MAT 534: HOMEWORK 1

DUE FRI, SEPT. 7

Problems marked by asterisk (*) are optional.

For some problems might need the following basic result from number theory (we will prove it later): an integer k is invertible modulo n if and only if k, n are relatively prime.

1. Do the problem discussed in class: if $x \in G$ is an element of order n, then the subgroup generated by x is isomorphic to $\mathbb{Z}_n$.

2. 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. (The map was discussed in class; you need to show that it is a bijection).

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

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

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

6. Let p be a prime number and $\mathbb{Z}_p^\times$— the group of all non-zero remainders modulo p (with respect to multiplication). Deduce from Lagrange theorem that for any integer a not divisible by p, we have $a^{p-1} \equiv 1 \mod p$.

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. From Dummit and Foote, p.101, problem 7.