Permutations of massive vacua

Antoine Bourget[a] **and Jan Troost**[b]

[a]*Department of Physics, Universidad de Oviedo,*
Avenida Calvo Sotelo 18, 33007 Oviedo, Spain

[b]*Laboratoire de Physique Théorique de l'É cole Normale Supérieure, CNRS,*
PSL Research University, Sorbonne Universités, 75005 Paris, France

E-mail: bourgetantoine@uniovi.es, troost@lpt.ens.fr

ABSTRACT: We discuss the permutation group G of massive vacua of four-dimensional gauge theories with $\mathcal{N} = 1$ supersymmetry that arises upon tracing loops in the space of couplings. We concentrate on superconformal $\mathcal{N} = 4$ and $\mathcal{N} = 2$ theories with $\mathcal{N} = 1$ supersymmetry preserving mass deformations. The permutation group G of massive vacua is the Galois group of characteristic polynomials for the vacuum expectation values of chiral observables. We provide various techniques to effectively compute characteristic polynomials in given theories, and we deduce the existence of varying symmetry breaking patterns of the duality group depending on the gauge algebra and matter content of the theory. Our examples give rise to interesting field extensions of spaces of modular forms.

Contents

1 Instigation

Four-dimensional gauge theories play a paramount role in our description of nature. While we understand the phase structure of gauge theories reasonably well, we have an even better control over the subset of theories with supersymmetry. The minimal amount of supersymmetry in four dimensional Poincaré invariant theories is four supercharges, or $\mathcal{N} = 1$. We comprehend a lot of the vacuum structure of $\mathcal{N} = 1$ theories, including the number of vacua for the pure $\mathcal{N} = 1$ super Yang-Mills theory, methods to solve for the superpotential in any given vacuum, as well as the systematics of the chiral ring of $\mathcal{N} = 1$ theories (see e.g. [1, 2] and [3] respectively). While the theory of the chiral sector of $\mathcal{N} = 1$ theories is well-grounded, concrete answers about the vacuum structure or the chiral ring of particular theories can still be hard to obtain. In this paper, we develop further tools to characterize the vacua.

We consider quantum field theories that can be defined using discrete data (for instance, the gauge group and the field content) as well as parameters that take values in a continuous space (e.g. the coupling constants). We call the space of parameters $\bar{C}$, which is a connected space by definition. In a regime where a Lagrangian description is available, the space $\bar{C}$ can be identified with the parameters needed to define this Lagrangian, such as gauge coupling constants and masses. If the theory permits duality transformations, those appear as discrete quotients and $\bar{C}$ is an orbifold.

We focus on $\mathcal{N} = 1$ supersymmetric gauge theories in four dimensions. In such theories, an efficient probe of the space $\bar{C}$ is the vacuum structure, which is a fiber bundle with base $\bar{C}$. More precisely, we expect to find at each point of $\bar{C}$ a finite number of massive isolated vacua, along with massless vacua that form continuous branches. Let us call V_{massive} the space of massive vacua: it is a fiber bundle where the fiber is finite or in other words, V_{massive} is an n-fold cover of $\bar{C}$, where n is the number of massive vacua. However, there might be points in parameter space where some or all vacua become indistinguishable — for instance at the zero coupling point in pure $\mathcal{N} = 1$ Yang-Mills theory. We assume that these points are isolated. In order to characterize completely both the parameter space and the bundle of massive vacua, we will restrict our attention to the subspace $C \subset \bar{C}$ where the massive vacua are distinguishable, i.e. the space C is the parameter space $\bar{C}$ with points where vacua merge excluded.

As a consequence, when moving along a non-contractible cycle of C the n vacua are permuted in a well defined way. This means that the cover $V_{\text{massive}} \to C$ can be described through a map

$$\sigma : \pi_1(C) \to \mathfrak{S}_n \,, \tag{1.1}$$

where $\mathfrak{S}_n$ is the permutation group of n elements acting on the massive vacua of the theory. The full parameter space $\bar{C}$ is in general an orbifold characterized by the fact that its fundamental group $\pi_1(\bar{C})$ is a maximal quotient of $\pi_1(C)$ such that σ passes to the quotient. In other words, the fundamental group of $\bar{C}$ is the smallest subgroup of $\pi_1(C)$

whose image under σ is all of $\operatorname{Im} \sigma$, and the following diagram commutes

$$
\begin{array}{ccc}
\pi_1(C) & & \\
\downarrow & \searrow^{\sigma} & \\
\pi_1(\bar{C}) & \xrightarrow{\bar{\sigma}} & \mathfrak{S}_n
\end{array}
\tag{1.2}
$$

One goal of this paper is to develop tools that allow to understand the map σ, which in turn gives precious information about the two objects that it relates:

- On the $\mathfrak{S}_n$ permutation group side, we learn how the vacua are transformed when the parameters are varied. For reasons that will become clear in the following, we call the image of σ the *Galois group*

$$
G = \operatorname{Im} \sigma = \operatorname{Im} \bar{\sigma} \, .
\tag{1.3}
$$

  Amongst other information, this provides knowledge on which semi-classically distinct vacua can be continuously connected in the quantum theory.

