1. Groups

1.1. Abstract groups versus transformation groups. An abstract group is a collection $G$ of elements with a multiplication rule for them, i.e., a map:

$$G \times G \to G : (g_1, g_2) \mapsto g_1 \ast g_2.$$  

The sign $\ast$ of group multiplication in concrete cases can denote either addition $+$, or multiplication $\times$ (or $\cdot$), or composition $\circ$, etc.

The group multiplication satisfies three axioms:

a) there exists a unit element $e \in G$ such that $e \ast g = g \ast e = g$ for any $g \in G$;

b) for any $g \in G$ there exists an inverse element $g^{-1}$ such that

$$g^{-1} \ast g = g \ast g^{-1} = e;$$

c) for any $g_1, g_2, g_3 \in G$ the associativity relation holds: $(g_1 \ast g_2) \ast g_3 = g_1 \ast (g_2 \ast g_3)$.

A transformation group is a collection $G$ of invertible transformations of some set $X$ which:

a) contains the identical transformation $Id$;

b) together with any transformation $T$ contains the inverse transformation $T^{-1}$;

c) together with any two transformation $T_1, T_2$ contains their composition $T_1 \circ T_2$ defined as $T_1T_2(x) = T_1(T_2(x))$.

Any transformation group $G$ defines an abstract group $G_{abs}$. Namely, as a set, $G_{abs}$ coincides with $G$ but we forget about the set $X$ and about the meaning of $T \in G$ as transformations of $X$. The only thing which remains is a law of multiplication of elements of $G_{abs}$. The existence of unit ($= Id$) and the inverse is postulated by definition. As for associativity relation, it is a god-given property of composition: $T_1 \circ (T_2 \circ T_3) = (T_1 \circ T_2) \circ T_3$. Being applied to an $x \in X$ both parts give $T_1(T_2(T_3(x)))$.

A homomorphism of one abstract group $G$ to another abstract group $H$ is a map $\varphi : G \to H$ such that $\varphi(g_1 \ast g_2) = \varphi(g_1) \ast H \ \varphi(g_2)$. In this case we have also $\varphi(g^{-1}) = \varphi^{-1}$ and $\varphi(e) = H e$. If a homomorphism $\varphi : G \to H$ is an invertible map, it is called isomorphism and we say that $G$ and $H$ are isomorphic. Many different transformation groups may correspond to isomorphic abstract groups.

Date: Sept 2008.

Key words and phrases. Group, subgroup, $G$-set, stabilizer, normal subgroup,
1.2. **Subgroups, G-sets, cosets and homogeneous spaces.** A set $H \subset G$ is called a *subgroup* in a group $G$, if the following conditions are satisfied:

1. $H$ contains the unit $e$;
2. if $h \in H$ then $h^{-1} \in H$;
3. if $h_1, h_2 \in H$, then $h_1 \cdot h_2 \in H$.

The number of elements in $G$ is called the *order* of $G$ and is denoted $|G|$.

Lagrange Theorem: $|H|$ is a divisor of $|G|$ (the proof is given below).

Corollary: if $|G|$ is a prime number, $G$ has no proper subgroups.

We say that $X$ is a *left $G$-set* if the map $G \times X \to X : (g, x) \mapsto g \cdot x$ is defined and satisfies the axioms:

$$
e \cdot x = x \quad \text{for all } x \in X, \quad (g_1 \cdot g_2) \cdot x = g_1 \cdot (g_2 \cdot x) \quad \text{for all } x \in X \text{ and } g_1, g_2 \in G.$$

Denote by $L(g)$ the transformation $x \mapsto g \cdot x$. Then the axioms above mean that the correspondence $g \mapsto L(g)$ is a homomorphism of $G$ into the group of transformations of the set $X$. Indeed, they mean $L(g_1 \cdot g_2) = L(g_1) \circ L(g_2)$ and $L(e) = Id$. Instead of saying “$X$ is a left $G$-set” one often use the expression: “$G$ acts on $X$ from the left”.

