**Алгебра, листок 5 (крайний срок сдачи – 2 февраля)**

**1.** **a)** Докажите, что $S_n$ порождается перестановками $(1,2)$ и $(1,2,\ldots,n)$.
**b)** Докажите, что $A_n$ порождается перестановками $(1,2,3)$, $(1,2,4),\ldots,(1,2,n)$.
**c)** Докажите, что при $n \geq 5$ группа $A_n$ порождается перестановками вида $(ij)(kl)$. Что происходит при $n = 4$?

**2.** **a)** Пусть $\sigma$ — четная перестановка, $\pi$ — нечетная перестановка, коммутирующая с $\sigma$. Докажите, что $\sigma$ тогда содержит либо цикл четной длины, либо два цикла *равной* нечетной длины.
**b)** Докажите обратное утверждение: если $\sigma \in A_n$ раскладывается на циклы различной нечетной длины, то никакая нечетная перестановка с ней не коммутирует.

**3.** **a)** Пользуясь предыдущей задачей, опишите классы сопряженности в группе $A_n$.
**b)** Как связано число элементов в классе сопряженности данной перестановки в $S_n$ и $A_n$?

**4.** **a)** Докажите, что группа $A_5$ проста, т.е. не содержит нетривиальных нормальных подгрупп.
**b)**$^\times$ Докажите простоту группы $A_n$ при $n \geq 5$.
**c)**$^\times$ Пользуясь предыдущим пунктом, перечислите все нормальные подгруппы в $S_n$, $n \in \mathbb{N}$.

Напомним, что *действием* группы $G$ на множестве $X$ называется гомоморфизм из $G$ в группу перестановок $X$, результат применения образа $g \in G$ при этом гомоморфизме к элементу $x \in X$ обозначается через $gx$, а *орбитой* и *стабилизатором* элемента $x \in X$ называются множества $Gx = \{gx \,|\, g \in G\}$ и $Stab(x) = \{g \in G \,|\, gx = x\}$ соответственно.

**5.** **a)** Группа $G$ действует на $X$ двумя способами, причем орбиты и стабилизаторы каждого элемента $x \in X$ при этих действиях одинаковы. Правда ли, что эти два действия совпадают?
**b)** Правда ли, что они совмещаются некоторой перестановкой элементов $X$?
**c)** Две группы действуют на $X$ так, что у каждого элемента $x \in X$ орбиты двух действий совпадают, а стабилизаторы изоморфны. Правда ли, что группы изоморфны?
**d)** Докажите, что $|G| = |Gx| \cdot |Stab(x)|$.
**e)** Докажите, что классы сопряженности группы $G$ – это орбиты ее действия на себе *внутренними автоморфизмами* (элемент $a \in G$ действует отображением $f_a : G \to G$, $f_a(g) = a^{-1}ga$), и что внутренние автоморфизмы – действительно автоморфизмы группы.
**f)** Перечислите все конечные группы, в которых не более трех классов сопряженности.
**g)** Докажите, что конечная группа не может оказаться объединением классов сопряженности элементов своей собственной подгруппы. **h)** А бесконечная может.
**i)** Докажите формулу Бернсайда: пусть при действии конечной группы $G$ каждый элемент $g \in G$ оставляет на месте $n_g$ точек, тогда число орбит этого действия равно $\sum_{g\in G} n_g/|G|$.
**j)** Если конечная группа действует транзитивно и нетривиально, то некоторый ее элемент действует без неподвижных точек. **k)** А для бесконечной группы это не верно.

**6.** **a)** Докажите, что в группе $\mathbb{Z}/m\mathbb{Z}$ ровно $\varphi(d)$ (функция Эйлера) элементов порядка $d|m$.
**b)** Докажите, что $\sum_{d|m} \varphi(d) = m$.

*Мультипликативная группа* кольца $(R, +, \cdot)$ – это $R^\times = (\{\text{обратимые элементы } R\}, \cdot)$.

**7.** **a)** Докажите, что $R_1^\times \times R_2^\times = (R_1 \times \mathbb{R}_2)^\times$.
**b)** Пусть поле $\mathbb{K}$ состоит из $n$ элементов, обозначим через $\psi(d)$ число элементов порядка $d$ в группе $\mathbb{K}^\times$. Докажите, что $\psi(d) \leqslant \varphi(d)$ при $d|n-1$.
**c)** Докажите, что $\sum_{d|n-1} \psi(d) = n - 1$.
**d)** Докажите, что мультипликативная группа конечного поля циклическая.
**e)** Докажите, что конечная подгруппа мультпликативной группы любого поля циклическая. Покажите, что это неверно для неассоциативных полей (колец с делением).
**f)**$^\times$ Докажите, что $(\mathbb{Z}/p^m\mathbb{Z})^\times$ циклическая при всех простых $p$ кроме случая $p = 2$, $m > 2$.
**g)** Выведите из результата предыдущего пункта, что $(\mathbb{Z}/n\mathbb{Z})^\times$ циклическая если и только если $n = 1, 2, 4, p^m$ или $2p^m$ для некоторого простого $p > 2$. Образующие этой циклической группы называются *примитивными корнями* по модулю $n$.