- On the π_1 side, we learn about the structure of the space $\bar{C}$. The homotopy subgroup Γ_{Galois} is identified with the kernel of σ,

$$
\Gamma_{\text{Galois}} = \operatorname{Ker} \sigma \, .
\tag{1.4}
$$

Our main tool of analysis is the characteristic polynomial associated to an operator $\mathcal{O}$, defined by

$$
P_{\mathcal{O}}(X) = \prod_{i=1}^{n} (X - \langle \mathcal{O} \rangle_i) \, ,
\tag{1.5}
$$

where $\langle \mathcal{O} \rangle_i$ is the expectation value in the vacuum i, X is a formal variable and we multiply over the set of n vacua. Although $\langle \mathcal{O} \rangle_i$ is multi-valued on C, the characteristic polynomial is well defined and single-valued on C, and if the operator $\mathcal{O}$ is *generic*, the Galois group associated to the polynomial[1] characterizes completely the way the vacua are permuted [6, 7]:

$$
\operatorname{Gal}(P_{\mathcal{O}}) = G = \operatorname{Im} \sigma \, .
\tag{1.6}
$$

We say that $\mathcal{O}$ is *generic* if its Galois group is maximal, in the sense that for any operator $\mathcal{O}'$, we have that the Galois group of $P(\mathcal{O})$ satisfies $\operatorname{Gal}(P_{\mathcal{O}'}) \subseteq \operatorname{Gal}(P_{\mathcal{O}})$. Determining the Galois group of a polynomial or of a field extension is generically a difficult task; we will show on various examples how to overcome the difficulties by combining algebraic facts, group theory databases like [8, 9] and the software Sage [10].

The analysis of the Galois group of the characteristic polynomial will serve to determine the breaking pattern of the symmetries of the theory under massive deformation. Specifically, in the mass deformed $\mathcal{N} = 2$ superconformal theories on which we concentrate, we will characterize the breaking of modular invariance in the vacua in this manner.

---

[1]See e.g. [4, 5] for pedagogical introductions.

Moreover, the study of the characteristic polynomial of the superpotential will also lead to further insight into the vacuum expectation values of the superpotential. The latter are useful for instance in determining domain wall tensions, or the coupling dependence of the glueball expectation value.

Plan of the paper. Our ideas are illustrated in examples of growing complexity. The whole of sections 2, 3 and 4 are dedicated to mass deformed $\mathcal{N} = 4$ theories. In section 2, we demonstrate that the characteristic polynomial of the extremal superpotential values in this theory is a polynomial with coefficients in the graded ring of modular forms. We analyze how the roots, i.e. the extremal superpotential values, extend the field of functions on modular curves, and generate the corresponding Galois group. The analysis of the characteristic polynomial shows that there are two possibilities for the fate of modular invariance in the vacua:

- There can be a residual modular invariance, that is characterized by the fact that Γ_{Galois} is a congruence subgroup of $\text{PSL}(2, \mathbb{Z})$. The theories with gauge algebra $\mathfrak{su}(N)$ fall in this category, as shown in section 3. We show that in general the Galois group is a strict subgroup of the permutation group, and we compute it explicitly in low-rank examples.

- Modular invariance can be completely broken. In this case the roots of the polynomial with coefficients in the ring of modular forms provide an extension which goes beyond the theory of modular forms for congruence subgroups and includes functions with singularities inside the fundamental domain. The theory with gauge algebra $\mathfrak{so}(8)$ has this property. It is analyzed in section 4.

In section 5 we illustrate how the concepts we covered in the case of the mass deformed $\mathcal{N} = 4$ theory generalize to $\mathcal{N} = 2$ superconformal QCD broken by mass terms to an $\mathcal{N} = 1$ supersymmetric theory. In the process, we provide a detailed analysis of how the duality group acts in the mass deformed theory, and how the permutation group supersedes the duality group in describing the set of massive vacua. We prove that superconformal QCD belongs to the class of theories where modular invariance is completely broken in a given vacuum.

Our detailed discussion builds in part on previous work, in which we analyzed the vacuum structure of $\mathcal{N} = 4$ supersymmetric Yang-Mills theory with mass deformations for the three adjoint chiral multiplets. This $\mathcal{N} = 1^*$ theory has a rich structure of massive vacua [11, 12]. In the work [13], we used a combination of numerical analysis of the associated elliptic integrable system [11, 14, 15], as well as expectations from gauge theory to amass a treasure trove of data, which required further interpretation on several points. In [16], we provided a systematic and simplified count of the number of massive vacua of all $\mathcal{N} = 1^*$ theories on $\mathbb{R}^4$. In [17], we analyzed the count of vacua upon compactifying the theory on a circle, and the analytic description of massless branches of vacua. In [18] we showed how the count of massive vacua for the compactified theory, and its invariance under duality, leads to intriguing number theoretic identities.

Using the general picture described in this paper we further our understanding of the wealth of data we excavated in [13]. We acquire a deeper algebraic and analytic understanding of both the extremal superpotential values in the massive vacua as well as the duality symmetry breaking patterns by embedding our findings in Galois theory.

2 Mass deformed $\mathcal{N} = 4$ super Yang-Mills theories

In this section, we study the $\mathcal{N} = 4$ super Yang-Mills theory deformed by three mass terms for the three $\mathcal{N} = 1$ chiral multiplets in the adjoint. In this deformed theory, an operator that distinguishes all the vacua at generic coupling is the superpotential W. The superpotential will therefore serve as our generic operator $\mathcal{O}$, in the sense of section 1. We first recall a few salient features of the $\mathcal{N} = 1^*$ theory and its vacua. Then we write down the characteristic polynomial of the superpotential and explain how it diagnoses the way in which the modular invariance of the $\mathcal{N} = 4$ theory is partially broken in the vacua. The theory is then illustrated in the simplest case of the $\mathfrak{su}(2)$ theory. We provide example applications as well as remarks on the relation to the vacuum expectation values of the full chiral ring. In section 3 we will further exemplify our analysis with the $\mathfrak{su}(N)$ theories with $N \geq 3$.

2.1 Duality in the $\mathcal{N} = 4$ theory and permutations of $\mathcal{N} = 1^*$ vacua

In this subsection, we identify the parameter space, the characteristic polynomial, the relevant Galois theory, and the reduced modular covariance of the theory in a given vacuum.

