# Implicit function theorem over free groups and genus problem 

O. Kharlampovich, A. Myasnikov

## 1 Introduction

In late 40 's Ralph Fox introduced derivatives over free groups to study invariants of group presentations (see [9]). That was a beginning of free differential calculus over free groups. It turns out that Fox's derivatives can be used to define matrix representations of free groups of finite rank, so called Magnus representations, and some of their groups of automorphisms, among which Burau and Gasner representations are the most notorious ones (see [3]). In 1950 R. Lyndon described cohomological dimensions of one relator groups [15]. His analysis was based on some non-trivial results from free differential calculus. Another development in the theory of differentiation over free groups is due to J. Birman. She proved that the inverse function theorem holds in free groups [4]. This gave rise to a new approach in the study of minimal generating systems (or, more generally, primitive systems) in various relatively free groups (see [1], [14], [17], [18]).

In this paper we discuss implicit function theorem over free groups and some of its applications.

## 2 Free differential calculus

Let $F=F(X)$ be a free group with basis $X=\left\{x_{1}, \ldots, x_{n}\right\}$ and $Z F$ be the integral group ring of $F$.

A linear map $D: Z F \rightarrow Z F$ is called a derivation in $Z F$ if it satisfies the following condition:

$$
D(f g)=D(f)+f D(g) \quad \text { for any } f, g \in F
$$

For any $i=1, \ldots, n$ there exists a unique derivation $d_{i}$ (it is called the derivative with respect to $x_{i}$ ) such that for any $k=1, \ldots, n$

$$
d_{i}\left(x_{k}\right)=\left\{\begin{array}{lll}
1 & \text { if } & i=k \\
0 & \text { if } & i \neq k
\end{array}\right.
$$

Let $Y=\left\{y_{1}, \ldots, y_{n}\right\}$ be a set of $n$ elements of the group $F$. The matrix

$$
J_{Y}=\left(d_{i}\left(y_{k}\right)\right)_{i, k=1, \ldots, n}
$$

is called the Jacobian matrix of $Y$. In particular, if $\phi: F \rightarrow F$ is an endomorphism of $F$, and $Y_{\phi}=\left\{x_{1}^{\phi}, \ldots, x_{n}^{\phi}\right\}$ then the Jacobian matrix $J_{\phi}=J_{Y_{\phi}}$ of $Y_{\phi}$ is called the Jacobian of $\phi$.

The following is an analog of the inverse function theorem for free groups.
Theorem 1 (J.Birman [3]) A homomorphism $\phi: F \rightarrow F$ is an automorphism of $F$ if and only if the Jacobian $J_{\phi}$ is right invertible over $Z F$.

## 3 Elements of algebraic geometry over groups

To formulate implicit function theorem over groups we need to introduce some basic notions of algebraic geometry over groups. We refer to [2] for details.

Let $G$ be a group, $F(X)$ be a free group with basis $X=\left\{x_{1}, x_{2}, \ldots x_{n}\right\}, G[X]=$ $G * F(X)$ be a free product of $G$ and $F(X)$. If $S \subset G[X]$ then $S=1$ is called a system of equations over $G$. As an element of the free product the left side of every equation in $S=1$ can be written as a product of some elements from $X \cup X^{-1}$ (which are called variables) and some elements from $G$ (constants). To emphasize this we sometimes write $S\left(x_{1}, \ldots, x_{n}\right)=1$ or $S(X)=1$.

A solution of the system $S(X)=1$ over a group $G$ is a tuple of elements $a_{1}, \ldots, a_{n} \in$ $G$ such that after replacement of each $x_{i}$ by $a_{i}$ the left side of every equation in $S=1$ turns into the trivial element of $G$. Equivalently, a solution of the system $S=1$ over $G$ can be described as a homomorphism $\phi: G[X] \longrightarrow G$ which is identical on $G$ and such that $\phi(S)=1$. By $V_{G}(S)$ we denote the set of all solutions in $G$ of the system $S=1$, it is called the algebraic set defined by $S$. This algebraic set $V_{G}(S)$ uniquely corresponds to the normal subgroup

$$
R(S)=\left\{u(x) \in G[X] \mid \forall A \in V_{G}(S) u(A)=1\right\}
$$

of the group $G[X]$. The subgroup $R(S)$ contains $S$, and it is called the radical of $S$. The quotient group

$$
G_{R(S)}=G[X] / R(S)
$$

is the coordinate group of the variety $V(S)$.
We define a Zariski topology on $G^{n}$ by taking as a sub-basis for the closed sets of this topology, the algebraic sets in $G^{n}$. If $F$ is a free non-abelian group then the union of two algebraic sets is again algebraic, therefore the closed sets in the Zariski topology over $F$ are precisely the algebraic sets. The Zariski topology over $F^{n}$ is noetherian for
every $n$, i.e., every proper descending chain of closed sets in $F^{n}$ is finite. This implies that every algebraic set $V$ in $F^{n}$ is a finite union of irreducible subsets (they are called irreducible components of $V$ ), and such decomposition of $V$ is unique.