The definition of a *right $G$-set* $Y$ (or the right action of $G$ on $Y$) is analogous: there is a map $Y \times G \to Y : (y, g) \mapsto y \cdot g$ satisfying axioms

$$y \cdot e = y \quad \text{for all } y \in Y, \quad y \cdot (g_1 \cdot g_2) = (y \cdot g_1) \cdot g_2 \quad \text{for all } y \in Y \text{ and } g_1, g_2 \in G.$$

Define by $R(g)$ the transformation $y \mapsto y \cdot g$. Then the right action is a so-called *antihomomorphism* of $G$ into the group of transformations of the set $X$. It has the properties: $R(e) = Id$, $R(g_1 \cdot g_2) = R(g_2) \circ R(g_1)$.

**Example.** Let $X$ be the set of column vectors, $Y$ be the set of row vectors and $G$ be the set of invertible square matrices of size $n$ over some field $K$. Then the ordinary matrix multiplication makes $G$ a group, $X$ is a left $G$-set, and $Y$ is a right $G$-set.

**Remarks.**

a) By default the “$G$-action” means a left $G$-action.

b) For abelian (commutative) groups there is no difference between left and right action.

c) From any left $G$-set we can easily manufacture a right $G$-set and vice versa. Namely, if $g \mapsto L(g)$ is a left action, then $g \mapsto L(g)^{-1}$ is a right action; and if $g \mapsto R(g)$ is a right action, then $g \mapsto R(g)^{-1}$ is a left action.

Let $X$ be a left $G$-set. Choose any point $x_0 \in X$ and consider the map $p : G \to X : g \mapsto g \cdot x_0$. The set $H = p^{-1}(x_0)$ is a subgroup in $G$ (check it!). It is called the *stabilizer* of $x_0$ in $G$ and is denoted by $Stab_G(x_0)$.

The $G$-set $X$ is called *homogeneous*, if for any two points $x_1, x_2 \in X$ there exists an element $g \in G$ such that $g \cdot x_1 = x_2$. In this case we also say that $G$ acts *transitively* on $X$. 
Let $X$ be an homogeneous $G$-set and $H = \text{Stab}_G(x_0)$. The sets $C_x = \overline{p}^{-1}(x)$ for $x \in X$ are called left $H$-cosets in $G$. It is clear (is it?) that they are disjoint and cover the whole group $G$. The set of all left $H$-cosets in $G$ is denoted by $G/H$. (For the set of all right cosets - define them yourself - the notation $H\backslash G$ is used).

**Lemma 1.1.** a) Let $g_x$ be any representative of a left $H$-coset $C_x \subset G$; then $C_x = g_x \cdot H$.

b) All left $H$-cosets have the same cardinality $|H|$.

c) We have $|G| = |H| \cdot |X|$.

1.3. **Normal subgroups and quotient groups.** We saw that for any pair of groups $G \supset H$ the number $|G|$ is always divisible by $|H|$ and the ratio is $|G/H|$. Does it mean that $G/H$ is a group by itself? The answer is: “no” in general, but for special cases - “yes”.

The product $C_1 \ast C_2$ of two left cosets is always defined but usually it is not a coset, but a union of several cosets. There are two lucky exceptions: the case of abelian group $G$ and the case of normal subgroup $H$. A subgroup $H$ is called normal in $G$ if for all $g \in G$ we have $g \ast H \ast \overline{g} = H$. (Note, that in an abelian group any subgroup is normal).

In these cases every left $H$-coset is also a right $H$-coset because $g \ast H = H \ast g$. Therefore, we have:

$$C_1 \ast C_2 = g_1 \ast H \ast g_2 \ast H = g_1 \ast g_2 \ast H \ast H = g_1 \ast g_2 \ast H.$$ 

Thus, the product of two cosets is again a coset and we have a multiplication law in $G/H$. It satisfies the group axioms and so $G/H$ is a group by itself. It is called factorgroup or quotient group.

Assume $G$ has a normal subgroup $G_1$ and let $G_2$ denote the quotient group $G/G_1$. Can we reconstruct $G$, knowing $G_1$ and $G_2$? This interesting question is still not completely solved. But if it were so, the study of all groups would be reduced to study simple groups which have no proper normal subgroups.

