Galois symmetries in super Yang-Mills theories

JHEP03(2009)128

(http://iopscience.iop.org/1126-6708/2009/03/128)

Published by IOP Publishing for SISSA

Received: *January 28, 2009*
Accepted: *February 28, 2009*
Published: *March 25, 2009*

Galois symmetries in super Yang-Mills theories

Frank Ferrari[a,b]

[a] *Service de Physique Théorique et Mathématique, Université Libre de Bruxelles and International Solvay Institutes, Campus de la Plaine, CP 231, B-1050 Bruxelles, Belgique*

[b] *Simons Center for Geometry and Physics, Stony Brook University, Stony Brook, NY 11794-3840, U.S.A.*

E-mail: frank.ferrari@ulb.ac.be

Abstract: Classifying the phases of gauge theories is hindered by the lack of local order parameters. In particular, the standard Wilson's and 't Hooft's non-local order parameters are known to be insufficient to explain the existence of the plethora of phases that are found in supersymmetric gauge theories. Motivated by these observations, we reanalyze the concept of gauge symmetry breaking using Galois theory. Unlike the ordinary classical notion of unbroken gauge group, the Galois symmetry makes sense in the full quantum theory and must be a phase invariant. The algebraic structure underlying the space of vacua of supersymmetric gauge theories, that we have developed recently, is precisely designed to allow a rigorous mathematical implementation of these ideas.

Keywords: Supersymmetric gauge theory, Gauge Symmetry, Nonperturbative Effects, Differential and Algebraic Geometry

ArXiv ePrint: 0901.4079

doi:10.1088/1126-6708/2009/03/128

JHEP03(2009)128

Contents

1 Introduction

The fundamental idea, due to Landau, to understand and classify the possible phases of a physical system is based on the concept of symmetry. Suppose that the physics is invariant under some symmetry group in some regime. Since the group structure is rigid, it cannot change when the parameters of the theory are varied, except by going through a singularity, which corresponds to a phase transition. The symmetry group can thus be used to characterize the phases. In particular, if in some regime the symmetry group is E and in

JHEP03(2009)128

another regime it is $E' \neq E$, then a smooth interpolation between the two regimes cannot exist: they must be in different phases. For example, it is not possible to go smoothly from solid to liquid water (the liquid has full translational symmetry whereas in the solid this symmetry is broken down to a discrete subgroup), whereas the transition from liquid to vapour can be smooth (this is associated with the existence of the critical point in the water phase diagram).

The symmetry E can be determined by computing the expectation values of observables, called order parameters in this context, that transform non-trivially under E. One of the main interest in Landau's ideas is that this computation can be done *locally* in parameter space, i.e. by looking at the system in some particular regime, without needing to probe the full phase diagram. For example, the translational symmetry of the liquid/vapour phase of water can be seen by looking at a regime of pressure and temperature where water looks like a liquid, or like vapour, but one doesn't need to look at both. The fact that they belong to the same phase ensures that the result for E will be the same in both regimes. In other words, the symmetry E is a *phase invariant*. It is a very powerful tool, because from a local analysis one obtains global constraints on the phase diagram.

One would like to apply the same ideas to classify the phases of gauge theories. However, in this case, one runs into well-known subtleties. The basic difficulty is that gauge invariance is not really a symmetry. It is more accurately described as a redundancy in the description of the system under consideration. Physical observables must be gauge invariant and thus we do not see the gauge group, at least in any obvious way, in the physics. In particular, there is no obstacle in principle in having equivalent physical theories based on two different gauge groups, or in having vacua belonging to the same phase but having different patterns of gauge symmetry breaking. There is also no obstacle in principle in having a formulation of the theory based only on physical observables, in which the original notion of gauge invariance is altogether absent. Actually, this is exactly what happens in the closed string description of gauge theories.

To be a little bit more precise, let us consider a four dimensional gauge theory based on a compact Lie group G and let us denote by $\mathscr{G}$ the group of local gauge transformations. As a consequence of Gauss' law, the theory is defined by modding out by the group $\mathscr{G}_0$ of gauge transformations that are connected to the identity. One is thus left in principle with a symmetry group $\mathscr{G}/\mathscr{G}_0 = G_\infty \simeq G$ which is often called "the group of gauge transformations at infinity." Imagine now that you consider a local observable $\mathcal{O}(x)$. As for any observable in the theory, it must be invariant under $\mathscr{G}_0$. But for a *local* operator, invariance under $\mathscr{G}_0$ obviously implies invariance under $\mathscr{G}$ and thus G_∞ as well. Thus we see that in gauge theory, *there is no local order parameter*, at least in any obvious sense.[1]

On the other hand, one can use non-local order parameters, like the Polyakov-'t Hooft-Wilson's lines. This yields many interesting results. For example, it is widely believed that the so-called 't Hooft's classification of the *massive* phases of gauge theories that one obtains in this way is complete (see for example [1] for a nice discussion and references).

[1] Of course gauge theories may have global symmetries and associated local order parameters. We are focusing in this paper on the possibility to use the gauge symmetry itself in order to distinguish the phases and thus in particular to understand the phase structure of gauge systems that do not have a global symmetry.

Unfortunately, for phases with no mass gap, 't Hooft's arguments are not powerful enough to provide a complete classification. These massless phases are ubiquitous in gauge theories, since they occur for instance each time there is a massless photon in the spectrum.

Our goal in the present paper is to try to shed some new light on this problem by using the nice mathematical structures underlying the solutions of $\mathcal{N}=1$ supersymmetric gauge theories [2]. We shall see that the concept of gauge symmetry breaking which, in its usual form, makes sense only classically, can be elevated to a well-defined quantum concept using Galois theory. The Galois symmetry is shown to be a phase invariant and thus can be used to classify the phases, in line with Landau's ideas. The Galois group is also an intrinsic property of the phase, independent of the particular realization of the phase in a given model.

For concreteness, we shall focus on the paradigmatic example of the $\mathcal{N}=1$ theory with gauge group $\mathrm{U}(N)$, one adjoint chiral multiplet ϕ and tree-level superpotential $\operatorname{Tr} W(\phi)$ such that

$$W'(z)=\sum_{k=0}^{d} g_k z^k = g_d\prod_{i=1}^{d}(z-w_i)\,. \tag{1.1}$$

As is well known, the vacua of this model can be labeled as $|N_1,k_1;\ldots;N_d,k_d\rangle$, where $0\leq k_i\leq N_i-1$. The integer N_i corresponds to the number of eigenvalues of ϕ that are equal to w_i classically. The pattern of gauge symmetry breaking in $|N_1,k_1;\ldots;N_d,k_d\rangle$ is thus $\mathrm{U}(N)\rightarrow\mathrm{U}(N_1)\times\cdots\times\mathrm{U}(N_d)$. The integer k_i is associated with chiral symmetry breaking in the unbroken factor $\mathrm{U}(N_i)$ of the gauge group. The phase structure of this model is extremely rich and has been much studied in the literature [2–5]. The standard analysis yields two phase invariants: the rank r and the confinement index t. The rank of $|N_1,k_1;\ldots;N_d,k_d\rangle$ is the number of non-zero integers N_i. Physically it corresponds to the rank of the low energy gauge group, which is $\mathrm{U}(1)^r$ taking into account the mass gap in the simple non-abelian factors $\mathrm{SU}(N_i)$ for $N_i\geq 2$. The confinement index t is defined to be the smallest integer such that the t^{th} tensor product of the fundamental representation of $\mathrm{U}(N)$ does not confine [5]. It can be shown that the confinement index in the vacuum $|N_1,k_1;\ldots;N_d,k_d\rangle$ is given by

$$t=N_1\wedge\cdots\wedge N_d\wedge(k_1-k_2)\wedge\cdots\wedge(k_1-k_d)\,, \tag{1.2}$$

where $a\wedge b$ represents the greatest common divisor of two integers a and b [5]. It is elementary to show directly on the solution of the model that r and t are indeed phase invariants, i.e. that they cannot change under analytic continuation (see for example the discussion in section 5.2.2 of [2]). The main result of the present paper will be to construct a new phase invariant, the Galois group.

The plan of the paper is as follows. In section 2, we review some background material from [2] that will be useful for our analysis. In section 3 we revisit the concept of gauge symmetry breaking. The usual notion does not make sense at the quantum level, but we show that a related notion actually does. This leads to the Galois symmetries. We also briefly explain the relation to Galois theory of algebraic equations. In section 4 we analyse some basic properties of the Galois groups associated with the phases, showing explicitly that they are phase invariants and that they are intrinsic characteristics of the phases. In section 5 we provide a few explicit calculations in simple cases. Finally we conclude in section 6.

JHEP03(2009)128

Important remark. The reader is not assumed to be familiar with Galois theory. We have included in the discussion all the required notions, which are fairly elementary, from a physicist point of view. Excellent references on Galois theory are listed in [6].

Notation and terminology. In the following, a *field* is a ring in which every non-zero element has an inverse. If R is a ring (which may be a field), we denote by $R[X_1, \ldots, X_n]$ the polynomial ring in n variables. If K is a field, we denote by $K(X_1, \ldots, X_n)$ the field of rational functions in n variables.

2 Background material

Let us consider an arbitrary $\mathcal{N} = 1$ supersymmetric gauge theory in four dimensions. Let us denote by $\boldsymbol{g}$ the set of parameters that enter in the tree-level superpotential and by $\boldsymbol{q}$ the set of instanton factors that are associated with each simple non-abelian factor of the gauge group. In the case of the $\mathrm{U}(N)$ theory with one adjoint and tree-level superpotential W with W' given by (1.1), one has $\boldsymbol{g} = (g_0, \ldots, g_d)$ and there is a unique instanton factor given in terms of the dynamically generated scale Λ by $q = \Lambda^{2N}$. The parameters $\boldsymbol{g}$ and $\boldsymbol{q}$ are best viewed as background chiral superfields. The *ring of parameters* a of the theory is defined to be the polynomial ring[2]

$$\mathsf{a} = \mathbb{C}[\boldsymbol{g}, \boldsymbol{q}]\,. \tag{2.1}$$

The chiral ring. Any chiral operator in the theory can be expressed as a finite sum of finite products of a finite set of generators $\mathcal{O}_1, \ldots, \mathcal{O}_n$. In other words, any chiral operator $\mathcal{O}$ can be written in the form

$$\mathcal{O} = \rho_{\mathcal{O}}(\mathcal{O}_1, \ldots, \mathcal{O}_n)\,, \tag{2.2}$$

where $\rho_{\mathcal{O}} \in \mathsf{a}[X_1, \ldots, X_n]$ is a polynomial in n variables and coefficients in a. For example, in the $\mathrm{U}(N)$ theory with the adjoint field ϕ, the generators $\mathcal{O}_i$ can be taken to be the

$$u_k = \operatorname{Tr} \phi^k \tag{2.3}$$

for $1 \leq k \leq N$ together with the generalized glueball operators $v_k = -\frac{1}{16\pi^2} \operatorname{Tr} W^\alpha W_\alpha \phi^k$ for $0 \leq k \leq N-1$.