2.1.1 The parameter space

We recall that the $\mathcal{N} = 4$ super Yang-Mills theories with gauge algebra $\mathfrak{g}$ take on various guises, depending on the global choice of gauge group, and the spectrum of line operators [19]. The implications of these global choices are commented on in the case of the Lie algebra $\mathfrak{g} = \mathfrak{su}(N)$ in the appendix, section B.1. In the following, we will focus on local physics on the topologically trivial space $\mathbb{R}^{1,3}$, which depends only on the choice of Lie gauge algebra. We will correspondingly refer to *the $\mathcal{N} = 4$ theory with gauge algebra $\mathfrak{g}$*.

When the algebra $\mathfrak{g}$ is simply laced, which will be the case throughout this article, the $\mathcal{N} = 4$ theory is invariant under the action of the modular group $\mathrm{PSL}(2, \mathbb{Z})$ acting on the complexified coupling constant τ. The parameter space can then be identified with the quotient

$$\bar{C}_{\mathcal{N}=4} = \mathrm{PSL}(2, \mathbb{Z}) \backslash \mathfrak{H} \tag{2.1}$$

of the upper half-plane $\mathfrak{H}$ by this group. The half-plane $\mathfrak{H}$ contains two equivalence classes of fixed points for the action of $\mathrm{PSL}(2, \mathbb{Z})$ and as a result, the space $\bar{C}_{\mathcal{N}=4}$ is a non-trivial orbifold. It can be seen as a space with the topology of a plane with two orbifold points of order two and three respectively. Using the appropriate notion of loops in an orbifold, we can define the fundamental group of $\bar{C}_{\mathcal{N}=4}$ and find

$$\pi_1(\bar{C}_{\mathcal{N}=4}) = \mathbb{Z}_2 * \mathbb{Z}_3 = \mathrm{PSL}(2, \mathbb{Z}), \tag{2.2}$$

where the symbol $*$ denotes the free product between groups.

When we deform $\mathcal{N} = 4$ on $\mathbb{R}^{1,3}$ by three mass terms for the adjoint chiral multiplets, we obtain the $\mathcal{N} = 1^*$ theory. This theory has a finite number n of massive vacua, which can be characterized by the expectation value of the superpotential W. Since the vacua are identified with the extrema of the superpotential, the latter is a good generic operator whose characteristic polynomial allows to probe the vacuum structure.

The space of massive vacua is a bundle V_{massive} over the parameter space with finite fiber. The parameter space includes the three masses, in addition to the space $\bar{C}_{\mathcal{N}=1^*}(\mathfrak{g})$ corresponding to the complexified coupling constant. As long as the masses remain non-zero, they can be rescaled without changing the vacuum structure, and therefore they factorize in the bundle $V_{\text{massive}} \to \bar{C}_{\mathcal{N}=1^*}(\mathfrak{g})$. As a consequence, a minimal hypothesis is that even after the mass deformation, the parameter space of the $\mathcal{N} = 1^*$ theory is a one complex dimensional manifold $\bar{C}_{\mathcal{N}=1^*}(\mathfrak{g})$. When no extra singularity is introduced by the mass deformation, this manifold is equal to the space (2.1). We will loop back to this hypothesis and discuss that Occam's razor may well cut too deep.

2.1.2 The characteristic polynomial

We analyze the structure of the bundle of massive vacua over the coupling space $C_{\mathcal{N}=1^*}(\mathfrak{g})$ using the values of the superpotential at its n massive extrema. For the $\mathfrak{su}(N)$ theories, the superpotential extrema W_i in the massive vacua are known explicitly [11, 12, 20], while for other gauge algebras only partial results are available [13]. We define the characteristic superpotential polynomial P_τ which has as roots the values of the superpotential in the massive vacua at gauge coupling $\tau \in C_{\mathcal{N}=1^*}(\mathfrak{g})$, and coefficient one for the maximal degree term:

$$P_\tau(W) = \prod_{i=1}^{n}(W - W_i(\tau)). \tag{2.3}$$

According to equation (1.1), if there is no extra singularity, the superpotentials $W_i(\tau)$ constitute a vector-valued modular form of weight two for the modular group $\text{PSL}(2,\mathbb{Z})$ where all the elements of this group are represented by permutation matrices. In any case, the coefficients of (2.3) are symmetric functions of the roots, and therefore are modular forms of $\text{PSL}(2,\mathbb{Z})$ with weight equal to twice their degree in the values W_i, which means that they belong to the graded ring $\mathfrak{m}$ of polynomials in E_4 and E_6 with coefficients in $\mathbb{C}$

$$\mathfrak{m} = \mathbb{C}[E_4, E_6]. \tag{2.4}$$

Here and in the following, the functions E_{2n} for $n \geq 1$ are the Eisenstein series of weight $2n$ with unit leading coefficient, and Fourier expansion

$$E_2(\tau) = 1 - 24\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}, \qquad E_4(\tau) = 1 + 240\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n}, \qquad E_6(\tau) = 1 - 504\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n}, \tag{2.5}$$

with $q = e^{2\pi i \tau}$. The graded dimension of the ring $\mathfrak{m}$ is encoded in the Hilbert series

$$\dim \mathfrak{m} := \sum_{k=0}^{\infty} t^k \dim \mathcal{M}_k(\text{PSL}(2,\mathbb{Z})) = \frac{1}{(1-t^4)(1-t^6)}. \tag{2.6}$$

We assign a modular weight two to the formal variable W such that the whole characteristic polynomial has a modular weight equal to twice its degree. It will also be useful to introduce another degree n polynomial $\tilde{P}_\tau(Z)$, where $Z = \frac{E_4}{E_6} W$ is a formal variable of weight zero, defined by

$$\tilde{P}_\tau(Z) = \left(\frac{E_4}{E_6}\right)^n P_\tau \left(\frac{E_6}{E_4} Z\right) . \tag{2.7}$$

The coefficients of this polynomial are meromorphic functions on the space (2.1), which can be written as quotients of polynomials in the modular Klein invariant

$$j(\tau) = \frac{1728 E_4^3(\tau)}{E_4^3(\tau) - E_6^2(\tau)} , \tag{2.8}$$

or in other words $\tilde{P}_\tau \in \mathfrak{k}[Z]$ where $\mathfrak{k} = \mathbb{C}(j)$.