1.4. **Direct and semidirect products.** There are several ways to construct new groups from given ones. A direct product $G_1 \times G_2$ of two groups $G_1$ and $G_2$ is defined as follows: as a set, it is a direct product of sets, i.e., collection of pairs $(g_1, g_2), g_i \in G_i$. The group law is defined componentwise:

$$(g_1, g_2) \ast (g'_1, g'_2) := (g_1^1 \ast g'_1, g_2^2 \ast g'_2)$$

where $^1$ and $^2$ are group laws in $G_1$ and in $G_2$ respectively. Note, that both $G_1$ and $G_2$ can be considered as normal subgroups of $G_1 \times G_2$:

$$G_1 \simeq G_1 \times \{e\}, \quad G_2 \simeq \{e\} \times G_1.$$ 

Assume that a group $G$ has a normal subgroup $G_1 \subset G$ and for any coset $C \in G/G_1$ we can choose a representative $g_C \in C$ so that these representative form a subgroup $G_2 \subset G$. Of course, this subgroup must be isomorphic to the quotient group $G/G_1$. 

Lemma 1.2. The group multiplication establishes the set isomorphism:

$$(g_1, g_2) \mapsto g_1 * g_2 \quad \text{of } G_1 \times G_2 \text{ to } G.$$ 

In these “coordinates” the group law in $G$ takes the form:

$$(x_1, x_2) * (y_1, y_2) := \left( x_1 * (x_2 * y_1 * x_2)^{-1}, x_2 * y_2 \right).$$

We see that the abstract group $G$ can be reconstructed if we know the following data:

1. Abstract groups $G_1$ and $G_2$.
2. For any $g_2 \in G_2$ an automorphism $A(g_2)$ of the group $G_1$, such that $A(e) = Id$ and $A(g_2 * g_2') = A(g_2) \circ A(g_2')$.

Namely, we define the new group, the so-called semidirect product $G_1 \rtimes G_2$ (or $G_2 \ltimes G_1$) as follows. As a set, $G_1 \rtimes G_2$ is a direct product $G_1 \times G_2$. The group law is defined by the rule:

$$(g_1, g_2) * (g'_1, g'_2) := \left( g_1 \cdot (A(g_2)g'_1, g_2 \cdot g'_2) \right).$$

Remarks. 1. In this construction $G_1$ and $G_2$ play non-symmetric role what is reflected in notation.

2. It can happen that both $G_1$ and $G_2$ are abelian, but $G$ is not. A good example: the group $G$ of isometries of $\mathbb{R}^n$ is a semidirect product of a normal subgroup $G_1$ of translations and a subgroup $G_2$ of isometries, preserving the origin (rotations around origin and reflections in mirrors, containing origin).

3. In the case we have started the automorphism $A(g_2)$ has the form $g_1 \rightarrow g_2 * g_1 * g_2^{-1}$. It allows us to remember the group law in $G_1 \rtimes G_2$, considering the group $G$ as generated by $G_1$ and $G_2$ with relations

$$g_2 * g_1 = A(g_2)g_1 * g_2. \quad \text{(See next section).}$$

1.5. Examples of transformation groups. a) Let $X_n$ be a finite set of $n$ elements. E.g., $X_n = \{1, 2, 3, \ldots, n\}$. The set of all invertible transformations of $X_n$ forms a group $S_n$ of all permutations of $n$ objects a.k.a symmetric group.

b) Consider the set $Y_n$ consisting of $2n$ points labelled by $\pm 1, \pm 2, \ldots, \pm n$. Let $C_n$ be a collection of all permutation $s \in S_{2n}$ such that $s(-k) = -s(k)$. It is a subgroup in $S_{2n}$. It is isomorphic to $S_n \ltimes S_2^n$.

c) Let $M$ be a metric space with a distance $d(x, y)$. The set of all invertible maps $T$ which preserve the distance:

$$d(T(m_1), T(m_2)) = d(m_1, m_2) \quad \text{for all } m_1, m_2 \in M,$$

form a group $\text{Iso}(M)$ of isometries of $M$. Some particular cases are:

1) Let $\triangle_n$ denote a regular simplex in $\mathbb{R}^n$, then the group $\text{Iso}(\triangle_n)$ is isomorphic to $S_{n+1}$.

