Lecture 0.

Prerequisits.

Groups.

Theorems about homomorphisms. Let $G \xrightarrow{\varphi} G'$ be a homomorphism of groups, $H = \ker\varphi$ a normal subgroup, $\varphi(G) \cong G/H$ factor group.

Cosets. $H < G$ a subgroup, $G = \dot{\bigcup_i} Hx_i = \dot{\bigcup_j} y_j H$ coset decompositions.

If $|G| < \infty$ then $|G| = |H| \cdot |G:H|$

Lagrange Theorem. $\forall g \in G \quad g^{|G|} = 1$.

Generation. For a subset $X \subset G$ let $\langle X \rangle$

let $\langle X \rangle$ denote the set of all products $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$, where $x_1, \dots, x_n \in X$ (repetitions are allowed), $\varepsilon_i = \pm 1$, $n \geq 1$. Then $\langle X \rangle$ is a subgroup of G. Moreover, it is the smallest subgroup of G that contains X. We say that $\langle X \rangle$ is <u>the subgroup generated by X</u>.

If $\langle X \rangle = G$ then we say that X generates G or, X is a <u>generating subset of G</u>.

<u>Commutation</u>. Two elements $x, y \in G$ commute if $xy = yx$. A measure of there "non-commutation" is the commutator $[x, y] = x^{-1}y^{-1}xy$,

$$xy = yx\,[x,y].$$

<u>Conjugation</u>. Two elements $x, y \in G$ are <u>conjugate</u> if there exists an element $g \in G$ such that $y = g^{-1}xg$. The relation: $x \sim y$ if x, y are conjugate, is an equivalence. Hence,

$$G = \dot{\bigcup}\,(\text{conjugacy classes})$$

For a fixed element $g \in G$ the <u>conjugatio</u>

$$\hat{g} : G \to G, \quad x \to g^{-1}xg,$$

is an automorphism of G.

<u>Cartesian Product</u>. Let G_i, $i \in I$, be a family of groups. Let

$$\prod_{i\in I} G_i = \{ f : I \to \bigcup_{i\in I} G_i \text{, such that } f(i) \in G_i \}$$

If $I = N = \{1, 2, \ldots\}$ then

$$\prod_{i\in I} G_i = \{ \text{sequences } (g_1 \in G_1, g_2 \in G_2, \ldots) \}$$

The multiplication is componentwise,

i.e. $\cancel{(fg)(i) =} (f_1 f_2)(i) = f_1(i) f_2(i)$.

Thus defined $\prod_{i\in I} G_i$ is a group that is called the Cartesian product of groups G_i, $i \in I$.

The subgroup

$$\overline{\prod_{i\in I}} G_i = \{ f : I \to \bigcup_{i\in I} G_i, f(i) \in G_i, \text{ for all but finitely many } i \in I \text{ we have } f(i) = 1_{G_i} \}$$

is called the direct product of groups G_i, $i \in I$.

If we identify a group G_i with its image in $\prod_{j \in I} G_j$,

$$G_i \ni g \to (1 \dots 1 \underset{i}{g} 1 \dots)$$

then $[G_i, G_j] = (1)$, $i \neq j$, and the set $\bigcup_{i \in I} G_i$ generates $\prod_{i \in I} G_i$.

Rings.

Theorems about homomorphisms,

$\varphi : R \to R'$, $I = \ker \varphi$ is an ideal of the ring R, i.e. $RI, IR \subseteq I$.

Generation. $X \subseteq R$ a subset,

$$\langle X \rangle = \left\{ \sum k_i x_1 \cdots x_n \,\middle|\, k \in \mathbb{Z},\ x_i \in X \right\}$$

is the subring generated by X.

Matrix Ring. $M_n(R) = \left\{ (a_{ij})_{n \times n} \,\middle|\, a_{ij} \in R \right\}$.

Direct sums of rings.

R, S rings; $R \oplus S = \{a+b\}$, formal sums},

$(a_1+b_1)(a_2+b_2) = a_1a_2 + b_1b_2$; $R, S \hookrightarrow R \oplus S$,

$a \to a+0,\ b \to 0+b$.

Inside of $R \oplus S$: $RS = SR = (0)$.

$R_1, \dots, R_n$ rings $\Rightarrow R_1 \oplus \cdots \oplus R_n$, similarly.

Fields.

There are 2 or 3 places in the course, where we refer to Galois Theory.

Algebras.

Let F be a field. An algebra A over the field F (or an F-algebra) is

(1) a vector space over the field F,

(2) a ring, that is, A is equipped with multiplication that, together with addition (from the vector space structure), makes A a ring,

(3) $\alpha(ab) = (\alpha a)\cdot b = a\cdot(\alpha b)$ for arbitrary elements $\alpha \in F$; $a, b \in A$.

<u>Examples.</u> Polynomial algebra $F[x]$, matrix algebra $M_n(F)$.

Theories of rings and algebras are parallel. In a way,

a ring = algebra over $\mathbb{Z}$.

<u>Generation:</u> $X \subset A$,

$\langle X \rangle = \{ \sum \alpha x_1 \dots x_n \mid \alpha \in F, x_i \in X$; linear combinations of products of elements from $X \}$,

is <u>the subalgebra of A generated by X.</u>

<u>Modules.</u>

We will talk about modules over algebras, but everything remains true for algebras over $\mathbb{Z}$, i.e. Rings.

Fix a field F. All vector spaces are vector spaces over F.

Let A be an associative F-algebra. Let V be a vector space. Suppose that there defined a bilinear mapping $A \times V \to V$, $a \times v \to av$, such that

$$a(bv) = (ab)v.$$

If $A \ni 1$ then we also assume $1v = v$. Then V is called a left A-module. Similarly, we can define right A-modules: bilinear binary product $V \times A \to V$, $v \times a \to va \in V$,

$(va)b = v(ab)$.

Let V be a left A-module. Then for a fixed element $a \in A$ the mapping

$$a' : V \to V, \quad v \to av$$

is a linear transformationand

$$(ab)' = a'b'$$

for arbitrary elements $a, b \in A$.

Let $Lin(V)$ be the vector space of all linear transformations $V \to V$. The space $Lin(V)$ is an F-algebra with respect to composition $(\varphi\psi)(v) = \varphi(\psi(v))$.

The mapping

$$A \to Lin(V), \quad a \to a',$$

is a homomorphism of F-algebras.

On the other hand, if $A \xrightarrow{f} Lin(V)$ is a homomorphism of F-algebras then the binary bilinear operation

$$a v = f(a) v$$

makes V a left module over A.

Submodules. Homomorphisms of modules.

A module V is <u>irreducible</u> if it does not have any nontrivial ($\neq (0), \neq V$) submodules and $AV \neq (0)$.