2.1.3 The Galois correspondence

Consider an $\mathcal{N} = 1^*$ theory with a simply laced Lie gauge algebra $\mathfrak{g}$, with its characteristic polynomial $P_\tau \in \mathfrak{m}[W]$ constructed in (2.3). The degree n of this polynomial is equal to the number of massive vacua, and its roots W_i are pairwise distinct.[2] The polynomial defines a map

$$\begin{aligned} P : C_{\mathcal{N}=1^*}(\mathfrak{g}) &\to \mathbb{C}[W] \\ \tau &\mapsto P_\tau . \end{aligned} \tag{2.9}$$

This map provides an explicit realization of the function σ defined in (1.1). Indeed, along a loop drawn in $C_{\mathcal{N}=1^*}(\mathfrak{g})$, on which by definition the roots of the polynomial are always distinct, we can continuously follow these roots and compute their permutation. This leads us to introduce the discriminant of the characteristic polynomial

$$D(\tau) = \text{Discriminant}(P_\tau) = \prod_{i<j} (W_i(\tau) - W_j(\tau))^2 \in \mathfrak{m} - \{0\} . \tag{2.10}$$

We expect to have permutations of roots when looping around the orbifold points, and around points where two or more roots coincide, which appear as zeros of the discriminant. A zero with a non-trivial monodromy will be called a *non-trivial zero*. In particular, any end of a branch cut of $\sqrt{D(\tau)}$ is a non-trivial zero.

The field extension $\mathfrak{k}(Z_1, \ldots, Z_n)$ is by definition a Galois extension,[3] and the fundamental theorem of Galois theory states that there exists a finite group

$$G = \text{Gal}\left(\mathfrak{k}(Z_1, \ldots, Z_n)/\mathfrak{k}\right) \tag{2.11}$$

---

[2]It is possible that the superpotentials in two different vacua coincide for some particular value of τ, as it happens for instance in the limit $\tau \to i\infty$. However, the W_i considered as functions of τ are pairwise distinct.

[3]We recall that a Galois extension is characterized by the fact that it is the splitting field of some separable polynomial with coefficients in the base field. A polynomial is called separable if its roots in any algebraic closure of the base field are distinct.
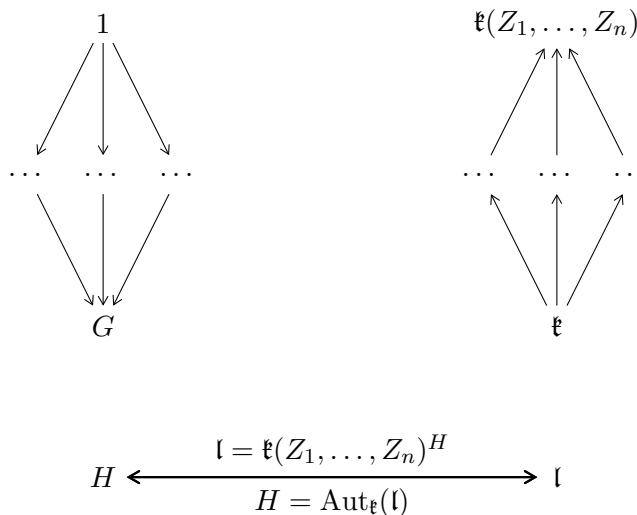
Figure 1. Schematic Galois correspondence.

such that the subgroup structure of G coincides with the field extensions that sit between $\mathfrak{k}$ and $\mathfrak{k}(Z_1, \ldots, Z_n)$, as illustrated in figure 1. This gives us a cross-fertilizing relation between global aspects of the geometry of the parameter space, characterized by the Galois group, and local data about individual vacua.

Note that if $\sqrt{D(\tau)}$ has branch cuts, or more generally non-trivial zeros, the modular transformations like T or S become path-dependent. Correspondingly, the superpotential values in the multiplets of vacua that contain roots of a characteristic polynomial with such a discriminant no longer exhibit modular covariance. This situation will be illustrated in section 4. On the other hand, if there is no non-trivial zero, modular transformations can be performed, and modular covariance is broken in any given vacuum to a reduced modular covariance that can be studied using Galois theory, as described in the next paragraph.

2.1.4 Reduced modular covariance

In this subsection, we assume that $D(\tau)$ has no non-trivial zero. From the polynomial we can then always construct a duality diagram which represents the action of the generators S and T of the modular group. In other words, the vector $(W_1, \ldots, W_n)$ is a weight two vector-valued modular form. The fact that $D(\tau)$ has no non-trivial zero assures that this action is well-defined and independent from the path followed to compute it. There is a one-to-one correspondence between irreducible factors of the polynomial P over the ring $\mathfrak{m}$ and connected components of the duality diagram, and for simplicity we will focus in this section on an irreducible factor.

We then have a transitive permutation representation of $\mathrm{PSL}(2, \mathbb{Z})$, and this defines uniquely a conjugacy class of subgroups of $\mathrm{PSL}(2, \mathbb{Z})$. There is an algorithm [21] that allows to know whether this conjugacy class contains a congruence subgroup or not.[4] In the following, we assume the conjugacy class does contain a congruence subgroup that

---

[4]Definitions and useful facts about congruence subgroups are collected in appendix A.

we call Γ_{roots}.[5] This notation is justified by the fact that the roots of the characteristic polynomial are in bijection with coset representatives of Γ_{roots}. Congruence subgroups are fairly well known, and an exhaustive list has been computed for genus lower than 24, see [22]. In order to identify the congruence subgroup, one first reads off from the permutation diagram

- the number c_2 of roots fixed by S,

- the number c_3 of roots fixed by ST^{-1},

- the partition ρ of n given by the T-cycles structure, and in particular the number c_∞ of T-cycles.

