Mathematics GU4041
Introduction to Modern Algebra

Answers to Final Exam
December 20, 2016

1. Every finite group G has a composition series, that is, a sequence of subgroups $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ such that each G_i/G_{i-1} is simple. Although this is not unique, any other composition series $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$ has the same length n, and there exists $\sigma \in \Sigma_n$ such that $G_i/G_{i-1} \cong H_{\sigma(i)}/H_{\sigma(i)-1}$ for each $i \in \langle n \rangle$.

2. If ϕ is a homomorphism, then for all $g, h \in G$ we have $gh = (g^{-1})^{-1}(h^{-1})^{-1} = \phi(g^{-1})\phi(h^{-1}) = \phi(g^{-1}h^{-1}) = (g^{-1}h^{-1})^{-1} = (h^{-1})^{-1}(g^{-1})^{-1} = hg$, so G is abelian. Conversely, if G is abelian, then $\phi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \phi(g)\phi(h)$, so ϕ is a homomorphism.

3. Since $S = gSg^{-1}$, for every $s \in S$, we have $gsg^{-1} \in S$ as well. Hence if s^{-1} is the inverse of an element in S, then $gs^{-1}g^{-1} = (gsg^{-1})^{-1}$ is also the inverse of an element in S. Let $\prod_{i=1}^{k} s_i$ be an element of $\langle S \rangle$, that is, a product of elements in S and their inverses. Then, by the foregoing, $g(\prod_{i=1}^{k} s_i)g^{-1} = \prod_{i=1}^{k}(gs_ig^{-1})$ is also a product of elements in S and their inverses. Hence $g\langle S \rangle g^{-1} \subset \langle S \rangle$, that is, $\langle S \rangle$ is normal.

4. (a) Since every conjugate of a k-cycle in Σ_n is another k-cycle, $gS_kg^{-1} = S_k$ for all $g \in \Sigma_n$. The statement therefore follows from the previous problem.

(b) If k is odd, then every k-cycle has sign $+1$, so $S_k \subset A_n$ and hence $G_k < A_n$. By (a), $\langle S_k \rangle \lhd \Sigma_n$, so $G_k \lhd A_n$. But A_n is simple for $n \geq 5$, so $G_k = 1$ or A_n. Clearly $G_k \neq 1$ as it contains a nontrivial cycle! Hence $G_k = A_n$.

(c) By (a) and the second isomorphism theorem, $G_k \cap A_n \lhd A_n$, hence equals 1 or A_n. But the left-hand side certainly contains a non-trivial element, such as any product gh^{-1} for $g \neq h \in S_k$, so $G_k \cap A_n = A_n$, that is, $A_n < G_k < \Sigma_n$. But $A_n \neq G_k$ since the latter contains k-cycles. Hence $[\Sigma_n : G_k] < [\Sigma_n : A_n] = 2$, so that $[\Sigma_n : G_k] = 1$ and $\Sigma_n = G_k$.

Note: the statement is still true for $n < 5$. In fact, since we already proved that Σ_n and A_n are generated by bicycles and tricycles, respectively, the only remaining part is checking that Σ_4 is generated by 4-cycles, which can be done by hand.

5. The series is $1 \lhd \langle (12)(34) \rangle \lhd \langle (12)(34), (13)(24), (14)(23) \rangle \lhd A_4 \lhd \Sigma_4$. Here each subgroup is normal because it has index 2, except for $\langle (12)(34), (13)(24), (14)(23) \rangle < A_4$ which is of index 3, but $\langle (12)(34), (13)(24), (14)(23) \rangle \lhd \Sigma_4$ by problem **3**. And the composition factors are all simple since they are of prime order (2 or 3), hence cyclic.

6. (a) If $f : \mathbb{Z} \to \mathbb{Z}$ is any homomorphism, let $k = f(1) \in \mathbb{Z}$. Then for all $i \in \mathbb{Z}$, $f(i) = if(1) = ki$. If f has an inverse g, it is likewise of the form $g(i) = \ell i$, and then $i = fg(i) = k\ell i$, so $k\ell = 1$ and hence $k = \pm 1$. Hence $\text{Aut } \mathbb{Z} = \{\pm 1\} \cong \mathbb{Z}_2$.

(b) Any automorphism of $\mathbb{Z}_2$ must take the identity $[0]$ to $[0]$, so as a bijection it must also take the only other element $[1]$ to $[1]$. Hence $\text{Aut } \mathbb{Z}_2 = 1$.

(c) A semidirect product $\mathbb{Z} \rtimes \mathbb{Z}_2$ is determined by an action of $\mathbb{Z}_2$ on $\mathbb{Z}$ by group automorphisms, that is, a homomorphism $\mathbb{Z}_2 \to \text{Aut } \mathbb{Z}$. By (a) there is a nontrivial such homomorphism, so there is a semidirect product in which $\mathbb{Z}_2$ acts nontrivially on $\mathbb{Z}$ by conjugation, which is therefore nonabelian. (In fact, it is the group of all functions $g : \mathbb{Z} \to \mathbb{Z}$ of the form $g(i) = ai + b$ for $a = \pm 1$ and $b \in \mathbb{Z}$.)

