the list $[1^3, 2^3, 3^3, 4^3] \equiv [1, 3, 2, 4] \bmod 5$. Similarly $[1^5, 2^5, 3^5, 4^5] \equiv [1, 2, 3, 4] \bmod 5$. In fact for any odd k the list $[1^k, 2^k, 3^k, 4^k]$ will reduce mod 5 to give either $[1, 2, 3, 4]$ or $[1, 3, 2, 4]$.
   Let p be prime and consider the list $S = [1^k, 2^k, ..., (p-1)^k]$.

- If k is even, why will S always contain repetitions (hence not be complete)?
- Using part (d) show that if S mod p is $1, 2, ..., (p-1)$ in some order then $p = 2$ or p is a Fermat prime. Is the converse true?