An *operator relation* between chiral operators $\mathcal{O}^{(1)}, \ldots, \mathcal{O}^{(p)}$ is a relation of the form

$$P(\mathcal{O}^{(1)}, \ldots, \mathcal{O}^{(p)}) = 0\,, \tag{2.4}$$

where $P \in \mathsf{a}[X_1, \ldots, X_p]$, which is valid in all the vacua of the theory. This definition is unambiguous because, as is well-known, chiral operators expectation values factorize, for example $\langle P(\mathcal{O}^{(1)}, \ldots, \mathcal{O}^{(p)})\rangle = P(\langle \mathcal{O}^{(1)}\rangle, \ldots, \langle \mathcal{O}^{(p)}\rangle)$. A crucial constraint on the form of an operator relation is that the coefficients of the polynomial P in (2.4) must be in a, i.e.

[2] As explained in great details in [2], there are cases where this ring must be enlarged, in particular in theories that have a zero β function. These cases will not enter into the present paper.

JHEP03(2009)128

must be polynomials in the parameters $\boldsymbol{g}$ and $\boldsymbol{q}$. As explained in [2], the full set of operator relations always follows from a finite number of relations between a set of generators,

$$P_i(\mathcal{O}_1, \ldots, \mathcal{O}_n) = 0\,, \quad P_i \in \mathsf{a}[X_1, \ldots, X_n]\,, \quad 1 \leq i \leq m\,. \tag{2.5}$$

A fundamental result derived in [2] is that, in all cases, the expectation values of the generators (and thus of any other chiral operator from (2.2)) are unambiguously fixed by the relations (2.5).

The ring generated by the chiral operators is called the quantum chiral ring A. The equations (2.2) and (2.5) show that this ring is a quotient ring given by

$$\mathsf{A} = \mathsf{a}[X_1, \ldots, X_n]/\mathscr{I} = \mathbb{C}[\boldsymbol{g}, \boldsymbol{q}, X_1, \ldots, X_n]/\mathscr{I}\,, \tag{2.6}$$

where $\mathscr{I}$ is the ideal generated by the full set of operator relations,

$$\mathscr{I} = (P_1, \ldots, P_m)\,. \tag{2.7}$$

The quantum chiral ring A defined above cannot have nilpotent elements [2], i.e. $\mathcal{O}^s = 0$ in A for some $s \in \mathbb{N}$ implies that $\mathcal{O} = 0$. Equivalently, the ideal $\mathscr{I}$ is radical.

Note that the knowledge of the chiral ring A is *equivalent* to the knowledge of the full solution of the theory in the chiral sector. Indeed, the ring A can be constructed from the knowledge of the expectation values $\langle \mathcal{O} \rangle$ for all $\mathcal{O}$ and conversely, the full set of expectation values can be found from the structure of the chiral ring via the relations (2.5) [2].

Geometry. The polynomial equations (2.5) define an affine algebraic variety $\mathscr{M}$ that we shall call the *chiral variety* of the theory. The chiral ring A corresponds to the ring of regular functions defined on $\mathscr{M}$, also called the coordinate ring of $\mathscr{M}$,

$$\mathsf{A} = \mathbb{C}[\mathscr{M}]\,. \tag{2.8}$$

There are thus three *equivalent* ways to present the solution of the model: a standard way by giving the full set of expectation values; an algebraic way by giving the ring A; a geometric way by giving the variety $\mathscr{M}$.

To make the link between the geometric perspective and the standard notions of vacua and expectation values, one can consider the intersection of the space $\mathscr{M}$ with the linear spaces of constant parameters $\boldsymbol{g}$ and $\boldsymbol{q}$. Generically, there is a finite number v of intersection points, corresponding to a finite number of solutions to the algebraic equations (2.5) in which the parameters $\boldsymbol{g}$ and $\boldsymbol{q}$ are fixed to some particular complex numbers. Each solution yields the expectation values in a particular vacuum $|i\rangle$ of the theory. In this picture, the variety $\mathscr{M}$ is thus viewed as a v-fold cover of $\mathbb{C}^\delta$, where δ is the total number of parameters $\boldsymbol{g}$ and $\boldsymbol{q}$, and the expectation values are v-valued analytic functions of $\boldsymbol{g}$ and $\boldsymbol{q}$. In particular, on each sheet (i.e. in each vacuum) there is a semi-classical region corresponding to small values of $\boldsymbol{q}$, with a certain pattern of gauge symmetry breaking and chiral symmetry breaking.

In some special theories, the equations (2.5), instead of having a finite number of solutions for fixed $\boldsymbol{g}$ and $\boldsymbol{q}$, have a continuum of solutions corresponding to a moduli space of vacua. The variety $\mathscr{M}$ may then be viewed as a fibered space with base $\mathbb{C}^\delta$, the fiber over a point $(\boldsymbol{g}, \boldsymbol{q})$ being the moduli space of vacua for given parameters $\boldsymbol{g}$ and $\boldsymbol{q}$.

JHEP03(2009)128

Phases. The description of $\mathscr{M}$ as a v-fold cover of $\mathbb{C}^\delta$ is quite arbitrary. Equivalently, the usual notion of a vacuum is quite arbitrary. A much better defined concept in the full quantum theory is the notion of *phase* [2]. The chiral variety $\mathscr{M}$ decomposes into *irreducible* components according to the phase structure of the model,

$$\mathscr{M} = \bigcup_{\varphi} \mathscr{M}_{|\varphi)} . \tag{2.9}$$

Each irreducible component $\mathscr{M}_{|\varphi)}$ corresponds to a given phase, denoted by $|\varphi)$, of the theory [2].

A phase may contain several vacua. A fundamental property is that one can always interpolate smoothly between two vacua in the same phase by performing analytic continuations along closed loops in $(\boldsymbol{g}, \boldsymbol{q})$ space [2–5]. Conversely, vacua in different phases *cannot* be smoothly connected to each other. Different irreducible components of $\mathscr{M}$ may intersect, but going from one component to the other is a non-analytic process associated with a second order phase transition.

The phase diagram of the theory, or equivalently the decomposition (2.9), can be derived in principle by performing the most general analytic continuations on the expectation values, finding in this way which vacua can be smoothly connected to each other and which cannot. This method is very cumbersome to implement in non-trivial cases, but fortunately the problem has an equivalent algebraic formulation that turns out to be much more powerful [2]. Finding the decomposition (2.9) is equivalent to decomposing the ideal $\mathscr{I}$ of operator relations into prime ideals,

$$\mathscr{I} = \bigcap_{\varphi} \mathscr{I}_{|\varphi)} . \tag{2.10}$$

In practice, this can often be done by factorizing suitable polynomials into irreducible factors, which yields an elegant and effective method to compute the phase diagram [2].

Vacua in a given phase can look very different. For example, they can have different patterns of gauge symmetry breaking [5], showing most clearly that the gauge group is not a real symmetry and cannot be used to classify the phases. In the following, our main goal will be to uncover an underlying symmetry shared by all the vacua in a given phase.

The field of a phase. In general, the chiral ring A defined by (2.6) has zero divisors, i.e. non-zero elements $\mathcal{O}$ and $\mathcal{O}'$ such that

$$\mathcal{O}\mathcal{O}' = 0 . \tag{2.11}$$

This possibility is directly related to the existence of several phases. Indeed, (2.11) implies that one can split the vacua into two sets, those for which $\langle\mathcal{O}\rangle = 0$ but $\langle\mathcal{O}'\rangle \neq 0$ and those for which $\langle\mathcal{O}'\rangle = 0$ but $\langle\mathcal{O}\rangle \neq 0$. Clearly one cannot join these two sets of vacua by analytic continuation. Morevoer, we see that in a given phase there are new relations, like $\mathcal{O} = 0$ or $\mathcal{O}' = 0$, that are valid in all the vacua of the phase but not in all the vacua of the theory. The full set of relations valid in the phase $|\varphi)$ is generated by the ideal $\mathscr{I}_{|\varphi)}$ in the decomposition (2.10). This ideal is *prime*, which means that the chiral ring in the phase $|\varphi)$,

$$\mathsf{A}_{|\varphi)} = \mathsf{a}[X_1, \dots, X_n]/\mathscr{I}_{|\varphi)} , \tag{2.12}$$

has no zero divisor. This is equivalent to the irreducibility of $\mathscr{M}_{|\varphi)}$ in (2.9), and we have

$$\mathsf{A}_{|\varphi)} = \mathbb{C}[\mathscr{M}_{|\varphi)}] \,. \tag{2.13}$$

Rings that do not have zero divisors are called integral domains. The simplest example is the ring of integers $\mathbb{Z}$. Their fundamental property is that one can consistently consider fractions of the elements of the ring and build a field of fractions in the same way as one builds the field of rational numbers $\mathbb{Q}$ from $\mathbb{Z}$. The field of fraction of $\mathsf{A}_{|\varphi)}$ will be called the *chiral field in the phase* $|\varphi)$ and denoted by $\mathsf{K}_{|\varphi)}$. It is simply the field of rational functions on the irreducible variety $\mathscr{M}_{|\varphi)}$,

$$\mathsf{K}_{|\varphi)} = \mathrm{Frac}(\mathsf{A}_{|\varphi)}) = \mathbb{C}(\mathscr{M}_{|\varphi)}) \,. \tag{2.14}$$

When the theory has a finite number of vacua, this field has an extremely simple description. There always exists an operator $\mathscr{O}_{|\varphi)}$, called a primitive operator in [2] (there are many primitive operators in a given phase), such that

$$\mathsf{K}_{|\varphi)} = \mathsf{k}[\mathscr{O}_{|\varphi)}] = \mathsf{k}[X]/(P_{\mathscr{O}_{|\varphi)}}) \,, \tag{2.15}$$

where

$$\mathsf{k} = \mathrm{Frac}(\mathsf{a}) = \mathbb{C}(\boldsymbol{g}, \boldsymbol{q}) \tag{2.16}$$

is the field of parameters of the theory. The result (2.15) is very powerful. It means that in a given phase, *all* the chiral operators can be expressed as simple polynomials with coefficients in k of a given primitive operator $\mathscr{O}_{|\varphi)}$. All the non-trivial structure is contained in the single irreducible polynomial equation $P_{\mathscr{O}_{|\varphi)}} = 0$ satisfied by $\mathscr{O}_{|\varphi)}$ in the phase $|\varphi)$. The irreducibility of this equation ensures that any rational function of the chiral operators can always be rewritten as a polynomial in $\mathscr{O}_{|\varphi)}$.