2) Let $\square_n$ denote a cube in $\mathbb{R}^n$, then, as abstract group, $\text{Iso}(\square_n)$ is isomorphic to $C_n$.

3) Let $S^{n-1}$ be a unit sphere in euclidean space $\mathbb{R}^n$. Then the group $\text{Iso}(S^{n-1})$ is isomorphic to the group $O(n, \mathbb{R})$ of all real orthogonal matrices of size $n$.  

c_4) Let \( \mathbb{R}^n \) be the euclidean space of dimension \( n \). Then \( \text{Iso}(\mathbb{R}^n) \) is isomorphic to the semidirect product \( O(n, \mathbb{R}) \ltimes \mathbb{R}^n \).

1.6. **Presentation of groups.** A way to define an abstract group is so-called presentation:

\[
P = \{g_1, g_2, \ldots \mid R_1, R_2, \ldots \}.
\]

where \( R_i \) are equations of the form \( g_i^{k_1} * g_i^{k_2} * \cdots * g_i^{k_N} = e \).

Call a group \( G \) a P-group if it generated by elements \( g_1, g_2, \ldots \) satisfying all relations \( R_1, R_2, \ldots \). The following remarkable theorem is true.

**Theorem 1.3** (Universal P-group). For any presentation \( P \) there exists a universal P-group denoted \( (G_P; \bar{g}_1, \bar{g}_2, \ldots) \) such that for any P-group \( (G; g_1, g_2, \ldots) \) there is a unique homomorphism \( \varphi : G_P \to G \) such that \( \varphi(\bar{g}_i) = g_i \).

**Examples.**
1. For \( P = \{g_1 \mid \emptyset \} \) we have \( G_P \simeq \mathbb{Z} \);
2. For \( P = \{g_1 \mid g_1^2 = e, g_1^5 = e \} \) we have \( G_P \simeq \{e\} \);
3. For \( P = \{s_1, s_2 \mid s_1^2 = s_2^2 = (s_1s_2)^3 = e \} \) we have \( G_P \simeq S_3 \);
4. For \( P = \{g_1, g_2 \mid g_1g_2g_1^{-1}g_2^{-1} = e \} \) we have \( G_P \simeq \mathbb{Z} \times \mathbb{Z} \).

1.7. **Conjugacy classes.** Every non-abelian group has many non-trivial automorphisms. Namely, every non-central element \( x \in G \) defines an automorphism

\[
A(x) : g \mapsto x * g * x^{-1}.
\]

Indeed,

\[
A(x)(g_1 * g_2) = x * (g_1 * g_2) * x^{-1} = x * g_1 * x^{-1} * x * g_2 * x^{-1} = A(x)(g_1) * A(x)(g_2),
\]

\[
A(x)(g^{-1}) = (A(x)(g))^{-1} \quad \text{and} \quad (A(x)(e) = e).
\]

These automorphisms are called inner. They acts on group elements, subsets, subgroups etc. Two objects are called conjugate if one is obtained from another by an inner automorphism. Collection of all objects conjugate to a given one is called a conjugacy class. The conjugate objects have many common features. For example, group elements from the same conjugacy class have the same order. Two conjugate subgroups are stabilizers of two different points of the same homogeneous space.

2. **RINGS AND FIELDS**

2.1. **Definition of rings and fields.** Consider a set \( R \) with two operations: addition \( + \) and multiplication \( \cdot \). Often instead of \( a \cdot b \) the simple notation \( ab \) is used. The two operations are subordinate to conditions:

1. \( (R, +) \) is an abelian group with the neutral element \( 0 \).
2. Multiplication is distributive: \( a \cdot (b + c) = a \cdot b + a \cdot c \) and \( (b + c) \cdot a = b \cdot a + c \cdot a \).

**Remark.** Multiplication may subject to additional conditions: commutativity, associativity, existence of neutral element 1 and an inverse element \( a^{-1} \) for all \( a \neq 0 \). If one of these properties is present, it must be mention in the definition and reflected in the name: commutative ring, associative ring, division ring. If all the properties hold, \( R \) is called a field; the associative division ring is called a skew-field.
Many fields consist of ordinary real or complex numbers. Then they necessarily contain the field $\mathbb{Q}$ of rational numbers.