## 4 Algebraic sets over a free non-abelian group

Let $F$ be a free non-abelian group. In this section, following [11] and [12], we describe algebraic sets over $F$. Quadratic equations play the central part in this description.

An equation $S=1$ is called quadratic in variables $X=\left\{x_{1}, \ldots, x_{n}\right\}$ if every variable from $X$ occurs in $S$ not more then twice.

Let $X_{1}, \ldots, X_{m}$ be disjoint tuples of variables. A system $U\left(X_{1}, \ldots, X_{m}\right)=1$ (with coefficients from $F$ ) of the following type

$$
\begin{aligned}
S_{1}\left(X_{1}, X_{2}, \ldots, X_{m}\right) & =1 \\
S_{2}\left(X_{2}, \ldots, X_{m}\right) & =1 \\
\ddots & \\
S_{m}\left(X_{m}\right) & =1
\end{aligned}
$$

is said to be triangular quasi-quadratic if for every $i$ the equation $S_{i}\left(X_{i}, \ldots, X_{m}\right)=1$ is quadratic in the variables from $X_{i}$.

Denote by $G_{i}$ the coordinate group of the subsystem $S_{i}=1, \ldots, S_{m}=1$ of the system $U=1$ :

$$
G_{i}=F\left[X_{i}, \ldots X_{m}\right] / R\left(S_{i}\left(X_{i}, \ldots, X_{m}\right), \ldots, S_{m}\left(X_{m}\right)\right) \quad(i=1, \ldots, m+1)
$$

in particular, $G_{m+1}=F$ and $G_{1}=F_{R(U)}$. The system $U=1$ is said to be non-degenerate if for each $i$ the equation $S_{i}\left(X_{i}, \ldots, X_{m}\right)=1$ has a solution in $G_{i+1}$ (with elements from $X_{i}$ considered as variables and elements from $X_{i+1}, \ldots, X_{m}$ as coefficients from $\left.G_{i+1}\right)$.

Observe, that if the system $U=1$ is non-degenerate then the coordinate group $G_{i+1}$ is embedable into $G_{i}(i=1, \ldots, m)([13])$, i.e., we have a chain of groups

$$
F=G_{m+1} \leq G_{m} \leq \ldots \leq G_{1}=F_{R(U)}
$$

To solve the system $U=1$ over $F$ one needs to solve the last quadratic equation $S_{m}\left(X_{m}\right)=1$ over $G_{m+1}=F$, then the previous one (which is again quadratic!)
$S_{m-1}\left(X_{m-1}, X_{m}\right)=1$ over the coordinate group $G_{m}$, and continue the process going up along the triangular system until the first equation $S_{1}\left(X_{1}, \ldots, X_{m}\right)=1$ has been solved in the group $G_{2}$. Now, to get solutions of this system in the initial free group $F$, one needs to specialize the solutions obtained in $G_{2}$ into $F$ (in this case to specialize means to take an arbitrary homomorphism from $G_{2}$ into $F$, that fixes elements from $F$, and apply it to the obtained set of solutions in $G_{2}$ ).

Now, the following crucial result from [12] describes the solution set in $F$ of an arbitrary system $S(X)=1$ with coefficients from $F$ : for any such $S(X)=1$ one can effectively find a finite family of non-degenerate triangular quasi-quadratic systems $U_{1}\left(Y_{1}\right)=1, \ldots, U_{n}\left(Y_{n}\right)=1$ (here $Y_{i}$ 's are disjoint tuples of variables of, possibly, different length) and word mappings $p_{1}\left(Y_{1}\right), \ldots, p_{n}\left(Y_{n}\right)$ such that

$$
V_{F}(S)=p_{1}\left(V_{F}\left(U_{1}\right)\right) \cup \ldots \cup p_{n}\left(V_{F}\left(U_{n}\right)\right) .
$$

The discussion above shows that algebraic sets defined by quadratic equations are building blocks for construction of arbitrary algebraic sets over $F$. This allows us to focus now just on quadratic equations.