What one needs to remember. Chiral operators satisfy a set of algebraic equations generated by an ideal $\mathscr{I}$ that determines completely the expectation values in all the vacua of the theory. These algebraic equations define an algebraic variety $\mathscr{M}$, and the chiral operators are simply the regular functions on this variety. Phases $|\varphi)$ of the gauge theory correspond to irreducible components $\mathscr{M}_{|\varphi)}$ of $\mathscr{M}$. On $\mathscr{M}_{|\varphi)}$, chiral operators satisfy additional relations generated by a prime ideal $\mathscr{I}_{|\varphi)} \supset \mathscr{I}$. Thanks to these relations, the chiral operators in a given phase are actually elements of a field $\mathsf{K}_{|\varphi)}$, the chiral field in the phase $|\varphi)$, which is the field of rational functions on $\mathscr{M}_{|\varphi)}$. This fact will be of utmost importance in the following. When the theory has a finite number of vacua, the chiral field in a phase is generated by a single operator and has thus the very simple description (2.15).

3 Galois symmetries

We are now going to explain how Galois' ideas allow to circumvent, in a very subtle and interesting way, the argument showing that the gauge group cannot be seen in the algebra of local observables. The idea is to build the gauge variant quantities, as for example the eigenvalues of the adjoint field ϕ, from the gauge invariant algebraic equations these

JHEP03(2009)128

quantities must satisfy. It turns out that the gauge symmetry can be spontaneously broken by this construction. The unbroken symmetry, which is a subgroup of the gauge group, is a group of automorphisms called the Galois group.

3.1 General considerations

In the quantum gauge theory, we have direct access to particular combinations of the matrix elements ϕ_{ij}, $1 \leq i, j \leq N$, that are gauge invariant,

$$u_k = \operatorname{Tr} \phi^k = \phi_{i_1 i_2} \phi_{i_2 i_3} \cdots \phi_{i_k i_1} \, , \tag{3.1}$$

but not to the matrix ϕ itself on which the gauge group acts. Since our goal is to use the gauge group, we need to reconstruct the gauge variant objects ϕ_{ij}. Note that this is an extremely simple case of the much more general problem of reconstructing open string degrees of freedom from closed strings. The puzzle is that, to build the ϕ_{ij}, we can use only the physical information contained in the gauge invariants u_k.

The key to the solution of this problem is to characterize the ϕ_{ij} by the set of algebraic equations *with gauge invariant coefficients* that they must satisfy. This set of equations is not difficult to find in our case. Let us introduce the characteristic polynomial

$$C(z) = \det(z - \phi) = z^N + \sum_{k=1}^{N} (-1)^k \sigma_k z^{N-k} \, , \tag{3.2}$$

where the σ_ks can be expressed in terms of the u_ks using the standard Newton's formulas,

$$\sigma_1 = u_1 \, , \ \sigma_2 = \frac{1}{2}\bigl(u_1^2 - u_2\bigr) \, , \ \sigma_3 = \frac{1}{6}\bigl(u_1^3 - 3u_1 u_2 + 2u_3\bigr) \, , \ldots \tag{3.3}$$

The Cayley-Hamilton theorem implies that the matrix equation

$$C(\phi) = \phi^N + \sum_{k=1}^{N} (-1)^k \sigma_k \phi^{N-k} = 0 \tag{3.4}$$

must be valid. This yields N^2 algebraic equations for the matrix coefficients ϕ_{ij}. The idea is then to study the symmetry properties of the algebraic structure that describes the extension from the set of variables u_k to the set of variables ϕ_{ij} governed by the equations (3.4).

In order to simplify the discussion, while keeping the main relevant features, we are going to focus on the symmetric subgroup $\mathrm{S}_N \subset \mathrm{U}(N)$ of the gauge group, generated by the permutation matrices $U_{ij} = \delta_{i\sigma(j)}$ for $\sigma \in \mathrm{S}_N$. This means that instead of decomposing the traces in terms of the ϕ_{ij} as in (3.1), we are going to use the simpler decomposition

$$u_k = \operatorname{Tr} \phi^k = \sum_{i=1}^{N} x_i^k \, , \quad 1 \leq k \leq N \, . \tag{3.5}$$

The group S_N acts by permuting the x_is,

$$\sigma : \ x_i \longmapsto x_{\sigma(i)} \, . \tag{3.6}$$

JHEP03(2009)128

The x_is are the roots of the characteristic polynomial,

$$C(x_i) = 0\,, \quad 1 \le i \le N\,. \tag{3.7}$$

This gauge invariant set of equations fully characterize the x_is, in the sense that

$$C(z) = \prod_{i=1}^{N} (z - x_i) \tag{3.8}$$

immediately implies that

$$\sigma_k = \sum_{i_1<\cdots<i_k} x_{i_1} \cdots x_{i_k}\,, \quad 1 \le k \le N\,, \tag{3.9}$$

and then (3.5) follows from Newton's formulas. The x_is may be interpreted as being the eigenvalues of the matrix ϕ, but this is not necessary and ϕ does not need to be diagonalizable. The important point is that (3.5) is equivalent to (3.7), from purely algebraic manipulations.

At first sight, the above construction does not seem very promising to achieve our goal of classifying the phases using the gauge symmetry. It is true that we can define the x_is from the gauge invariant data, since the equation $C(z) = 0$ clearly is gauge invariant, but it looks like that we really obtain the x_is only modulo the action of the permutation group. It is not obvious to see how some order parameter, or phase invariant, could emerge from such a construction.

In order to gain some insight into how things might work out, let us look at the classical theory. The matrix ϕ must satisfy the constraint

$$W'(\phi) = 0 = \prod_{i=k}^{d} (\phi - w_k) \tag{3.10}$$

in this case. The most general solution is labeled as $|N_1; \ldots ; N_d\rangle$, where N_k gives the number of x_i equal to w_k. One says that the gauge group $\mathrm{U}(N)$ is broken down to $\mathrm{U}(N_1) \times \cdots \times \mathrm{U}(N_d)$ for this particular solution. The unordered set of integers $\{N_k\}$ completely characterizes the phase at the classical (or perturbative) level. The crucial point here is that all this non-trivial information is actually contained in the equations (3.7), without the need to use the matrix ϕ explicitly. Indeed, the integers N_k simply give the multiplicity of the roots of the gauge invariant characteristic polynomial C in (3.2). These multiplicities are coded in the special algebraic relations the gauge invariant u_ks (or σ_ks) satisfy. For example, if there is only one double root ($\mathrm{U}(N)$ broken down to $\mathrm{U}(2) \times \mathrm{U}(1)^{N-2}$), then the discriminant of the polynomial must vanish. This constraint on the coefficients of C characterizes the $\mathrm{U}(N) \to \mathrm{U}(2) \times \mathrm{U}(1)^{N-2}$ pattern of gauge symmetry breaking, yet it is completely gauge invariant. More generally, for a given set of integers $\{N_k\}$, the coefficients of C will satisfy a set of constraints generating a certain prime ideal and corresponding to a certain irreducible algebraic variety. These constraints are equivalent to the fact that the characteristic polynomial takes the form

$$C(z) = \prod_{k} (z - w_k)^{N_k} \tag{3.11}$$

JHEP03(2009)128

and can be derived by eliminating the w_k from the equations obtained by equating the coefficients of various powers of z in (3.11).

In the quantum theory, the coefficients of the characteristic polynomial will still satisfy special algebraic constraints in a given phase. As reviewed in section 2, these constraints generate a prime ideal $\mathscr{I}_{|\varphi)}$. However, these constraints will no longer imply that C has multiple roots and the x_k will be all distinct. In other words, the usual notion of gauge symmetry breaking will be useless in the quantum theory. This is of course not surprising, since it is known that the set of integers $\{N_k\}$ is not a phase invariant in the full quantum theory. However, Galois theory teaches us that we still have a well-defined and non-trivial notion of gauge symmetry breaking that can be used to classify the phases, as we now explain.

3.2 The Galois group

According to section 2, in a given phase $|\varphi)$, the gauge invariant observables belong to a field $\mathsf{K}_{|\varphi)}$, the chiral field in the phase $|\varphi)$. In particular, the coefficients of the characteristic polynomial C are elements of $\mathsf{K}_{|\varphi)}$,

$$C \in \mathsf{K}_{|\varphi)}[X]\,. \tag{3.12}$$

3.2.1 The space of eigenvalues

As a first step, we need to define precisely the space in which the roots x_i of the characteristic polynomial live. The construction is based on the following theorem.

Theorem 1 *Let $Q \in K[X]$ be a polynomial with coefficients in some field K. Then there exists an extension field $S \supset K$, unique up to field isomorphisms, such that*

(i) Q factorizes into linear factors in S, i.e. $Q(z) = \prod_{k=1}^{N}(z - x_k)$ with $x_k \in S$.

(ii) S is generated by the roots of Q over K, $S = K(x_1, \dots, x_N)$.

The field S is called the splitting field of the polynomial Q.

We shall denote by $\mathsf{S}_{|\varphi)}$ the splitting field of the characteristic polynomial C in the phase $|\varphi)$. Note that even though the roots of C are not gauge invariant, the notion of the splitting field is a perfectly well-defined and gauge invariant concept, since it is uniquely determined in terms of the gauge invariant polynomial $C \in \mathsf{K}_{|\varphi)}[X]$. In physical terms, th. 1 provides a very precise statement about the construction of gauge-variant data (or "open string variables"), which are the roots x_i, from gauge invariant data (the "closed string variables"), which are the completely symmetric polynomials in the roots. The splitting field is the space in which the gauge-variant data lives.

