GROUPS AND RINGS 2021. BONUS SHEET 1

QUESTIONS BY ALEXEI N. SKOROBOGATOV

This sheet is not examinable. However, thinking about questions in this sheet will help you to understand the course better.

Free groups

1. Let a_s, $s \in S$, be symbols indexed by a set S. Let e be one more symbol. Let F_S be the set consisting of the 1-letter word e and all words $x_1 x_2 \dots x_n$, for $n \geqslant 1$, where each x_i is either some a_s or a_s^{-1}, and no cancellations are possible (that is, there is no i such that $x_i = a_s$ and $x_{i+1} = a_s^{-1}$, or $x_i = a_s^{-1}$ and $x_{i+1} = a_s$ for some $s \in S$). Define the group structure on F_S as follows:

- the product of the word e and the word $x_1 x_2 \dots x_n$ is $x_1 x_2 \dots x_n$;
- the product of the word $x_1 x_2 \dots x_n$ and the word e is $x_1 x_2 \dots x_n$;
- the product of the word $x_1 x_2 \dots x_n$ and the word $y_1 y_2 \dots y_m$ is obtained by performing cancellations in $x_1 x_2 \dots x_n y_1 y_2 \dots y_m$ (that is, any pair like aa^{-1} or $a^{-1}a$ is erased). If, after cancellation, no symbols are left, we declare the result to be e.

Prove that this law turns F_S into a group with unit element e. This group is called the *free group* generated by S. If S has cardinality n, then we write F_n for F_S and call it *the free group with n generators.*

2. Let $\mathrm{SL}(2, \mathbb{Z})$ be the group of matrices with entries in $\mathbb{Z}$ and determinant 1. Consider the matrices

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Prove that the subgroup of $\mathrm{SL}(2, \mathbb{Z})$ generated by A and B is isomorphic to the free group F_2 with two generators.

(Proceed as follows. We need to show that a non-trivial word (where no cancellations are possible) is not the identity matrix Id. First consider a word of the form

$$w = A^{a_1} B^{b_1} \dots A^{a_n} B^{b_n} A^{a_{n+1}}, \tag{0.1}$$

where the a_i and b_j are non-zero integers. The group $\mathrm{SL}(2, \mathbb{Z})$ acts by linear transformations on $\mathbb{R}^2$. Let $X_1 \subset \mathbb{R}^2$ be the set of points (x, y) such that $|x| > |y|$. Let $X_2 \subset \mathbb{R}^2$ be the set of points (x, y) such that $|x| < |y|$.

(a) Prove that $A^n(X_2) \subset X_1$ and $B^n(X_1) \subset X_2$.

(b) Deduce that $w(X_2) \subset X_1$, so $w \neq \mathrm{Id}$.

(c) Now deal with an arbitrary non-trivial word w. Prove that there is an integer n such that after cancellations the word $A^n w A^{-n}$ is of the form (0.1). Use (b) to prove that $A^n w A^{-n} \neq \mathrm{Id}$.

(d) Conclude that $w \neq \mathrm{Id}$.)

Date: October 10, 2021.

3. (a) Prove that for any group G generated by n elements, there is a surjective homomorphism $F_n \to G$.

(b) Show that F_n, $n \geqslant 1$, does not contain elements of finite order other than the unit element e.

(c)Show that $Z(F_n) = \{e\}$ if $n \geqslant 2$.

(d) Give an example of a non-trivial normal subgroup of F_n, that is, a normal subgroup G such that $G \neq \{e\}$ and $G \neq F_n$.

Sylow's theorems.

Let G be a finite group of order $|G| = p^n m$, where $n \geqslant 1$ and m is not divisible by p.

4. For $s \leqslant n$ let $N_p(s)$ be the number of subgroups of G of order p^s. Prove that

$$N_p(s) \equiv 1 \bmod p,$$

and conclude that G contains at least one subgroup of order p^s.

(Proceed as follows. Let X be the set of all subsets of G of cardinality p^s. Then G acts on X by left translations, that is, g sends $\{h_1, \ldots, h_{p^s}\}$ to $\{gh_1, \ldots, gh_{p^s}\}$. Call a point in X *normalised* if the corresponding p^s-element subset of G contains e. The set X is the disjoint union of G-orbits $\cup_{i=1}^n X_i$. Choose a normalised point $x_i \in X_i$ for each $i = 1, \ldots, n$, and write $\mathrm{St}(x_i) \subset G$ for the stabiliser of x_i.

(a) Prove that x_i, as the p^s-element subset of G, is the disjoint union of right cosets $\mathrm{St}(x_i)g$, for some $g \in G$. Conclude that the order of $\mathrm{St}(x_i)$ divides p^s.

(b) Prove that if $|\mathrm{St}(x_i)| = p^s$, then x_i, as the p^s-element subset of G, is $\mathrm{St}(x_i)$.

(c) Show that if $|\mathrm{St}(x_i)| = p^s$, then $\mathrm{St}(x_i)$ depends only on X_i, and not on a normalised point $x_i \in X_i$.

(d) Prove that this gives a bijection between the G-orbits in X of cardinality $p^{n-s}m$ and the subgroups of G of order p^s.

(e) Using the orbit–stabiliser theorem prove that

$$\binom{p^n m}{p^s} \equiv p^{n-s} m N_p(s) \bmod p^{n-s+1} m.$$

(f) Observe that the congruence in (e) holds for any group G of order $p^n m$. In particular, it holds for the cyclic group of this order. Compute the right hand side in this case, hence deduce that $N_p(s) \equiv 1 \bmod p$.)

A p-subgroup of G of maximal possible size p^n is called a *Sylow p-group*. The previous result says that Sylow p-subgroups exist for any prime p.

5. Let H and P be Sylow p-subgroup of G. Consider the action of P on G/H such that $a \in P$ sends gH to agH.

(a) Using that $|G/H| = m$ is coprime to p, prove that this action of P on G/H has a fixed point.

(b) Let gH be a fixed point of P. Deduce that P is contained in a Sylow p-group gHg^{-1}.

(c) Conclude that all Sylow p-subgroups are conjugate.

6. Let $H \subset G$ be a Sylow p-subgroup. Let $N(H) = \{g \in G | gHg^{-1} = H\}$. Show that $N(H)$ is a subgroup of G of index equal to the number of Sylow p-subgroups in G.