Examples of rings: $\mathbb{Z}$, $n\mathbb{Z}$, $\mathbb{Z}/(n\mathbb{Z})$, $\mathbb{Z}[\frac{1}{n}]$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$. From these examples $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}/(p\mathbb{Z})$ for $p$ prime are fields; $\mathbb{H}$ is a skew-field.

The notion of a subring of a ring $R$ is defined naturally: it is a subset of $R$, closed under both ring operations.

A subring $I \subset R$ is called a left ideal, if $I \cdot R \subset I$;
a right ideal, if $R \cdot I \subset I$;
a two-sided ideal, if $I \cdot R \subset I$ and $R \cdot I \subset I$.

E.g. $\mathbb{Z}/(n\mathbb{Z})$ is a two-sided ideal in $\mathbb{Z}$.

For a ring $R$ and a two-sided ideal $I \subset R$ the quotient ring or factor ring $R/I$ is defined. As an abelian group, it is a quotient group $R/I$ and the multiplication is defined in a standard way: $[a + I] \cdot [b + I] = [ab + I]$.

Example: $\mathbb{Z}/n\mathbb{Z}$ is a factor ring of $\mathbb{Z}$.

2.2. Matrix ring. For any ring $R$ and any natural number $n$ we construct the ring $\text{Mat}_n(R)$, consisting of square matrices of size $n \times n$ with entries from $R$. Shortly this matrix is denoted by $A = [a_{ij}]$ where $i$ and $j$ run from 1 to $n$. The full notation is
\[ A = \begin{pmatrix}
  a_{11} & a_{12} & \cdots & a_{1n} \\
  a_{21} & a_{22} & \cdots & a_{2n} \\
  \cdots & \cdots & \cdots & \cdots \\
  a_{n1} & a_{n2} & \cdots & a_{nn}
\end{pmatrix}.
\]

The ring operation are given by the rules:
\[ A + B = [a_{ij} + b_{ij}], \quad AB = \left[ \sum_{k=1}^{n} a_{ik}b_{kj} \right]. \tag{2.1} \]

If $R$ is associative, so is $\text{Mat}_n(R)$. But it is not commutative for $n > 1$ even if $R$ is. Most associative rings are isomorphic to subrings of $\text{Mat}_n(R)$ for an appropriate $R$ and $n$.

3. Vector spaces, modules and algebras

Some algebraic structures we want to study, need for their definition an auxiliary algebraic structure, a ring or a field.

3.1. Vector spaces. A vector space over a field $K$ is an abelian group $(V, +)$ endowed by an action of a field $K$. This means that a map $K \times V \to V : (\lambda, v) \mapsto \lambda v$ is given, which satisfied the conditions:
\[ \lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2; \quad (\lambda + \mu)v = \lambda v + \mu v; \quad (\lambda \mu)v = \lambda(\mu v). \]

Usually elements of $K$ are called “numbers” and elements of $V$ are called “vectors”. In most cases $K = \mathbb{R}$ or $K = \mathbb{C}$; then $V$ is called real or complex vector space.

We denote numbers by lower case Greek letters $\alpha, \beta, ... \lambda, \mu, \nu...$ and vectors by lower case Roman letters, sometimes with an arrow above: $\vec{u}, \vec{v}, \vec{w}...$. The
vector spaces and related structures: linear operators, polylinear forms, tensors etc constitutes the overwhelming majority of all application of algebra.

**Definition 3.1.** A linear combination of vectors \( \vec{v}_1, \ldots, \vec{v}_n \) is an expression of the form

\[
\lambda_1 \vec{v}_1 + \lambda_2 \vec{v}_2 + \cdots + \lambda_n \vec{v}_n.
\]

It is called trivial if \( \lambda_1 = \lambda_2 = \cdots = \lambda_n = 0 \). Otherwise it is called non-trivial.

**Definition 3.2.** Vectors \( \vec{v}_1, \ldots, \vec{v}_n \) are called linearly dependent (or simply dependent) if there is a non-trivial linear combination of these vectors which is equal to zero vector \( \vec{0} \). Otherwise the vectors are called independent.