The genus of the group is then given by

$$g = 1 + \frac{n}{12} - \frac{c_\infty}{2} - \frac{c_3}{3} - \frac{c_2}{4}. \tag{2.12}$$

This set of data entirely characterizes the group Γ_{roots}.[6] If $g \leq 24$, it can be found in the tables of [22] using the above data and the T-multiplet structure. The conjugates of Γ_{roots} are the stabilizers of the individual roots of the characteristic polynomial. Their intersection is a congruence[7] subgroup that is equal to Γ_{Galois}.

To the standard Galois duality that relates subgroups of the Galois group and field extensions, as depicted in the first two columns of figure 2, we now add a third structure, namely the congruence subgroups containing Γ_{Galois}. Let us then consider a congruence subgroup Γ such that

$$\Gamma_{\mathrm{Galois}} \subseteq \Gamma \subseteq \mathrm{PSL}(2,\mathbb{Z}). \tag{2.14}$$

From Γ we can construct a compact Riemann surface, called the *modular curve* $\mathbf{X}(\Gamma)$, which is the appropriate compactification [23, 24] of $\Gamma\backslash\mathfrak{H}$. This permits us to use the general idea that an algebraic curve is entirely characterized by fields of functions $\mathbb{C}(\mathbf{X}(\Gamma))$ defined on it, and that field extensions correspond to morphisms between curves. It is clear that (2.14) implies

$$\mathbb{C}(\mathbf{X}(\Gamma_{\mathrm{Galois}})) \supseteq \mathbb{C}(\mathbf{X}(\Gamma)) \supseteq \mathbb{C}(\mathbf{X}(\mathrm{PSL}(2,\mathbb{Z}))). \tag{2.15}$$

---

[5]For practical purposes, this assumption is not needed. In any particular situation, one simply computes the group Γ_{roots} assuming that it is a congruence subgroup, and then checks that it indeed leaves one root invariant.

[6]In particular, we remind the reader that the graded dimension of the ring of modular forms for any congruence subgroup Γ that contains the matrix $-I$ is given by [23]

$$H_\Gamma(t) = \dim \mathcal{M}(\Gamma) = 1 + \sum_{k=1}^\infty t^{2k} \left((2k-1)(g-1) + \left\lfloor \frac{k}{2} \right\rfloor c_2 + \left\lfloor \frac{2k}{3} \right\rfloor c_3 + k c_\infty \right). \tag{2.13}$$

If Γ does not contain $-I$, the above formula still gives the correct contribution for even powers of t, but there is an additional contribution from odd powers of t for which we found no general formula.

[7]The group $\Gamma(N)$ is normal in $\mathrm{PSL}(2,\mathbb{Z})$ as it is the kernel of the reduction modulo N. Then if $\Gamma(N) \subset \Gamma_{\mathrm{roots}}$, the group $\Gamma(N)$ is also contained in all the conjugates of Γ_{roots}, and in their intersection.
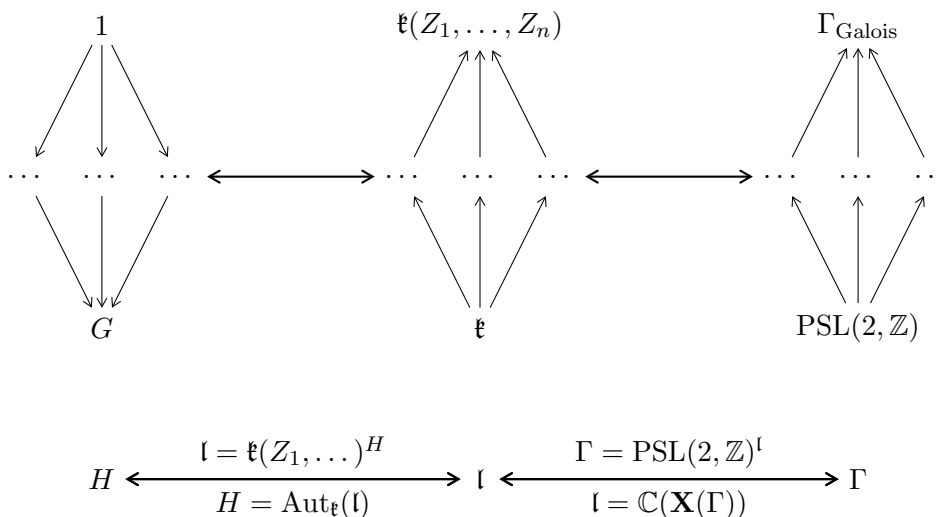
Figure 2. Schematic Galois correspondence for rings of modular forms. The diagram on the left represents the subgroup structure of G, the middle one the fields of meromorphic functions on modular curves generated by polynomials of the roots of the characteristic polynomial and the diagram on the right represents congruence subgroups that contain Γ_{Galois}. The bottom line gives the explicit bijections between corresponding elements in the different diagrams.

In other words, every group contained between Γ_{Galois} and $\text{PSL}(2,\mathbb{Z})$ gives a field extension of $\mathbb{C}(\mathbf{X}(\text{PSL}(2,\mathbb{Z})))$ contained inside $\mathbb{C}(\mathbf{X}(\Gamma_{\text{Galois}}))$. Conversely, given such a field extension, the subgroup of $\text{PSL}(2,\mathbb{Z})$ that leaves all its elements invariant contains Γ_{Galois}, and in particular it is a congruence subgroup.