A standard quadratic equation over a group $G$ is an equation of the one of the following forms:

$$
\begin{gather*}
\prod_{i=1}^{n}\left[x_{i}, y_{i}\right]=1, \quad n>0  \tag{1}\\
\prod_{i=1}^{n}\left[x_{i}, y_{i}\right] \prod_{i=1}^{m} z_{i}^{-1} c_{i} z_{i} d^{-1}=1, \quad n, m \geq 0, \quad m+n \geq 1  \tag{2}\\
\prod_{i=1}^{n} x_{i}^{2}=1, \quad n>0  \tag{3}\\
\prod_{i=1}^{n} x_{i}^{2} \prod_{i=1}^{m} z_{i}^{-1} c_{i} z_{i} d^{-1}=1, \quad n, m \geq 0, \quad n+m \geq 1 \tag{4}
\end{gather*}
$$

where $d, c_{i}$ are nontrivial elements from $G$.
The equation $S=1$ is strictly quadratic in variables $X=\left\{x_{1}, \ldots, x_{n}\right\}$ if every letter from $X$ occurs in $S$ exactly twice. A quadratic, not strictly quadratic, equation is easy to solve over a group $G$ (it has the form $x=W(Y)$, where the variable $x$ does not occur in $W(Y)$ ).

In the case when $G$ is a free non-abelian group a strictly quadratic equation over $G$ is equivalent to a standard one in the following way. Let $S(X, Y)=1$ be a strictly quadratic equation in variables $X$ over $G$. Then there is an automorphism $\phi$ of the free
group $G * F(X \cup Y)$ such that $\phi$ fixes all the letters from $Y$ and all the elements from $G$ and such that $\phi(S)=1$ is a standard quadratic equation over $G$.

Thus the standard quadratic equations play a key part in constructing algebraic sets over free groups. This explains the following definition.

Definition 1 Let $S=1$ be a standard quadratic equation over a free group $F$. Then the algebraic set $V_{F}(S)$ is called an elementary neighborhood over $F$.

## 5 Implicit function theorem

In this section we formulate the implicit function theorem over free groups in its basic simplest form. We refer to [13] for the proofs and generalizations.

Let $F$ be a free non-abelian group. Recall that by an elementary neighborhood over $F$ we understand an algebraic set $V_{F}(S)$ defined by a standard quadratic equation $S=1$ over $F$. In general these neighborhoods are "rich" enough, but there are few exceptions. To define them we need the following definitions.

Strictly quadratic words of the type

$$
[x, y], x^{2}, z^{-1} c z
$$

where $c \in F$, are called atoms. It follows that any standard quadratic equation $S=1$ over $F$ can be written as a product of atoms $r_{i}$ :

$$
r_{1} r_{2} \ldots r_{k}=g \quad(\text { for some } g \in F)
$$

The minimal such number $k$ is called the atomic rank of $S=1$.
Definition $2 A$ solution $\phi$ of a quadratic equation $r_{1} r_{2} \ldots r_{k}=g$ of the atomic rank $k \geq 2$ is called commutative if $\left[r_{i}^{\phi}, r_{i+1}^{\phi}\right]=1$ for all $i=1, \ldots, k-1$.

The following standard quadratic equations have non-commutative solutions (see [11]:

1. $S=1$ is of type $1, n>2$,
2. $S=1$ is of type $2, n>0, n+m>1$,
3. $S=1$ is of type $3, n>3$,
4. $S=1$ is of type $4, n>2$.

Now we can describe equations which define "rich" neighborhoods. A standard quadratic equation $S=1$ over $F$ is called regular if its atomic rank is not less then 3 and it has a non-commutative solution. Elementary neighborhoods defined by such equations are called regular neighborhoods. Notice, that regular neighborhoods are irreducible in the Zariski topology [11].

Theorem 2 (Implicit function theorem) Let $T(X, Y)=1$ be an equation over a free group $F,|X|=m,|Y|=n$. Suppose that for any $A$ from a regular neighborhood $V_{F}(S) \subset F^{m}$ there exists a tuple of elements $B \in F^{n}$ such that $T(A, B)=1$. Then there exists a tuple of words $P=\left(p_{1}(X), \ldots, p_{n}(X)\right)$, with constants from $F$, such that $T(A, P(A))=1$ for any $A \in V_{F}(S)$.