3.2.2 Gauge symmetry breaking à la Galois

The construction of $\mathsf{S}_{|\varphi)}$ is perfectly S_N-symmetric, yet, as Galois realized, this symmetry can be spontaneously broken. This yields a new version of the concept of gauge symmetry breaking that makes sense in the quantum theory and that, as we shall explain in details in the following, is a phase invariant.

Galois' notion of symmetry breaking can be introduced as follows. Consider a polynomial $Q \in K[X]$, where K is a field, and let $S = K(x_1, \ldots, x_N)$ be its splitting field. Let $\mathscr{O}$ be an arbitrary element of S. $\mathscr{O}$ is a rational function of the roots with coefficients in K, $\mathscr{O} = \mathscr{O}(x_1, \ldots, x_N)$. Let us ask the following question: what conditions do we need to impose on $\mathscr{O}$ to ensure that $\mathscr{O} \in K$? Clearly, a *sufficient* condition is to impose full symmetry of $\mathscr{O}$ under arbitrary permutations of the roots. This condition is also necessary if Q is a generic polynomial (i.e. a polynomial for which the coefficients are algebraically independent over K). However, this condition is *not* necessary in general. For example, a given Q might have some of its roots in K, in which case *any* rational function of these roots is of course in K. One of the main result in Galois theory is to show that the necessary and sufficient condition for $\mathscr{O} \in S$ to be in K is governed by a symmetry principle.

More precisely, the symmetric subgroup S_N of the gauge group acts on $\mathscr{O} \in S$ as

$$\sigma \cdot \mathscr{O}(x_1, \ldots, x_N) = \mathscr{O}(x_{\sigma(1)}, \ldots, x_{\sigma(N)}) . \tag{3.13}$$

We then have the following theorem.

Theorem 2 *Let K be a field of characteristic zero (i.e. that contains $\mathbb{Q}$ as a subfield), $Q \in K[X]$ and S be its splitting field. There always exists a subgroup G of the permutation group S_N, called the Galois group of the polynomial Q, such that, for any $\mathscr{O} \in S$,*

$$\mathscr{O} \in K \Longleftrightarrow \sigma \cdot \mathscr{O} = \mathscr{O} \text{ for all } \sigma \in G . \tag{3.14}$$

In our case, $K = \mathsf{K}_{|\varphi)}$ is automatically of characteristic zero (since it contains $\mathbb{C}$) and the polynomial we consider is the characteristic polynomial.

Definition 1 *The* Galois group $G_{|\varphi)}$ of the phase $|\varphi)$ *is the Galois group of the characteristic polynomial $C \in \mathsf{K}_{|\varphi)}[X]$.*

Theorem 2 means that $G_{|\varphi)}$-invariant operators are physical. This may be confusing, since being $G_{|\varphi)}$-invariant is in general a *weaker* statement than being S_N-invariant, which is the standard condition for gauge invariance. However, it is important to realize that, even when $G_{|\varphi)}$ is a strict subgroup of S_N, the set of observables is not larger than usual and is still given by the completely symmetric functions in the roots. The theorem simply ensures that any $G_{|\varphi)}$-symmetric operator can be expressed unambiguously in terms of S_N-symmetric operators, or in other words that the $G_{|\varphi)}$-symmetric operators are completely fixed in terms of gauge invariant data only.

Very interestingly, the fact that the Galois group can be a strict subgroup of S_N is just an example of the familiar concept of symmetry breaking. Symmetry breaking occurs when then equations of the problem under consideration are symmetric, but the solution is not. In the case of a polynomial $Q \in K[X]$, the problem is the construction of the splitting field S in terms of Q and K. The equations that determine S are S_N-symmetric, but the structure of S may not be S_N-symmetric. In mathematical terms, this means that the group of automorphisms of S may be smaller than S_N.

The precise statements are as follows. Let $\mathrm{Gal}(S|K)$ be the group of K-automorphisms of S, i.e. automorphisms of S that act trivially on K. The polynomial $Q \in K[X]$ is clearly

JHEP03(2009)128

invariant under any element of $\mathrm{Gal}(S|K)$ and thus a K-automorphism acts by permuting the eigenvalues x_i. Moreover, a K-automorphism is completely determined by the permutation it induces on the roots, since $S = K(x_1, \ldots, x_N)$. One then has the following theorem.

Theorem 3 *The group of automorphisms of S that let K fixed coincides with the Galois group of the polynomial Q as defined in th. 2,*

$$G = \mathrm{Gal}(S|K)\,. \tag{3.15}$$

Note that in modern treatments of Galois theory, one usually starts from the group $\mathrm{Gal}(S|K)$. The non-trivial part of th. 3 is then to show that the field of $\mathrm{Gal}(S|K)$-invariant rational functions of the roots is K and not a larger field. This doesn't work for an arbitrary field extension, but it works in characteristic zero for the so-called normal extensions. The basic example of a normal extension is precisely the field extension corresponding to the splitting field of a polynomial.

Let us repeat once more the fundamental property of the Galois group, in physical terms. If $\sigma\,\cdot$ denotes the action of an element of the gauge group, here the symmetric group S_N, the observables are usually constrained to satisfy

$$\sigma\cdot\mathscr{O} = \mathscr{O} \quad \text{for any } \sigma\in\mathrm{S}_N\,. \tag{3.16}$$

However, the "kinematical" constraint (3.16) is not really justified. The physical requirement is rather that the expectation values should be gauge invariant,

$$\bigl\langle\sigma\cdot\mathscr{O}\bigr\rangle = \langle\mathscr{O}\rangle \quad \text{for any } \sigma\in\mathrm{S}_N\,. \tag{3.17}$$

Of course, (3.16) implies (3.17), but the converse is not necessarily true. Due to dynamical constraints, it can happen that kinematical constraints less stringent than (3.16) automatically imply the full gauge invariance (3.17) of the expectation values. From our previous discussion, we know that in a given phase $|\varphi)$, the kinematical constraints that ensure the validity of (3.17) take the form

$$\sigma\cdot\mathscr{O} = \mathscr{O} \quad \text{for any } \sigma\in G_{|\varphi)}\,, \tag{3.18}$$

where $G_{|\varphi)}$ is the Galois group of the phase $|\varphi)$. Indeed, the condition (3.18) ensures that $\mathscr{O}\in\mathsf{K}_{|\varphi)}$, i.e. $\langle\mathscr{O}\rangle = \langle\mathcal{O}\rangle$ in the phase $|\varphi)$, where $\mathcal{O}$ is a standard gauge invariant (i.e. completely symmetric) operator.

3.2.3 Relation with the solution of algebraic equations by radicals

In order to assuage a natural curiosity the reader may have, let us very briefly discuss the link with the theory of algebraic equations that are solvable by radicals, which is the original and most famous application of Galois theory.

An algebraic equation is said to be solvable by radicals when its roots can be expressed in terms of the coefficients by a formula that involves only ordinary additions, multiplications and extraction of p^{th} roots, for any p. It is possible to show that if one of the root of an irreducible polynomial has this property, all the other roots will also have it.

JHEP03(2009)128

If an algebraic equation is solvable by radicals, then its Galois group G cannot be an arbitrary group. If $G^{(1)}$ is the commutator subgroup of G (the subgroup generated by all the commutators of pairs of elements of G), $G^{(2)}$ the commutator subgroup of $G^{(1)}$ and so on, then there must exist a $k \geq 1$ such that $G^{(k)}$ is trivial. One then says that the group G is solvable.

Thus, if the Galois group of a particular equation is not solvable, we can immediately deduce that the equation cannot be solved by radicals. For example, the generic equation of degree N has Galois group $G = \mathrm{S}_N$ which is not solvable for $N \geq 5$ ($\mathrm{S}_N^{(k)} = \mathrm{A}_N$ the group of even permutations for all $k \geq 1$, because A_N is simple for $N \geq 5$). Thus a general formula involving only radicals for the roots of an arbitrary polynomial of degree greater than five does not exist.

Galois' idea is very similar to Landau's idea for classifying the phases. Laudau argues that two vacua in the same phase must have the same symmetry group, whereas Galois argues that all equations solvable by radicals must have solvable Galois groups. In the case of gauge theories, we are going to derive shortly that two phases must be distinct if they have distinct Galois symmetries.

Galois theory of algebraic equations is even more powerful, because it gives a complete solution to the problem (whereas we do not claim that the Galois symmetries of the phases yield a complete classification): if the Galois group of an algebraic equation is solvable, then the equation is solvable by radicals. The existence of equations of degree greater than five solvable by radicals of course does not contradict the result for the generic equation, because the formulas for the roots will be equation-dependent.

3.2.4 Galois groups and monodromy groups

We are now going to use the fact that, in the context of gauge theories, the base field $\mathsf{K}_{|\varphi)}$ is the field of rational functions of the irreducible variety $\mathscr{M}_{|\varphi)}$, see (2.14). This yields a very interesting characterization of the Galois group, that we shall use later in explicit computations.

The general problem is as follows. We consider a degree N polynomial $Q \in K[X]$, where $K = \mathbb{C}(V)$ is the field of rational functions on some irreducible algebraic variety V. Let $\mathcal{C}$ be a closed contour on V. Since the coefficients of Q are single-valued on V, Q is mapped onto itself if we perform an analytic continuation along $\mathcal{C}$. This shows that any given root of Q must be mapped onto another root under the analytic continuation. Thus, to any closed contour $\mathcal{C}$ in V, we can associate a permutation $\sigma_{\mathcal{C}}$ of the roots of Q obtained by performing the analytic continuation along $\mathcal{C}$. The subgroup of S_N generated by the $\sigma_{\mathcal{C}}$ for all closed contours $\mathcal{C} \subset V$ is called the *monodromy group* of the polynomial $Q \in \mathbb{C}(V)[X]$.