To summarize, we have constructed a bijection between the subgroups of G, the field extensions between $\mathfrak{k}$ and $\mathfrak{k}(Z_1, \ldots, Z_n)$, and the congruence subgroups that contain Γ_{Galois}, as illustrated in figure 2. In order to make the discussion more concrete, we work out an example in full detail.

2.2 The $\mathfrak{su}(2)$ $\mathcal{N} = 1^*$ theory

The simplest illustration of the general formalism above is provided by the $\mathcal{N} = 1^*$ theory with gauge algebra $\mathfrak{su}(2)$. It has three inequivalent vacua on $\mathbb{R}^4$ [11, 14]. The vacua can be described in terms of the extremal values of an elliptic integrable potential. The corresponding extremal values of the superpotential are[8] [11, 12]

$$
\begin{aligned}
W_1 &= -2E_2(q) + 4E_2(q^2)\,, \\
W_2 &= -2E_2(q) + E_2(q^{1/2})\,, \\
W_3 &= -2E_2(q) + E_2(-q^{1/2})\,,
\end{aligned}
\tag{2.16}
$$

where the parameter $q = e^{2\pi i \tau}$ is the exponential of the complexified coupling τ of the theory. The first value W_1 corresponds semi-classically to a Higgs vacuum obtained by

---

[8]We choose the normalization of the superpotential extremal values (2.17) such that the characteristic polynomial (2.17) has coefficients in $\mathbb{Z}[E_4, E_6]$.

giving a vacuum expectation value to the adjoint scalars while the two values $W_{2,3}$ correspond to confining vacua of an unbroken $\mathfrak{su}(2)$ pure $\mathcal{N} = 1$ theory. We then compute the characteristic polynomial:

$$P_\tau^{\mathfrak{su}(2)}(W) = (W - W_1)(W - W_2)(W - W_3) = W^3 - 3E_4(q)W - 2E_6(q). \qquad (2.17)$$

The discriminant of this degree three polynomial is

$$D(\tau) = 108 \left(E_4^3 - E_6^2\right) \propto \Delta(\tau), \qquad (2.18)$$

where $\Delta(\tau) = \frac{1}{1728}(E_4^3 - E_6^2)$ is the modular discriminant, which has no zero on $\mathfrak{H}$. We are then in the situation where $D(\tau)$ has no non-trivial zero, and we can use the tools of section 2.1.4. Using the well-known transformation of the Eisenstein series E_2 under $\tau \mapsto -1/\tau$, or physical expectations combined with consistency, one can derive the duality diagram of figure 3, on which we read $c_2 = 1$, $c_3 = 0$, $\rho = 2 + 1$, $c_\infty = 2$, and then $g = 0$. As explained in footnote 5, we assume that Γ_{roots} is a congruence subgroup, which allows us to identify it as

$$\Gamma_{\text{roots}} = \Gamma_0(2), \qquad (2.19)$$

and then using the set of generators $\Gamma_0(2) = \langle T, ST^2S \rangle$, one checks that it leaves W_1 invariant. The other roots W_2 and W_3 are left invariant under the two conjugates of $\Gamma_0(2)$, as can be read from the diagram: W_2 is left invariant by $S\Gamma_0(2)S$ and W_3 by $(ST)^{-1}\Gamma_0(2)(ST)$. One can check that this provides a set of coset representatives $\{\alpha_1 = 1, \alpha_2 = S, \alpha_3 = ST\}$ of $\Gamma_0(2)\backslash \mathrm{SL}(2, \mathbb{Z})$,

$$\mathrm{SL}(2, \mathbb{Z}) = \bigcup_{i=1}^3 \Gamma_0(2)\alpha_i. \qquad (2.20)$$

The three isomorphic stabilizers $\Gamma_0(2)_i = \alpha_i^{-1}\Gamma_0(2)\alpha_i$ are the groups of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \qquad (2.21)$$

that satisfy, respectively, $c \equiv 0$, $b \equiv 0$ and $a - b + c - d \equiv 0$ modulo 2. Using these characterizations, it is straightforward to prove that[9]

$$\bigcap_{i=1}^3 \Gamma_0(2)_i = \Gamma(2), \qquad (2.22)$$

which gives an alternative proof of the fact that $\Gamma(2) = \langle T^2, ST^2S \rangle$ is the stabilizer of all three superpotentials [20]. The space of modular forms of weight two for $\Gamma(2)$ is two dimensional, and a basis is given by any family of two independent elements constructed from the $W_{1,2,3}$, for instance $(W_1, W_2 - W_3)$. In fact, these two elements are also generators of the full ring of modular forms $\mathcal{M}(\Gamma(2))$.[10]

---

[9]A matrix in the intersection has $b \equiv c \equiv a - d \equiv 0$, and $ad \equiv 1$, hence $a \equiv d \equiv 1$ and it is in $\Gamma(2)$. The converse is obvious.

[10]One way to prove this is the following. According to example 1.7 in [25], the full field of modular forms is generated by the modular forms of weight up to 6. The space $\mathcal{M}_4(\Gamma(2))$ of modular forms of weight four has dimension three and $\mathcal{M}_6(\Gamma(2))$ has dimension four, and we can check that these two spaces are generated as rings by W_1 and $W_2 - W_3$.
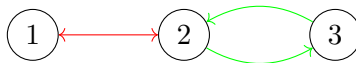
Figure 3. The duality group action on the three vacua of the $\mathfrak{su}(2)$ $\mathcal{N} = 1^*$ theory. The action of T on the complexified coupling is indicated in green, the action of S in red.
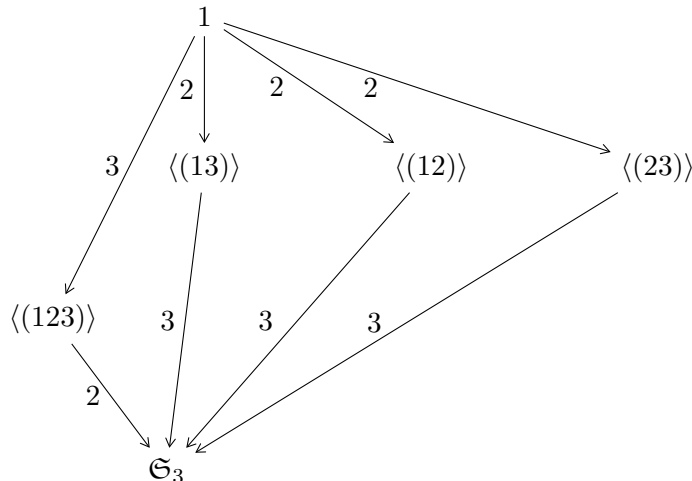

