MAT 534: HOMEWORK 1

DUE W SEP 2

Problems marked by asterisk (*) are optional.
Notation:
$\mathbb{Z}$ – integer numbers;
$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ – congruence classes modulo n (considered as a group with respect to addition).
For some problems one needs the following basic result from number theory: an integer k has a multiplicative inverse modulo n if and only if k, n are relatively prime.

1. Let D_{2n} be the group of all symmetries of a regular n-gon. Let $r \in D_{2n}$ be the counterclockwise rotation by $2\pi/n$ and let $s \in D_{2n}$ be a reflection around one of the lines of symmetry. Prove the following results:
   (a) $r^n = e$ (where e is the group unit)
   (b) $s^2 = e$
   (c) $rs = sr^{-1}$
   (d) For odd n, any reflection $s' \in D_{2n}$ can be written in the form $s' = r^k s r^{-k}$ for some $k \in \mathbb{Z}$

2. Construct the isomorphism between the dihedral group D_6 (all symmetries of equilateral triangle) and the symmetric group S_3.

3. Describe all subgroups of symmetric group S_3. For each of them, say whether it is normal; if it is, describe the quotient.

4. Prove that any subgroup of index 2 is normal.

5. Construct a bijection between the coset space $S_n/(S_k \times S_{n-k})$ and the set B of all sequences of k zeroes and $n-k$ ones. (Hint: applying an element of S_n to the sequence $00\dots0111\dots1$ produces a new sequence).

6*. Let p be a prime number and $\mathbb{Z}_p^*$ — the group of all non-zero remainders modulo p (with respect to multiplication). Deduce Fermat little theorem from Lagrange theorem.

7*. (a) Prove that an element $k \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if k is relatively prime with n.
   (b) A complex number ζ is called a primitive root of unity of order n if $\zeta^n = 1$, but for all $k = 1, 2, \dots, n-1$, we have $\zeta^k \neq 1$. How many primitive roots of unity of order 15 are there? Describe them all.

8*. Prove that any subgroup $H \leq \mathbb{Z}$ must be of the form $H = a\cdot\mathbb{Z}$ for some $a \in \mathbb{Z}$.