(d) Likewise, a semidirect product $\mathbb{Z}_2 \rtimes \mathbb{Z}$ is determined by a homomorphism $\mathbb{Z} \to \text{Aut } \mathbb{Z}_2$, but by (b) these are all trivial, so the semidirect product is a direct product $\mathbb{Z}_2 \times \mathbb{Z}$, hence abelian.

7. The Sylow p-subgroups are finite in number, and every conjugate of a Sylow p-subgroup is a Sylow p-subgroup. So if $S = \{H_1, \ldots, H_n\}$ is the set of Sylow p-subgroups, then conjugation by g defines a function from S to itself. It is a bijection, as its inverse is conjugation by g^{-1}. Hence for every $g \in G$ there exists $\sigma \in \Sigma_n$ such that $gH_ig^{-1} = H_{\sigma(i)}$. Then

$$g(H_1 \cap \cdots \cap H_n)g^{-1} = (gH_1g^{-1}) \cap \cdots \cap (gH_ng^{-1}) = H_{\sigma(1)} \cap \cdots \cap H_{\sigma(n)} = H_1 \cap \cdots \cap H_n.$$

8. If p is prime and $[a] \neq [0] \in \mathbb{Z}_p$, then $\{0\} \neq \langle [a] \rangle < \mathbb{Z}_p$, so $1 \neq \#\langle [a] \rangle \,|\, p$ by Lagrange, so $\#\langle [a] \rangle = p$ and hence $\langle [a] \rangle = \mathbb{Z}_p$. On the other hand, if n is composite, say $n = k\ell$ with $k, \ell > 1$, then $\langle [k] \rangle = k\mathbb{Z}_n \neq \mathbb{Z}_n$.

9. (a) Every element of Σ_p may be expressed as a product of disjoint cycles, and its order is then the least common multiple of the lengths of those cycles. The only way to express a prime p as a least common multiple of numbers adding to p is as p itself. So the elements of order p are exactly the p-cycles and may be expressed as $(\sigma(1)\,\sigma(2) \cdots \sigma(n))$ for some $\sigma \in \Sigma_n$, unique up to reordering and recycling. Since there is only one cycle, reordering is trivial. Recycling shows that each such cycle may be expressed in exactly p ways as $(\sigma(1)\,\sigma(2) \cdots \sigma(n))$, $(\sigma(2)\,\sigma(3) \cdots \sigma(n)\,\sigma(1))$, $(\sigma(3)\,\sigma(4) \cdots \sigma(n)\,\sigma(1)\,\sigma(2))$, and so on. So the total number is $\#\Sigma_n/p = p!/p = (p-1)!$.

(b) Since $p!$ is divisible by p but not p^2, the Sylow p-subgroups have order p and are hence cyclic. By the previous problem, each one is generated by any of its nontrivial elements, of which there are $p-1$. The total number is therefore $(p-1)!/(p-1) = (p-2)!$.

10. Let G be a group of order 15. By the third Sylow theorem, the number of Sylow 3-subgroups divides 5 and is congruent to 1 mod 3, so it is 1. Likewise, the number of Sylow 5-subgroups divides 3 and is congruent to 1 mod 5, so it is also 1. Hence both S_3 and S_5 are normal. We know that $G = S_3S_5$ and that $S_3 \cap S_5 = 1$ (since its order divides both 3 and 5 by Lagrange). By the Main Theorem on Direct Products, $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5$ (so in fact $G \cong \mathbb{Z}_{15}$ by the Chinese Remainder Theorem). There is only one isomorphism class.

11. By the classification of finite abelian groups, any such group is isomorphic to a product of cyclic groups of prime power order. Since $36 = 2^2 3^2$, this must be (a) $\mathbb{Z}_4 \times \mathbb{Z}_9$, (b) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$, (c) $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, or (d) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. These four groups are not isomorphic to each other, since (for example) (a) has an element of order 4 but (b) does not. There are four isomorphism classes.

12. Let S be the set of all functions $\{1, 2, 3, 4, 5, 6, 7\} \to \{B, W\}$. The colorings of the necklace correspond to elements of this set. It is acted upon by the dihedral group D_{14}, and we need to count the number of orbits. By Burnside's lemma, this is given by

$$\frac{1}{\#D_{14}} \sum_{g \in D_{14}} \#S^g.$$

The identity fixes all 2^7 functions. Since 7 is prime, any of the 6 other rotations generates $\mathbb{Z}_7$, which acts transitively on the set $\{1, 2, 3, 4, 5, 6, 7\}$. Hence the rotation fixes only 2 necklaces, the all-black and all-white ones. The other 7 elements are all reflections in an axis through one bead, as shown. They fix the 2^4 necklaces having the same colors on opposite pairs of beads. The grand total is therefore $(2^7 + 6 \cdot 2 + 7 \cdot 2^4)/14 = (64 + 6 + 56)/7 = 18$.