Figure 4. Subgroup structure of $\mathfrak{S}_3$. Each node is the subgroup that leaves invariant the corresponding field in figure 5. The integer on each arrow indicates the ratio of the cardinalities of the two groups connected by the arrow.

We now study the characteristic polynomial from the perspective of Galois theory. As by the general considerations of section 2.1, the polynomial (2.17) has coefficients in the graded ring $\mathfrak{m}$ of modular forms. The polynomial $\tilde{P}_\tau^{\mathfrak{su}(2)}$, defined in equation (2.7), is

$$\tilde{P}_\tau^{\mathfrak{su}(2)} = Z^3 - \frac{3j}{j - 1728} Z - \frac{2j}{j - 1728} \in \mathfrak{k}[Z] \, . \tag{2.23}$$

This polynomial is irreducible, and this gives degree three field extensions $\mathfrak{k}[Z_i]$ for $i = 1, 2, 3$. Adding another root to one of the fields $\mathfrak{k}[Z_i]$, one obtains immediately the full extension $\mathfrak{k}[Z_1, Z_2, Z_3]$ because $Z_1 + Z_2 + Z_3 = 0$, and this extension has degree lower or equal to two as a consequence of $Z_1 Z_2 + Z_2 Z_3 + Z_3 Z_1 = -\frac{3j}{j-1728}$. But the degree can not be one, since Z_2 has fractional powers of q in its expansion, and hence is not in $\mathfrak{k}[Z_1]$. So the degree is exactly two.

As a result of the Galois correspondence, there is a bijection between the diagram of ring extensions by polynomials of the roots of (2.17) and the subgroups of the Galois group $G^{\mathfrak{su}(2)}$, which is itself a subgroup of the group of permutations of these roots. The computations of the previous paragraph show that $|G^{\mathfrak{su}(2)}| \geq 2 \cdot 3$, which implies

$$G^{\mathfrak{su}(2)} = \mathfrak{S}_3 \, . \tag{2.24}$$

We then obtain immediately the diagram of subgroups, see figure 4. In this first example then, the Galois group is equal to the full permutation group of the roots. Moreover, the
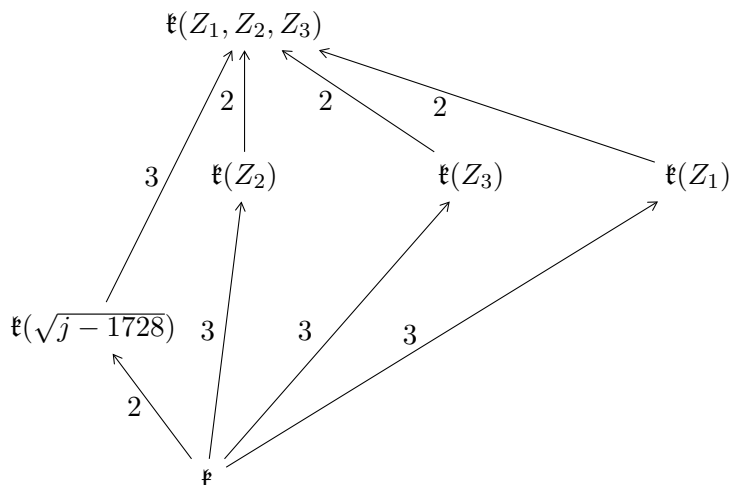
Figure 5. Field extensions generated by the roots of the characteristic polynomial for massive vacua of $\mathcal{N} = 1^*$ theory with $\mathfrak{su}(2)$ gauge algebra. The integer on each arrow indicates the degree of the field extension.

Galois group coincides with the duality group action on the massive vacua. According to the Galois correspondence, we observe that there should also be a degree two extension of $\mathfrak{k}$ given by the functions that are invariant under the permutation (123), but not under the exchange of only two roots. An example of a function leading to such an extension is

$$(Z_1 - Z_2)(Z_2 - Z_3)(Z_3 - Z_1) \propto \frac{j}{(j - 1728)^{3/2}}\,, \tag{2.25}$$

which indeed is of order two. The function $\sqrt{j - 1728}$ is sent to $-\sqrt{j - 1728}$ by the transformations S and T, so its stabilizer is the group $\Gamma^2 = \langle T^2, ST \rangle$ of elements of $\mathrm{PSL}(2, \mathbb{Z})$ of even length, when considered as words with letters S, T. This allows to complete the diagram of field extensions, see figure 5. In turn, we have computed the stabilizer group of all these field extensions, which gives birth to a third diagram where the vertexes are certain congruence subgroups, as represented in figure 6. This completes the explicit Galois correspondence of figure 2 in the $\mathfrak{su}(2)$ case.

2.3 Applications

In this subsection, we pause to consider a few applications of the constructions we presented. In section 3, we provide further examples.