Theorem 4 *The monodromy group of $Q \in \mathbb{C}(V)[X]$ coincides with the Galois group of Q.*

Let G_Q denotes the Galois group as usual, and $\tilde{G}_Q$ denotes the monodromy group. Let the x_is be the roots of Q and $S_Q = \mathbb{C}(V)(x_1, \ldots, x_N)$ denotes the splitting field. To any $\sigma_{\mathcal{C}} \in \tilde{G}_Q$ we can associate an automorphism of S_Q that let $\mathbb{C}(V)$ fixed by defining $\sigma_{\mathcal{C}} \cdot f(x_1, \ldots, x_N) = f(x_{\sigma_{\mathcal{C}}(1)}, \ldots, x_{\sigma_{\mathcal{C}}(N)})$ if $f \in S_Q$. This is well-defined because if $f = a/b$,

a and $b \neq 0$ being polynomials, then $\sigma_{\mathcal{C}} \cdot f = \sigma_{\mathcal{C}} \cdot a / \sigma_{\mathcal{C}} \cdot b$ and clearly $b \neq 0 \Rightarrow \sigma_{\mathcal{C}} \cdot b \neq 0$. This shows that $\tilde{G}_Q \subset G_Q$. Conversely, consider $f \in S_Q$ and assume that $\sigma_{\mathcal{C}} \cdot f = f$ for all $\sigma_{\mathcal{C}} \in \tilde{G}_Q$. This implies that f is a well-defined meromorphic function on V. Moreover, f is automatically algebraic over $\mathbb{C}(V)$, i.e. f satisfies an irreducible polynomial equation with coefficients in $\mathbb{C}(V)$. Indeed, this is true for any element of S_Q, because S_Q is a finite extension of $\mathbb{C}(V)$, of degree $|G_Q| \leq N!$ (this means that the degree of the equation satisfied by f is less than $N!$). Now, since f is single-valued on V, the irreducible equation that it satisfies must necessarily be of degree one, showing that $f \in \mathbb{C}(V)$. From th. 2 we thus get $G_Q \subset \tilde{G}_Q$ and finally $G_Q = \tilde{G}_Q$.

4 Properties of the Galois group of a phase

In this section, we discuss two important properties of the Galois group of a phase. The first property is that that the Galois group can be computed from the small q expansion of the correlators in any vacuum. The result is independent of the choice of vacuum in the phase $|\varphi)$. This makes explicit the fact that the Galois group is a phase invariant. The second property of the Galois group that we discuss is its intrinsic nature. We make precise the fact that, unlike the field $\mathsf{K}_{|\varphi)}$, $G_{|\varphi)}$ does not depend on the particular realization of the phase in a given model, but only on the phase itself.

4.1 The Galois group as a phase invariant

We have defined the Galois group of a phase in a global, vacuum-independent way in section 3.2. We are now going to exhibit a construction that makes clear that the Galois group can actually be computed from the knowledge of the solution in an arbitrary small neighbourhood of the classical limit $q = 0$ in any vacuum belonging to the phase.

Let us thus pick a vacuum $|i\rangle$ in a phase $|\varphi)$. As explained in section 2, this amounts to choosing a particular value $\langle i|\mathcal{O}|i\rangle$ for the multi-valued analytic functions $\langle\mathcal{O}\rangle$. In a given phase $|\varphi)$, we can focus on a primitive operator $\mathcal{O}_{|\varphi)}$, since all the other operators are polynomials in $\mathcal{O}_{|\varphi)}$. The operator $\mathcal{O}_{|\varphi)}$ satisfies an irreducible polynomial equation $P_{\mathcal{O}_{|\varphi)}} = 0$ with coefficients in $\mathsf{k} = \mathbb{C}(\boldsymbol{g}, q)$, and each root of this equation corresponds to a particular vacuum in the phase,

$$P_{\mathcal{O}_{|\varphi)}}(z) = \prod_{|j\rangle \in |\varphi)} \bigl(z - \langle j|\mathcal{O}_{|\varphi)}|j\rangle\bigr)\,. \tag{4.1}$$

We can consider the field generated by any of the roots $\langle i|\mathcal{O}_{|\varphi)}|i\rangle$ over k,

$$\mathsf{K}_{|i\rangle} = \mathsf{k}\bigl(\langle i|\mathcal{O}_{|\varphi)}|i\rangle\bigr)\,. \tag{4.2}$$

This is a field because $P_{\mathcal{O}_{|\varphi)}}$ is irreducible. The expectation value of the characteristic polynomial (3.2) in the vacuum $|i\rangle$ has its coefficients in $\mathsf{K}_{|i\rangle}$, $\langle i|C|i\rangle \in \mathsf{K}_{|i\rangle}[X]$. If $S_{\langle i|C|i\rangle}$ is the splitting field of $\langle i|C|i\rangle$, we can define the Galois group in the vacuum $|i\rangle$ to be

$$G_{|i\rangle} = \mathrm{Gal}(S_{\langle i|C|i\rangle}|K_{|i\rangle})\,. \tag{4.3}$$

The expectation value $\langle i|\mathcal{O}_{|\varphi)}|i\rangle$, as any other chiral operator expectation values in the vacuum $|i\rangle$, can be Puiseux-expanded at small q. The Puiseux expansion is a convergent expansion in terms of some fractional power of q. Of course this expansion strongly depends on the choice of vacuum. For example, it can be shown easily that the expansion parameter in a vacuum characterized by a pattern of gauge symmetry breaking $\mathrm{U}(N) \to \mathrm{U}(N_1) \times \cdots \times \mathrm{U}(N_r)$, where the N_is are all non-zero, is $q^{N_1\wedge\cdots\wedge N_r/(N_1\cdots N_r)}$ where $N_1 \wedge \cdots \wedge N_r$ is the greatest common divisor of the N_is. The Puiseux expansions give the local data associated with a vacuum. Clearly, $\langle i|\mathcal{O}_{|\varphi)}|i\rangle$ and thus $\mathsf{K}_{|i\rangle}$ and $G_{|i\rangle}$ are determined in terms of this local data only.

We can now state the basic result.

Theorem 5 *The Galois groups $G_{|i\rangle}$ are phase invariants, i.e. if $|i\rangle$ and $|j\rangle$ belong to the same phase $|\varphi)$, then $G_{|i\rangle} = G_{|j\rangle} = G_{|\varphi)}$.*

This theorem relies on two standard results in Galois theory,

Lemma 1

(i) Let $P \in K[X]$ be an irreducible polynomial, a and b two roots of P. Then there exists a field isomorphism $f : K(a) \to K(b)$, $f(a) = b$, that let K fixed. Moreover, $K(a)$ and $K(b)$ are both isomorphic to $K[X]/(P)$.

(ii) Let $Q \in K(a)[X]$ and $f(Q) \in K(b)[X]$ its image under f. Let S_Q be the splitting field of Q over $K(a)$ and $S_{f(Q)}$ the splitting field of $f(Q)$ over $K(b)$. Then the field isomorphism f can be extended into a field isomorphism $g : S_Q \to S_{f(Q)}$.

The part i) of the lemma states that, from the algebraic point of view, all the roots of an *irreducible* polynomial are indistinguishable. Part ii) of the lemma is a version of the unicity theorem for the splitting field. In our case, we use the lemma to construct various field isomorphisms f, g, F and G as in the following diagram. The vertical arrows represent the canonical inclusions.

$$\begin{array}{ccccc} S_{\langle i|C|i\rangle} & \xrightarrow{g} & S_{\langle j|C|j\rangle} & \xrightarrow{G} & \mathsf{S}_{|\varphi)} \\ \uparrow & & \uparrow & & \uparrow \\ \mathsf{K}_{|i\rangle} & \xrightarrow{f} & \mathsf{K}_{|j\rangle} & \xrightarrow{F} & \mathsf{K}_{|\varphi)} \\ \uparrow & & \uparrow & & \uparrow \\ \mathsf{k} & \xrightarrow{\mathrm{id}} & \mathsf{k} & \xrightarrow{\mathrm{id}} & \mathsf{k} \end{array} \tag{4.4}$$

Since the Galois groups are groups of field automorphisms, the isomorphisms between the groups follow immediately. For example, the isomorphism between $G_{|i\rangle}$ and $G_{|j\rangle}$ is given by $\sigma \mapsto g\sigma g^{-1}$ and the isomorphism between $G_{|j\rangle}$ and $G_{|\varphi)}$ is given by $\sigma \mapsto G\sigma G^{-1}$. This shows explicitly that the Galois group is a phase invariant.

4.2 Intrinsic nature of the Galois group

4.2.1 Generalities

The chiral field $\mathsf{K}_{|\varphi)}$ in a phase $|\varphi)$ does not characterize the phase $|\varphi)$. In particular, the number of vacua in a phase, which is the degree of $\mathsf{K}_{|\varphi)}$ over k [2], can vary depending on the way the phase is realized.

For example, consider the case where the derivative of the tree-level superpotential (1.1) is given by mz. Then the theory has N distinct vacua with unbroken gauge group $|N, k\rangle = |k\rangle$, $0 \le k \le N-1$, all belonging to the same confining phase $|C)$. By sending m to infinity, one obtains the pure $\mathcal{N}=1$ gauge theory, which is thus also in the phase $|C)$.

More generally, consider the case of an arbitrary tree-level superpotential (1.1). The Nd vacua of rank one can be labeled as $|i,k\rangle = |N_1, k_1; \ldots ; N_d, k_d\rangle$ with $N_j = N\delta_{ij}$ and $k_i = k$. It is not difficult to check that all these vacua belong to the same phase $|\tilde{C})$. Clearly, the number of vacua in $|C)$ and $|\tilde{C})$ are different (N and Nd respectively), and the fields $\mathsf{K}_{|C)}$ and $\mathsf{K}_{|\tilde{C})}$ are different. However, we would like to think about $|C)$ and $|\tilde{C})$ as describing the same physical phase, since the vacua in the phase $|C)$ can be obtained by taking an appropriate limit from the vacua of the phase $|\tilde{C})$. For example, the vacuum $|i,k\rangle \in |\tilde{C})$ goes to $|k\rangle \in |C)$ if the parameters in the tree level superpotential are set such that $W(z) = \frac{m}{2}(x - w_i)^2$.

The aim of the present subsection is to show that, unlike the chiral field, the Galois symmetry is an intrinsic property of the phase. In particular, in the example described above, one has $G_{|C)} = G_{|\tilde{C})}$. Mathematically, we have to study how the Galois group depends on the base field. We could use a purely algebraic route based on the so-called theorem on natural irrationalities (see for example the first reference in [6]) but we prefer to present a more analytic approach based on theorem 4.

