Math 191 Homework 9: Permutations and group theory

Due: Monday, November 6, 2017

The problems are weighted by (approximate) difficulty. Solve at least 12 points worth of problems; don't count problems whose solutions you've seen before. Complete proofs are required for all problems. As always, you must write your solutions up by yourself, and you must cite any ideas that aren't your own.

The first four (or so) problems below are standard exercises in group theory; they are aimed at people who haven't studied groups before. But you can still try any of the problems with no prior experience; I've attempted to provide you with all of the necessary tools.

1 point

1. Let G be a group. Prove that G has only one identity e, and that every $g \in G$ has only one inverse g^{-1}.

2. If G is a group, prove that the inverse function $\varphi(g) = g^{-1}$ from G to itself is a homomorphism if and only if G is abelian. (If $G = (G, \cdot)$ and $H = (H, *)$ are groups, a *homomorphism* from G to H is a function $\varphi : G \to H$ such that for all $g, g' \in G$, $\varphi(g \cdot g') = \varphi(g) * \varphi(g')$.)

3. Let $\varphi : G \to H$ be a group homomorphism. Prove that the image of φ is a subgroup of H, and the kernel of φ (i.e. $\{g \in G : \varphi(g) = e_H\}$) is a normal subgroup of G. (A *subgroup* $K < G$ is a subset that forms a group with the same operation. It is called a *normal* subgroup of G if for all $g \in G$ and $k \in K$, we have $gkg^{-1} \in K$.)

2 points

4. Prove that if G is a group of order $2n$ and H is a subgroup of order n, then H must be normal in G.

5. (1968 B2) A is a subset of a finite group G, and A contains more than one half of the elements of G. Prove that each element of G is the product of two elements of A.

6. (1969 B2) Show that a finite group can not be the union of two of its proper subgroups. Does the statement remain true if "two" is replaced by "three"?

7. (2001 A1) Consider a set S and a binary operation $*$, i.e., for each $a, b \in S$, $a * b \in S$. Assume $(a * b) * a = b$ for all $a, b \in S$. Prove that $a * (b * a) = b$ for all $a, b \in S$. (Note: we are not assuming that S is a group. In particular, $*$ may not be associative.)

8. (1989 B2) Let S be a non-empty set with an associative operation that is left and right cancellative ($xy = xz$ implies $y = z$, and $yx = zx$ implies $y = z$). Assume that for every a in S the set $\{a^n : n = 1, 2, 3, \dots\}$ is finite. Must S be a group?

3 points

9. (Alexander Givental, 2016 mock Putnam #5) Let A be an invertible $n \times n$ matrix such that in each row of A, one entry is equal to ± 1 while all others are 0. Prove that there exists a positive integer k such that $A^k = A^T$ ("A-transposed").

10. (2012 A2) Let $*$ be a commutative and associative binary operation on a set S. Assume that for every x and y in S, there exists z in S such that $x * z = y$. (This z may depend on x and y.) Show that if a, b, c are in S and $a * c = b * c$, then $a = b$.

11. The *15 puzzle* consists of a 4-by-4 square frame containing tiles labeled 1 through 15, with one empty space. You can move the tiles by sliding any neighboring square into the hole. In the solved configuration, the tiles are arranged in numerical order across the rows, with the empty space in the bottom right. In the 1890's, Sam Loyd popularized a version of the puzzle that begins with the 14 and 15 tiles switched; he offered a $1000 prize for anyone who could solve it. Prove that this is impossible.

4 points

12. (1997 A4) Let G be a group with identity e and $\phi : G \to G$ a function such that

$$\phi(g_1)\phi(g_2)\phi(g_3) = \phi(h_1)\phi(h_2)\phi(h_3)$$

whenever $g_1 g_2 g_3 = e = h_1 h_2 h_3$. Prove that there exists an element $a \in G$ such that $\psi(x) = a\phi(x)$ is a homomorphism (i.e. $\psi(xy) = \psi(x)\psi(y)$ for all $x, y \in G$).

13. (2009 A5) Is there a finite abelian group G such that the product of the orders of all its elements is 2^{2009}?

14. Prove that for every nonnegative integer k, every group of order $n = 4k+2$ has a subgroup of order $\frac{n}{2} = 2k + 1$. (You may need Cauchy's theorem in one step of your proof; see below.)

15. (2007 A5) Suppose that a finite group has exactly n elements of order p, where p is a prime. Prove that either $n = 0$ or p divides $n + 1$. (Note: this is related to Cauchy's theorem that a group whose order is divisible by p must contain an element of order p, which is a baby version of the very powerful Sylow theorems.)

16. (2012 B6) Let p be an odd prime number such that $p \equiv 2 \pmod 3$. Define a permutation π of the residue classes modulo p by $\pi(x) \equiv x^3 \pmod p$. Show that π is an even permutation if and only if $p \equiv 3 \pmod 4$.