A most important characteristic of a vector space \( V \) is the maximal number of linearly independent vectors in it. This number is called the dimension of \( V \), is denoted by \( \dim V \) and takes values \( \{0, 1, 2, \ldots, \infty\} \). Two finite dimensional vector spaces over the same field are isomorphic iff their dimensions are equal.

Let \( V_1 \) and \( V_2 \) be the vector space over a field \( K \).

**Definition 3.3.** A map \( A : V_1 \to V_2, \ v \mapsto Av \) is called linear if it has the property

\[
A(\lambda v + \mu w) = \lambda Av + \mu Aw.
\] (3.1)

The linear maps are also called linear operators.

3.2. **Modules over a ring.** A generalization of the notion of a vector space over a field \( K \) is the notion of module over a ring \( R \). More precisely, for non-commutative ring we have to distinguish the left modules and right modules. Often we restrict ourselves by left modules and call them simply modules.

**Definition 3.4.** A left module over the ring \( R \) is an abelian group \( (M, +) \) endowed by the left action of a ring \( R \), i.e. there is a map

\[
R \times M \to M : (a, m) \mapsto am
\]
satisfying two distributive laws

\[
a(m_1 + m_2) = am_1 + am_2; \quad (a + b)m = am + bm; \quad (ab)m = a(bm)
\]

and the action condition

\[
(ab)m = a bm.
\]

In other words, an element \( a \) of the ring \( R \) acts on the module \( M \) by the transformation \( L(a) : m \mapsto am \). The action condition means that \( L(ab) = L(a) \circ L(b) \).

\[\text{\footnote{Actually, there are different kinds of infinity, but in our course we do not go deep in the question.}}\]
For example, any abelian group \((M, +)\) has a canonical structure of a \(\mathbb{Z}\)-module. Namely, the action of \(n \in \mathbb{Z}\) on the element \(m \in M\) gives
\[
\begin{align*}
    nm = \begin{cases} 
        n \text{ times } m + m + \cdots + m & \text{if } n > 0, \\
        0 & \text{if } n = 0, \\
        -|n|m & \text{if } n < 0.
    \end{cases}
\end{align*}
\]

3.3. **Algebras.** The last object of our Zoo is a notion of algebra. We call a set \(A\) an *algebra over the field* \(K\) if it is simultaneously a ring \((A, +, \cdot)\) and a vector space over \(K\); these two structures are related by the condition that the ring multiplication is a bilinear operation:
\[
    (\lambda a + \mu b) \cdot c = \lambda ac + \mu bc; \quad a \cdot (\lambda b + \mu c) = \lambda ab + \mu ac.
\]

Algebras, as rings, can be associative, commutative or division algebras but in general do not possess any of these properties.

The most important example of an associative algebra over a field \(K\) is a matrix algebra \(\text{Mat}_n(K)\) with the natural structures of a ring and a vector space over \(K\).

For algebras, as for rings, the notion of a module makes sense. Namely, a vector space \(M\) is a left module over an algebra \(A\) (both over the same field \(K\)), if a bilinear map
\[
    A \times M \to M : (a, m) \mapsto am
\]
is defined and satisfies the usual axioms of a module.

Example. Consider the \(n\)-dimensional vector space \(V\) over \(K\) consisting of column vectors \(\vec{v}\) of size \(n\) with entries \(v_i, 1 \leq i \leq n\), from \(K\). It is a module over \(\text{Mat}_n(K)\) with respect to the action
\[
    (Av)^i = \sum_{j=1}^{n} a_{ij} v^j.
\]

So, a matrix \(A\) defines a linear operator \(L(A)\) in the space \(V\). Actually, the multiplication of matrices in \((2.1)\) above is defined specially to have the property \(L(A) \circ L(B) = L(AB)\), i.e. to be compatible with the composition of operators.

For algebras, as for rings, the notions of a left, right and two-sided ideal make sense. For any two-sided ideal \(I \subset A\) a quotient, or *factor algebra* \(A/I\) is defined.

---

1 Department of Mathematics, University of Pennsylvania, Phila, PA 19104-6395, USA.

E-mail address: kirillov@math.upenn.edu