4.2.2 Intrinsic nature of the Galois group

As we have mentioned in the Introduction section, the rank of the vacua is a phase invariant and the chiral variety (2.9) decomposes accordingly,

$$\mathscr{M} = \bigcup_{r=1}^{N} \mathscr{M}_r \, . \tag{4.5}$$

The varieties $\mathscr{M}_r$ are described by the following factorization conditions involving the characteristic polynomial (3.2) and the derivative of the tree-level superpotential (1.1) (see [2] for details and an extensive list of references)

$$C(z)^2 - 4q = M_{N-r}(z)^2 Y_{2r}(z) \, , \tag{4.6}$$

$$W'(z)^2 - D_{d-1}(z) = N_{d-r}(z)^2 Y_{2r}(z) \, . \tag{4.7}$$

In the above equations, M_{N-r}, Y_{2r} and N_{d-r} are polynomials of degrees $N-r$, $2r$ and $d-r$ respectively, whereas D_{d-1} is a polynomial of degree at most $d-1$. Of course, vacua of rank r exist only if $d \ge r$.

The equation (4.6) is the standard factorization condition on the Seiberg-Witten curve. It simply states that $C^2 - 4q$ has $N-r$ double roots. This condition is equivalent to a set of algebraic equations satisfied by the coefficients of C over $\mathbb{C}[q]$. These equations can be obtained for example by eliminating the coefficients of M_{N-r} and Y_{2r} from the constraints obtained by matching the powers of z in (4.6). Explicit examples of the resulting equations are given in section 5. We denote by $\mathscr{N}_r$ the corresponding $r+1$-dimensional algebraic variety. Standard local coordinates on $\mathscr{N}_r$ are given by $q, u_1, \ldots, u_r$. From the analysis in [2], it is straightforward to check that for given $q, u_1, \ldots, u_r$ there are

$$\hat{v}_r(N) = \binom{N+r-1}{2r-1} = \sum_{\sum_{k=1}^r N_k = N} N_1 \cdots N_r \tag{4.8}$$

points on $\mathscr{N}_r$. This is also the minimal number of vacua in any realization of the phases of rank r.

The defining equations of $\mathscr{M}_r$ are obtained by combining equations (4.6) and (4.7) and eliminating all variables except the u_ks (or equivalently the coefficients of C), q and the g_ks. It is a $d+2$ dimensional variety with standard local coordinates $(q, g_0, \ldots, g_d) = (q, \boldsymbol{g})$. It decomposes in terms of irreducible components according to

$$\mathscr{M}_r = \bigcup_{|r,\varphi)} \mathscr{M}_{|r,\varphi)}\,, \tag{4.9}$$

where we denote by $|r,\varphi)$ the phases at rank r.

It is useful to introduce the r-dimensional subvariety $\hat{\mathscr{M}}_r$ of $\mathscr{M}_r$ corresponding to $g_k = 0$ for $r+1 \le k \le d$ and $g_r = 1$. Using the results of [2], it is straightforward to show that the decomposition in irreducible components of $\mathscr{M}_r$ and $\hat{\mathscr{M}}_r$ are in one-to-one correspondence. The idea is that the non-trivial interpolations between the vacua in $\mathscr{M}_{|r,\varphi)}$ all follow from the non-trivial interpolations between the vacua that are also in $\hat{\mathscr{M}}_{|r,\varphi)}$ together with additional interpolations that can all be described in the semi-classical regime. One thus has

$$\hat{\mathscr{M}}_r = \bigcup_{|r,\varphi)} \hat{\mathscr{M}}_{|r,\varphi)}\,, \tag{4.10}$$

where $\hat{\mathscr{M}}_{|r,\varphi)}$ is the subvariety of $\mathscr{M}_{|r,\varphi)}$ obtained by setting $g_{r+1} = \ldots = g_d = 0$.

Let us now consider the projection map $\pi : \mathscr{M}_r \to \mathscr{N}_r$, $\pi(q, \boldsymbol{g}, u_1, \ldots, u_N) = (q, u_1, \ldots, u_N)$. π is well-defined since the equations on $q, u_1, \ldots, u_N$ that define $\mathscr{N}_r$ are automatically satisfied on $\mathscr{M}_r$. Moreover, we have the following fundamental property of π.

Lemma 2 *The restriction of the projection map $\hat{\pi} = \pi_{|\hat{\mathscr{M}}_r} : \hat{\mathscr{M}}_r \to \mathscr{N}_r$ is one-to-one.*

To prove this lemma, let us fix $q, u_1, \ldots, u_N$ in (4.6). This fixes the polynomials M_{N-r} and Y_{2r} in a unique way. If we assume that $g_{r+1} = \ldots = g_d = 0$, then (4.7) implies that $N_{d-r} = g_r^2 = 1$ and that W' is uniquely determined to be the polynomial part in the large z expansion of $\sqrt{Y_{2r}}$. The polynomial $D_{d-1} = W'^2 - Y_{2r}$ has then a degree bounded by $r-1 \le d-1$ as it should.

The algebraic varieties $\hat{\mathscr{M}}_r$ and $\mathscr{N}_r$ are thus isomorphic and in particular $\mathscr{N}_r$ decomposes into irreducible components as

$$\mathscr{N}_r = \bigcup_{|r,\varphi)} \mathscr{N}_{|r,\varphi)}\,, \tag{4.11}$$

where $\mathscr{N}_{|r,\varphi)} = \hat{\pi}(\mathscr{M}_{|r,\varphi)})$. One then has the

Theorem 6 *(Intrinsic nature of the Galois group) The Galois group of the phase $|r,\varphi)$, which is the Galois group of the characteristic polynomial (3.2) viewed as a polynomial with coefficients in the field $\mathbb{C}(\mathscr{M}_{|r,\varphi)})$, is the same as the Galois group of the characteristic polynomial (3.2) viewed as a polynomial with coefficients in the field $\mathbb{C}(\mathscr{N}_{|r,\varphi)})$.*

This theorem not only demonstrates the intrinsic nature of the Galois group of a phase but also shows that the computation of the group can be done by considering the varieties $\mathscr{N}_{|r,\varphi)}$ only. This will be used in the next section.

Let us prove the theorem by using the characterization of the Galois group given in th. 4. We consider the characteristic polynomial $C \in \mathbb{C}(\mathscr{M}_{|r,\varphi)})[X]$ with Galois group $G_{|r,\varphi)}$ and $\pi(C) \in \mathbb{C}(\mathscr{N}_{|r,\varphi)})[X]$ with Galois group $\tilde{G}_{|r,\varphi)}$. Let $\mathcal{L}$ be a closed contour in $\mathscr{M}_{|r,\varphi)}$, with associated element $\sigma_{\mathcal{L}} \in G_{|r,\varphi)}$ corresponding to the permutation of the roots of C obtained by performing the analytic continuation of C along $\mathcal{L}$. The analytic continuation of $\pi(C)$ along the closed contour $\pi(\mathcal{L}) \subset \mathscr{N}_{|r,\varphi)}$ will obviously yield the same permutation of the roots. Thus $G_{|r,\varphi)} \subset \tilde{G}_{|r,\varphi)}$. Conversely, let $\tilde{\mathcal{L}}$ be a closed contour in $\mathscr{N}_{|r,\varphi)}$, with associated element $\tilde{\sigma}_{\tilde{\mathcal{L}}}$. The Lem. 2 ensures that there exists a *closed* contour $\mathcal{L}$ in $\mathscr{M}_{|r,\varphi)}$ such that $\pi(\mathcal{L}) = \tilde{\mathcal{L}}$: one can choose $\mathcal{L} = \hat{\pi}^{-1}(\tilde{\mathcal{L}})$. This shows that $\tilde{G}_{|r,\varphi)} \subset G_{|r,\varphi)}$ and we can conclude.

5 A few simple examples of Galois groups

Computing Galois groups is, in general, rather subtle. It may be possible to find the Galois groups for all the phases of the model (1.1), but we shall be more modest here and limit ourselves to explicit calculations in a few very simple cases. Our goal is to make the discussions of the previous sections as concrete as possible. We start in 5.1 with the case of the U(2) and U(3) theories, which is very elementary. In 5.2, we present a few general features of the Galois groups valid in U(N) theories for any N. Finally, in 5.3, we compute the Galois groups for all the phases of the U(4) model.

The phases of the model have been studied extensively in [2] and we shall use the results of this paper as well as of the earlier references [3–5] in the following.

We want to compute the Galois group of the characteristic polynomial (3.2), where the coefficients satisfy a suitable set of constraints correponding to the phase under study. At the expense of shifting the variable $z \to z + \sigma_1/N$ in (3.2), we can always set $\sigma_1 = 0$. Obviously, such a shift of the indeterminate by an element of the base field doesn't change the Galois group. In other words, the Galois groups for the U(N) or SU(N) theories are the same. With $\sigma_1 = 0$, the irreducible varieties $\mathscr{N}_{|r,\varphi)}$ of section 4.2.2 are of dimension r instead of $r + 1$.

5.1 The Galois groups for U(2) and U(3)

In the case of U(2), the characteristic polynomial (3.2) is

$$C(z) = z^2 + \sigma_2 \,. \tag{5.1}$$

At rank $r = 2$, we have the usual Coulomb phase $|2)$ with unbroken gauge group $\mathrm{U}(1)^2$. The coefficient of C in this phase in not constrained. The Galois group is thus the same as for the generic polynomial, $G_{|2)} = \mathrm{S}_2 = \mathbb{Z}_2$. At rank $r = 1$ we have the confining phase $|1)$ with unbroken gauge group. This is characterized by the condition $\sigma_2^2 = 4q$. Since q is arbitrary, we are again in the case of a generic polynomial and thus $G_{|1)} = \mathrm{S}_2 = \mathbb{Z}_2$.

The above results are extremely simple to interpret. For example, in the case of the Coulomb phase, the roots of C are given by $x_1 = i\sqrt{\sigma_2}$ and $x_2 = -i\sqrt{\sigma_2}$. The only polynomials in the roots that can be expressed in terms of a polynomial of σ_2 are the symmetric polynomials in x_1 and x_2. Thus the Galois group is S_2. Another way to understand the result is to note that the irreducible variety $\mathscr{N}_{|2)}$ is just $\mathbb{C}^2$, with coordinates σ_2 and q. The roots x_1 and x_2 are exchanged by performing an analytic continuation along a closed contour that circles around $\sigma_2 = 0$, $\sigma_2 \rightarrow e^{2i\pi}\sigma_2$ and this transposition generates the Galois group S_2.