## 6 Genus problem

In this section we apply the implicit function theorem for genus problem. We refer to [5], [6], [7] and [8] for some results and a general discussion of the genus problem. Here we focus only on the genus problem for non-orientable quadratic equations without coefficients.

Let $F$ be a non-abelian free group.
Definition 3 Let $f$ be a non-trivial element from the derived subgroup $[F, F]$ of $F$. Genus of $f$ is the minimal number of commutators, say $n$, such that $f$ can be expressed as a product of $n$ commutators.

Let us consider the quadratic equation

$$
\begin{equation*}
S_{n}=x_{1}^{2} \ldots x_{n}^{2}=1, \quad n \geq 4 \tag{5}
\end{equation*}
$$

where $x_{1}, \ldots, x_{n}$ are variables. For a solution $u=\left(u_{1}, \ldots, u_{n}\right)$ of the equation (5) denote by $p(u)$ the product $p(u)=u_{1} \ldots u_{n}$. Notice, that $p(u)^{2}=1$ modulo $[F, F]$. Since $F /[F, F]$ is torsion free, then $p(u) \in[F, F]$. By the genus of the solution $u$ we understand the genus of the element $p(u)$. Notice that $p(u)=1$ for every solution $u$ of the equation $S_{n}=1$ for $n=1,2,3$, hence the restriction $n \geq 4$.

Now we define the genus of the equation (5) as the supremum of the genus of all its solutions in the group $F$. The following problem was posed by A.Gaglione and D.Spellman.

Problem 1 What is the genus of the equation $x_{1}^{2} \ldots x_{n}^{2}=1 \quad(n \geq 4)$ ?
Even for the case $n=4$ it is difficult to find solutions of genus $\geq 2$ (all "easy" solutions have genus 1, see [16]). In [8] J. Comerford and Y. Lee gave the first example of a such solution with genus 2. D. Spellman recently came up with another solution of genus 2 of the equation $S_{4}=1$ (see [16]).

Using implicit function theorem we prove the following result.
Theorem 3 For each $n \geq 4$ the genus of the equation $S_{n}=1$ over a non-abelian free group $F$ is infinite.

Proof. Suppose the equation $S_{n}=1$ is of a finite genus, say $m$, over a non-abelian free group $F$. Then the following formula is true in $F$ :

$$
\begin{equation*}
\Phi_{n, m}=\forall x_{1} \ldots x_{n} \exists y_{1} z_{1} \ldots y_{m} z_{m}\left(x_{1}^{2} \ldots x_{n}^{2}=1 \rightarrow x_{1} \ldots x_{n}=\left[y_{1}, z_{1}\right] \ldots\left[y_{m}, z_{m}\right]\right) . \tag{6}
\end{equation*}
$$

According to the implicit function theorem the equation

$$
\begin{equation*}
x_{1} \ldots x_{n}=\left[y_{1}, z_{1}\right] \ldots\left[y_{m}, z_{m}\right] \tag{7}
\end{equation*}
$$

in variables $y_{1}, z_{1}, \ldots, y_{m}, z_{m}$ and constants $x_{1}, \ldots, x_{n}$ has a solution in the non-orientable surface group

$$
G_{S_{n}}=\left\langle x_{1}, \ldots, x_{n} \mid x_{1}^{2} \ldots x_{n}^{2}=1\right\rangle .
$$

But it is easy to see that the product $x_{1} \ldots x_{n}$ does not belong to the derived subgroup of $G_{S_{n}}$. This contradiction shows that the genus of the equation $S_{n}=1$ is infinite.

## 7 Abelianization of cartesian powers of a free nonabelian groups

Let $F$ be a free non-abelian group and $\lambda$ an infinite cardinal. Denote by $F_{\lambda}$ the unrestricted cartesian product of $\lambda$ copies of the group $F$.

Below, for a group $G$ by $A b(G)$ we denote the abelianization $G /[G, G]$ of $G$. The following result is an answer to the question posed by A.Gaglione and D.Spellman (see [10] and [16]), whether the abelianization of the group $F_{\lambda}$ is torsion-free.

Theorem 4 For any non-abelian free group $F$ and any infinite cardinal $\lambda$ the abelianization $A b\left(F_{\lambda}\right)$ of the cartesian power $F_{\lambda}$ has non-trivial elements of order 2.