In the case of U(3),

$$C(z) = z^3 + \sigma_2 z - \sigma_3\,. \tag{5.2}$$

At rank $r = 3$, we have the Coulomb phase $|3)$ with a generic characteristic polynomial and $G_{|3)} = \mathrm{S}_3$. At rank $r = 2$, there is a unique phase $|2)$ with irreducible variety $\mathscr{N}_{|2)}$ given by the equation

$$\left(27\sigma_3^2 + 4\sigma_2^3\right)^2 - 216q\left(27\sigma_3^2 - 4\sigma_2^3\right) + 11664q^2 = 0\,. \tag{5.3}$$

This equation can be viewed as a constraint on q for given σ_2 and σ_3 but σ_2 and σ_3 can be choosen freely. As a consequence, C is generic and $G_{|2)} = \mathrm{S}_3$.

The first interesting case, for which the S_3 symmetry is spontaneously broken, corresponds to the confining phase $|1)$ at rank $r = 1$. The irreducible variety $\mathscr{N}_{|1)}$ is given by the equations that ensure that $C^2 - 4q$ has two double roots. This implies that the discriminant of the polynomials $C - 2q^{1/2}$ and $C + 2q^{1/2}$ both vanish, which yields, after some simple algebraic manipulations,

$$\sigma_3 = 0\,, \quad \sigma_2^3 + 27q = 0\,. \tag{5.4}$$

The polynomial C is thus reducible over $\mathbb{C}(\mathscr{N}_{|1)})$, $C(z) = z(z^2 + \sigma_2)$. Since σ_2 can be arbitrary, the Galois group is $G_{|1)} = \mathbb{Z}_2$, exchanging the two roots of $z^2 + \sigma_2 = 0$ and letting the third root fixed.

5.2 Galois groups for $\mathrm{U}(N)$

We can make a few simple general statements about the Galois groups of some phases for arbitrary N.

5.2.1 The phase at rank N

At rank $r = N$ there is only one phase, the Coulomb phase with unbroken gauge group $\mathrm{U}(1)^N$. The irreducible variety $\mathscr{N}_{|N)}$ is simply $\mathbb{C}^N$ in this case and the characteristic polynomial is a generic polynomial of degree N. The Galois group is thus automatically the full permutation group,

$$G_{|N)} = \mathrm{S}_N\,. \tag{5.5}$$

5.2.2 The phase at rank $N-1$

There is only one phase at rank $N-1$, in which all the vacua have a $\mathrm{U}(1)^{N-2}\times\mathrm{U}(2)$ unbroken gauge group [2]. The irreducible variety $\mathscr{N}_{|N-1)}$ is a hypersurface in $\mathbb{C}^N$ given by the vanishing of the discriminant of C^2-4q (this discriminant is automatically an irreducible polynomial from our previous discussions). This equation can be seen as a contraint on q for given u_ks, and thus the characteristic polynomial is generic, which implies that

$$G_{|N-1)} = \mathrm{S}_N\,. \tag{5.6}$$

5.2.3 The phase at rank one

The solution for the unique phase at rank $r=1$, corresponding to C^2-4q having $N-1$ double roots, is explicitly known [7]. In terms of the Chebyshev polynomials of the first kind T_N, defined by the identity $T_N(\cos\theta)=\cos N\theta$, we have

$$C(z) = 2q^{1/2}T_N\Bigl(\frac{z}{2q^{1/2N}}\Bigr)\,. \tag{5.7}$$

Expanding in powers of z, we find an explicit parametrization of the irreducible variety $\mathscr{N}_{|1)}$, generalizing (5.4),

$$\sigma_{2s+1}=0\,,\quad \sigma_{2s}=(-1)^s\frac{N}{N-s}\binom{N-s}{s}q^{s/N}\,. \tag{5.8}$$

Consistently with (4.8), $\mathscr{N}_{|1)}$ is an N-fold cover of the q-plane. The roots of $C(z)$ can also be explicitly computed,

$$x_i = 2q^{1/2N}\cos\Bigl(\frac{\pi}{N}(i-1/2)\Bigr)\,. \tag{5.9}$$

In particular, one has $x_i=-x_{N+1-i}$ and, using $\sigma_2=-Nq^{1/N}$ which follows from (5.8), $x_i^2=-\frac{4}{N}\sigma_2\cos^2[\frac{\pi}{N}(i-1/2)]$. In the case of even N, this implies that C factorizes over $\mathbb{C}(\mathscr{N}_{|1)})$ as

$$C(z)=\prod_{i=1}^{N/2}\Bigl(z^2+\frac{4}{N}\sigma_2\cos^2\bigl(\frac{\pi}{N}(i-1/2)\bigr)\Bigr)\,. \tag{5.10}$$

In the case of odd N we have similarly

$$C(z)=z\prod_{i=1}^{(N-1)/2}\Bigl(z^2+\frac{4}{N}\sigma_2\cos^2\bigl(\frac{\pi}{N}(i-1/2)\bigr)\Bigr)\,. \tag{5.11}$$

From (5.10) and (5.11), we immediately read off the Galois group,

$$G_{|1)}=\mathbb{Z}_2\,. \tag{5.12}$$

It is generated by the permutation τ acting on the roots as

$$\tau(x_i)=x_{N+1-i}\,. \tag{5.13}$$

The above examples show clearly that there is no direct relation between the pattern of symmetry breaking in the usual classical sense and the pattern of symmetry breaking described by Galois theory. This should not be too surprising: the usual notion makes sense only classically whereas the Galois symmetry make sense in the quantum theory; to a given phase may be associated several classical unbroken gauge groups (examples are provided below) whereas the Galois symmetry is a phase invariant.

5.3 The Galois groups for U(4)

We have to compute the Galois groups of

$$C(z) = z^4 + \sigma_2 z^2 - \sigma_3 z + \sigma_4 \tag{5.14}$$

in the various phases of the model. The phases of rank four, three and one have been studied in 5.2 and thus we can focus on the phases of rank two. There are two such phases [2] that we shall denote by $|2,t)$ with the confinement index $t = 1$ or 2.

5.3.1 The group $G_{|2,2)}$

The phase $|2,2)$ has confinement index $t = 2$ with unbroken gauge group $\mathrm{U}(2) \times \mathrm{U}(2)$. The irreducible variety $\mathscr{N}_{|2,2)}$ is given by the condition that $C(z) + 2q^{1/2}$ has two double roots. Taking into account the fact that the sum of all the roots are zero, this implies that C is of the form

$$C(z) = (z^2 - a)^2 - b \tag{5.15}$$

which corresponds to the following parametrization of $\mathscr{N}_{|2,2)}$,

$$\mathscr{N}_{|2,2)} : \ \sigma_2 = -2a\,, \ \sigma_3 = 0\,, \ \sigma_4 = a^2 - b\,, \ q = b^2/4\,. \tag{5.16}$$

One can invert these relations, $a = -\sigma_2/2$ and $b = \sigma_2^2/4 - \sigma_4$, which shows that the variety $\mathscr{N}_{|2,2)}$ is rational. Theorem 4 then implies that the Galois group $G_{|2,2)}$ coincides with the monodromy group of the polynomial (5.15).

The discriminant of (5.15) is given by

$$\Delta = 256 b^2 (a^2 - b)\,. \tag{5.17}$$

The monodromy group can be computed by considering the analytic continuations of the roots along non-contractible loops on $\mathbb{C}^2 \setminus \Sigma$, where $\mathbb{C}^2 = \{(a,b)\}$ and Σ is the zero locus of (5.17). The roots of (5.15) can be easily written explicitly,

$$x_1 = \sqrt{a + \sqrt{b}}\,, \ x_2 = \sqrt{a - \sqrt{b}}\,, \ x_3 = -\sqrt{a + \sqrt{b}}\,, \ x_4 = -\sqrt{a - \sqrt{b}}\,. \tag{5.18}$$

The monodromy around $b = 0$ yields the product of tranpositions (12)(34), the monodromy around $a = \sqrt{b}$ yields the transposition (24) and the monodromy arond $a = -\sqrt{b}$ yields the transposition (13). These permutations generate the symmetry group D_4 of a square whose vertices are labeled by the roots x_1, x_2, x_3, x_4 clockwise. The group D_4 is of order eight and is called the dihedral group,

$$G_{|2,2)} = \mathrm{D}_4\,. \tag{5.19}$$

Let us note that the monodromies that one needs to consider in this case can all be found by performing analytic continuations in the semi-classical regime, which corresponds to small q or equivalently small b. This possibility corresponds to the fact that all the vacua in the phase $|2,2)$ have the same unbroken gauge group and can all be smoothly connected at weak coupling.

JHEP03(2009)128

Another way to derive (5.19) is to note that the polynomial (5.15) is a generic even polynomial. For a particular ordering of the roots, consistent with the labeling (5.18), we thus have the relations

$$x_1 + x_3 = 0\,, \quad x_2 + x_4 = 0\,. \tag{5.20}$$

The only constraint on the Galois group is that it must preserve these relations. In particular, the cycle (1234) and the product of transpositions (12)(34) are in the group and these permutations generate D_4. The only subgroup of S_4 containing strictly D_4 is S_4 itself. However, the Galois group cannot be S_4 since, for example, the permutation (12) does not preserve the relations (5.20). We conclude.

5.3.2 The group $G_{|2,1)}$

The phase $|2,1)$ contains vacua with either $\mathrm{U}(2)\times\mathrm{U}(2)$ or $\mathrm{U}(1)\times\mathrm{U}(3)$ unbroken gauge groups [2, 4, 5]. The associated variety $\mathscr{N}_{|2,1)}$, which is given by the vanishing of the discriminants of $C + 2q^{1/2}$ and $C - 2q^{1/2}$, turns out to be rational. As in the previous subsection, this will drastically simplifies the calculation of the Galois group.

Lemma 3 *The variety $\mathscr{N}_{|2,1)}$ is rational, the birational mapping to $\mathbb{C}^2$ being given by*

$$\sigma_2 = 2(b - a^2) \tag{5.21}$$

$$\sigma_3 = 4ab \tag{5.22}$$

$$\sigma_4 = \frac{1}{2}\bigl(a^4 - 6a^2b + 2b^2\bigr) \tag{5.23}$$

$$q = \frac{1}{16}a^2\bigl(a^2 - 4b\bigr)^3\,. \tag{5.24}$$

To prove this result, we write

$$C(z) - 2q^{1/2} = \bigl(z + (z_1 + z_2)/2\bigr)^2\bigl(z - z_1\bigr)\bigl(z - z_2\bigr)\,, \tag{5.25}$$

$$C(z) - 2q^{1/2} = \bigl(z + (z_3 + z_4)/2\bigr)^2\bigl(z - z_3\bigr)\bigl(z - z_4\bigr)\,. \tag{5.26}$$

This yields

$$\sigma_2 = \frac{3}{4}\bigl(z_1^2 + z_2^2\bigr) - \frac{1}{2}z_1z_2 = \frac{3}{4}\bigl(z_3^2 + z_4^2\bigr) - \frac{1}{2}z_3z_4\,, \tag{5.27}$$

$$\sigma_3 = \frac{1}{4}(z_1 + z_2)(z_1 - z_2)^2 = \frac{1}{4}(z_3 + z_4)(z_3 - z_4)^2\,, \tag{5.28}$$

$$\sigma_4 = \frac{1}{4}z_1z_2(z_1 + z_2)^2 + 2q^{1/2} = \frac{1}{4}z_3z_4(z_3 + z_4)^2 - 2q^{1/2}\,. \tag{5.29}$$

The idea is then to eliminate the variables $z_1 - z_2$ and $z_3 - z_4$ from the above equations, keeping only $z_1 + z_2$ and $z_3 + z_4$. After a straightforward but slightly tedious calculation one obtains

$$(z_1 - z_2)^2 = 2(z_3 + z_4)(z_1 + z_2 + z_3 + z_4)\,,\ (z_3 - z_4)^2 = 2(z_1 + z_2)(z_1 + z_2 + z_3 + z_4)\,. \tag{5.30}$$

Plugging this result into (5.27), (5.28) and (5.29) and defining

$$a = \frac{1}{2}\bigl(z_1 + z_2 + z_3 + z_4\bigr)\,,\ b = \frac{1}{4}\bigl(z_1 + z_2\bigr)\bigl(z_3 + z_4\bigr)\,, \tag{5.31}$$

JHEP03(2009)128

we get the parametrization given in the lemma 3. To prove that the mapping is birational, we also have to express a and b in terms of the σ_is and q. Again this is a bit tedious but straightforward to do and we find

$$a = \frac{4}{\sigma_3}\,\frac{\sigma_2^5 - 12\sigma_4\sigma_2^3 + 6\sigma_3^2\sigma_2^2 + 32\sigma_4^2\sigma_2 - 18\sigma_3^2\sigma_4}{8\sigma_2^3 + 27\sigma_3^2}\,, \tag{5.32}$$

$$b = \frac{1}{2}\sigma_2 + a^2\,. \tag{5.33}$$

Combining lemma 3 with theorem 4 in section 3.2.4, we deduce that the Galois group $G_{|2,1)}$ in the phase $|2,1)$ can be derived by computing the monodromy group of

$$C(z) = z^4 + 2\bigl(b - a^2\bigr)z^2 - 4abz + \frac{1}{2}\bigl(a^4 - 6a^2b + 2b^2\bigr)\,. \tag{5.34}$$

The discriminant of this polynomial is given by

$$\Delta = 32a^2\bigl(a^2 - 4b\bigr)^3\bigl(a^4 + 10a^2b - 2b^2\bigr)\,. \tag{5.35}$$

If Σ is the zero locus of Δ, we have to consider analytic continuations of the roots of C along non-contractible loops on $\mathbb{C}^2\backslash\Sigma$. We can simplify the analysis by noting that (5.34) is homogeneous, with z, a and b of degree one, one and two respectively. Since $b = 0$ is not in Σ, it is then convenient to rescale the variables in such a way that $b = 1$. We thus focus on

$$C(z) = z^4 + 2\bigl(1 - a^2\bigr)z^2 - 4az + \frac{1}{2}\bigl(a^4 - 6a^2 + 2\bigr)\,, \tag{5.36}$$

with

$$\Delta = 32a^2\bigl(a^2 - 4\bigr)^3\bigl(a^4 + 10a^2 - 2\bigr)\,. \tag{5.37}$$

The zero locus Σ of Δ corresponds to the points $a = a_i$ and $a = -a_i$ with

$$a_1 = 0\,,\ \ a_2 = 2\,,\ \ a_3 = \sqrt{-5 + 3\sqrt{3}}\,,\ \ a_4 = i\sqrt{5 + 3\sqrt{3}}\,. \tag{5.38}$$

Let us pick a base point $a = a_*$ on the a-plane deprived of Σ. For example, we can choose $a_* = i$. The roots of C at the base point are then given by

$$x_1 \simeq -0.9 + 1.5i\,,\ \ x_2 \simeq 0.9 + 1.5i\,,\ \ x_3 \simeq -0.7i\,,\ \ x_4 \simeq -2.2i\,. \tag{5.39}$$

A set of generators of the monodromy group is obtained by studying the analytic continuations of the roots (5.39) along contours $\mathcal{C}_i$ and $\tilde{\mathcal{C}}_i$ that start from a_* and circle counterclockwise around the points a_i and $-a_i$ respectively (and not around any other point in Σ). Since C is of degree four, this can be done from the exact formulas for the roots. A more convenient method, that can be generalized to cases with $N > 4$, is to compute numerically the roots along the various contours and read off the corresponding permutations on the data. This can be easily implemented in Mathematica and we have used this method in the following.

Taking into account (5.24), the monodromies around $a = 0$ and $a = \pm 2$ are at weak coupling. When $a = a_1 = 0$, $C(z) = (1 + z^2)^2$ has two double roots. This case thus

JHEP03(2009)128

corresponds to the $\mathrm{U}(2) \times \mathrm{U}(2)$ vacua. The monodromy around $\mathcal{C}_1$ yields the permutation $(12)(34)$. This is reminiscent of (5.13), with a simultaneous exchange of the roots in the two $\mathrm{U}(2)$ factors. When $a = a_2 = 2$, $C(z) = (z-3)(z+1)^3$. This corresponds to the weak coupling region with unbroken gauge group $\mathrm{U}(1) \times \mathrm{U}(3)$. The monodromy around $\mathcal{C}_2$ must thus yield a transposition of the form (5.13). Which transposition it corresponds to precisely, taking into account that the monodromy around C_1 is the permutation $(12)(34)$, involves some strong coupling information. We find numerically the transposition (14). Similarly we have $\mathrm{U}(1) \times \mathrm{U}(3)$ vacua at $a = -a_2 = -2$, since $C(z) = (z+3)(z-1)^3$. The associated monodromy must be a transposition. Which one precisely involves again some strong coupling effects and is found to be (24). The permutations $(12)(34)$, (14) and (24) generate the full symmetric group S_4 and thus

$$G_{|2,1)} = \mathrm{S}_4\,, \tag{5.40}$$

without the need to consider additional monodromies.

Let us note that the same methods can be used to compute the Galois groups in $\mathrm{U}(N)$ theories for $N > 4$. For example, in the $\mathrm{U}(5)$ theory, there are two phases $|1)$ and $|2)$ at rank three and confinement index one. The associated varieties $\mathscr{N}_{|1)}$ and $\mathscr{N}_{|2)}$ turn out to be rational. We have shown that the Galois groups of both phases are S_5. Unfortunately, in this case, the Galois symmetry does not distinguish the phases.

6 Conclusion

In this paper, we have explained how new types of symmetries are hidden in the algebra of local observables in gauge theories. The general idea is to reconstruct the gauge-variant data from the gauge invariant observables by studying the gauge invariant set of equations that the gauge-variant quantities must satisfy. The solution of this problem is governed by a Galois symmetry group, which may be a strict subgroup of the gauge group. Remarkably, this provides a perfectly well-defined notion of gauge symmetry breaking at the quantum level.

In particular, the Galois symmetry is a phase invariant and can thus be used to classify the phases, unlike the usual pattern of gauge symmetry breaking which can be different in two vacua belonging to the same phase. We have been able to compute explicitly a few Galois groups using elementary methods. The classification obtained in terms of the Galois groups studied in this paper does not provide a complete classification of the phases, as explained at the end of the previous section. Our analysis was restricted to the S_N subgroup of the full gauge group and it is conceivable that a finer classification could be achieved by using the full gauge symmetry along the lines sketched in section 3.1.

It is natural to ask whether the Galois symmetries could play a rôle in other related problems, like for example to better understand 't Hooft's monopoles in the abelian projection or the Gribov ambiguity.[3] It is also interesting to note that in quantum gravity, the lack of local observables is very similar to the lack of local order parameters in gauge theory. This suggests that Galois theory might be useful in this context as well.

[3] I would like to thank M. Dougals for pointing out this possibility.

JHEP03(2009)128

Acknowledgments

This work is supported in part by the belgian Fonds de la Recherche Fondamentale Collective (grant 2.4655.07), the belgian Institut Interuniversitaire des Sciences Nucléaires (grant 4.4505.86) and the Interuniversity Attraction Poles Programme (Belgian Science Policy). The author is on leave of absence from Centre National de la Recherche Scientifique, Laboratoire de Physique Théorique de l'École Normale Supérieure, Paris, France.

References

[1] R. Donagi and E. Witten, *Supersymmetric Yang-Mills theory and integrable systems*, *Nucl. Phys.* **B 460** (1996) 299 [hep-th/9510101] [SPIRES].

[2] F. Ferrari, *On the geometry of super Yang-Mills theories: phases and irreducible polynomials*, *JHEP* **01** (2009) 026 [arXiv:0810.0816] [SPIRES].

[3] F. Ferrari, *Quantum parameter space and double scaling limits in $N = 1$ super Yang-Mills theory*, *Phys. Rev.* **D 67** (2003) 085013 [hep-th/0211069] [SPIRES].

[4] F. Ferrari, *Quantum parameter space in super Yang-Mills. II*, *Phys. Lett.* **B 557** (2003) 290 [hep-th/0301157] [SPIRES].

[5] F. Cachazo, N. Seiberg and E. Witten, *Phases of $N = 1$ supersymmetric gauge theories and matrices*, *JHEP* **02** (2003) 042 [hep-th/0301006] [SPIRES].

[6] E. Artin, *Galois theory*, Dover Publications Inc., U.S.A. (1998);
I. Stewart, *Galois theory*, Chapman and Hall Mathematical Series, U.S.A. (1989);
M. Reid, *Galois theory*, http://www.warwick.ac.uk/~masda/MA3D5/;
S. Lang, *Algebra*, Springer, U.S.A. (2005).

[7] M.R. Douglas and S.H. Shenker, *Dynamics of* $\mathrm{SU}(N)$ *supersymmetric gauge theory*, *Nucl. Phys.* **B 447** (1995) 271 [hep-th/9503163] [SPIRES].