Proof. Notice, that if $\lambda>\omega$, where $\omega$ is the first infinite cardinal, then $\lambda=\omega+\lambda$ and therefore

$$
F_{\lambda} \simeq F_{\omega} \times F_{\lambda} .
$$

Hence

$$
A b\left(F_{\lambda}\right) \simeq A b\left(F_{\lambda}\right) \times A b\left(F_{\omega}\right),
$$

which shows that it suffices to prove the theorem just for $\lambda=\omega$.
Consider the equation

$$
x_{1}^{2} x_{2}^{2} x_{3}^{2} x_{4}^{2}=1
$$

over the free group $F$. By Theorem 3 for each positive $n$ there exists a solution, say

$$
u(n)=\left(u(n)_{1}, u(n)_{2}, u(n)_{3}, u(n)_{4}\right)
$$

such that the element

$$
p(u(n))=u(n)_{1} u(n)_{2} u(n)_{3} u(n)_{4}
$$

can not be presented as a product of fewer then $n$ commutators in $F$. Denote by $U_{i}$ $(i=1, \ldots, 4)$ the following element of the cartesian power $F_{\omega}$ :

$$
U_{i}=\left(u(1)_{i}, u(2)_{i}, u(3)_{i}, \ldots, u(n)_{i}, \ldots\right),
$$

and put

$$
U=U_{1} U_{2} U_{3} U_{4}
$$

Then $U$ is not a product of finitely many commutators in $F_{\omega}$. Hence the image $\bar{U}$ of $U$ in the abelianization $A b\left(F_{\omega}\right)$ is not trivial. But $(\bar{U})^{2}=1$. So the abelianization $A b\left(F_{\omega}\right)$, as well as $A b\left(F_{\lambda}\right)$, has non-trivial 2-torsion, as desired.

## 8 Bibliography

## References

[1] S. Bachmuth, Automorphisms of free metabelian groups. Trans. Amer. Math. Soc. 118 (1965), 93-104.
[2] Baumslag G., Myasnikov A., Remeslennikov V., Algebraic geometry over groups I: Algebraic sets and ideal theory. To appear in J.of Algebra.
[3] J. S. Birman, An inverse function theorem for free groups. Proc. Amer. Math. Soc. 41 (1973), 634-638.
[4] J. S. Birman, Braids, Links and Mapping class groups. Annals of Math. Studies, Princeton Univ. Press. Amer. Math. Soc. (1975).
[5] M. Culler, Using surfaces to solve equations in free groups. Topology 20 (1981), 133-145.
[6] A.Duncan, J. Howie, The genus problem for one-relator products of locally indicable groups. Math. Z. 208 (1991), 225-237.
[7] L. P. Comerford, C. C. Edmunds, Genus of powers in a free group. In Geometric Group Theory (Eds.: Charney/Davis/Shapiro), Walter de Gruyter, Berlin, New York, 1995.
[8] J. A. Comerford, Y. Lee, Products of two commutators as a square in a free group. Canad. Math. Bull. 33 (1990), 190-196.
[9] R. H. Fox, Free differential calculus. I. Derivations in free group rings. Ann. of Math. (2) 57 (1953), 547-560.
[10] Unsolved problems in Group Theory. Kaurovka Notebook., Novosibirsk, 1995.
[11] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. 1: irreducibility of quadratic equations and nullstellensatz. J. of Algebra, 200 (1998), 472-516 .
[12] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. 2: systems in triangular quasi-quadratic form and description of residually free groups. J. of Algebra, 200 (1998), 517-570.
[13] O. Kharlampovich and A. Myasnikov. Elementary theory of free non-abelian groups I. Implicit function theorems and Skolem functions. To appear.
[14] A. F. Krasnikov, Generators of the group $F /[N, N]$. Math. Notes 24 (1979), 591-594.
[15] R. C. Lyndon, Cohomology theory of groups with a single defining relation. Ann. of math. 52 (1950), 650-665.
[16] Magnus software project on combinatorial group theory, http://zebra.sci.ccny.cuny.edu/web/exper.html
[17] V. A. Romankov, Criteria for the primitivity of a system of elements of a free metabelian group. Ukrainskii Mat. Zh. 43 (1991), 996-1002.
[18] U. U. Umirbaev, Partial derivatives and endomorphisms of some relatively free Lie algebras. Sibirsk. Mat. Zh. 34 (1993), no. 6, 179-188. English translation: in Sib. Math. J.