2.3.1 Tensor products

We have introduced a characteristic polynomial of degree n whose roots are the values of W in the n vacua of the theory $\mathcal{T}$. This polynomial can be interpreted as living in the tensor product of theories $\mathcal{T}^{\otimes n}$. We are thus lead to explore the tensor products of the theory $\mathcal{T}$ with itself. Some special diagonal sectors of this extended theory (with a different choice of vacuum for each factor) have a reduced set of vacuum expectation values for the superpotential, that correspond to non-trivial subgroups of the Galois group. In other
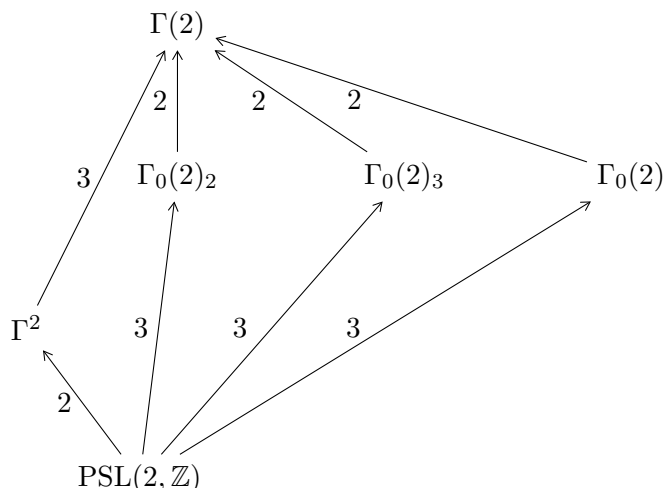
Figure 6. Congruence subgroups between $\Gamma(1)$ and $\Gamma(2)$. The integer on each arrow indicate the degree the group at the end of the arrow inside the group at the origin.

words, the Galois correspondence tells us what are the sectors within the tensor product that have an enhanced modular invariance. This provides an incarnation of the Galois correspondence in tensor product theories with a particular choice of boundary conditions in each factor theory.

2.3.2 On the chiral ring

In this subsection, we consider a few properties of the chiral ring. Firstly, we take the perspective that we give two of the three adjoint chiral multiplets a larger mass than the third. After having integrated out those two chiral multiplets, the effective superpotential can be expressed in term of the third one, which we call Φ, as

$$W = \langle \operatorname{tr} \Phi^2 \rangle. \tag{2.26}$$

The chiral ring is then generated by the operators $\operatorname{tr} \Phi^k$, $\operatorname{tr} \Phi^k W_\alpha$ and $\operatorname{tr} \Phi^k W_\alpha W^\alpha$ where W_α is the vector multiplet superfield. We focus on the bosonic sector. In the $\mathfrak{su}(N)$ theory, there are N operators $\operatorname{tr} \Phi^k$ and N operators $\operatorname{tr} \Phi^k W_\alpha W^\alpha$ which satisfy quantum chiral ring relations. Let us study the vacuum expectation values of $\operatorname{tr} \Phi^k$ first.

There are several possible ways to define condensates $\langle \operatorname{tr} \Phi^k \rangle$ in the $\mathcal{N} = 1^*$ theory. One of them is to use the Dijkgraaf-Vafa approach and solve a matrix model [26] and another is to use the exact integrable system and compute traces of powers of the Lax matrices [27]. However, mixing ambiguities [28] will makes these different results for $\langle \operatorname{tr} \Phi^k \rangle$ differ by linear combinations in the operators $\langle \operatorname{tr} \Phi^l \rangle$ for $l < k$ as well as vacuum independent functions of the coupling τ. This ambiguity can be solved when there are no non-trivial zeros by choosing the combination that behaves as a modular form under the modular transformations [29]. In this case, this proves that the sector of the chiral ring generated by the $\langle \operatorname{tr} \Phi^k \rangle$ is included in the space of forms $\mathcal{M}(\Gamma_{\text{Galois}})$.

The full chiral ring also contains quasi-modular forms, as for instance $\langle \operatorname{tr} W^\alpha W_\alpha \rangle = -\frac{1}{2\pi i}\partial_\tau \langle \operatorname{tr} \Phi^2 \rangle$. As we know the value of the exact effective superpotential $\langle W \rangle$ in a vacuum, we can deduce the value of the gaugino condensate because it appears in the tree-level superpotential multiplied by τ. We then have $\langle S \rangle = \langle \operatorname{tr} W^\alpha W_\alpha \rangle = -\frac{1}{2\pi i}\partial_\tau \langle W \rangle$. But we also know from our general discussion that there is a polynomial equation $P(\langle W \rangle, E_4, E_6) = 0$, where P is a polynomial with integer coefficients. We can differentiate with respect to τ:

$$- \langle S \rangle \partial_{\langle W \rangle} P + \frac{1}{3}(E_2 E_4 - E_6)\partial_{E_4} P + \frac{1}{2}(E_2 E_6 - E_4^2)\partial_{E_6} P = 0\,. \tag{2.27}$$

This equation shows that $\langle S \rangle$ belongs to the field $\mathfrak{k}(E_2, W_i) = \mathbb{C}(E_2, E_4, E_6, W_i)$:

$$\langle S \rangle = \frac{\frac{1}{3}(E_2 E_4 - E_6)\partial_{E_4} P + \frac{1}{2}(E_2 E_6 - E_4^2)\partial_{E_6} P}{\partial_{\langle W \rangle} P}\,. \tag{2.28}$$

In fact, we can say more: the derivative of any modular form in $\mathcal{M}(\Gamma)$ belongs to the ring of quasi-modular forms $\mathcal{M}^{\text{quasi}}(\Gamma)$ that is obtained by simply adding E_2,

$$\mathcal{M}^{\text{quasi}}(\Gamma) = \mathcal{M}(\Gamma)[E_2]\,. \tag{2.29}$$

As a consequence, although it is not obvious on the expression (2.28), the gaugino condensate can be expressed as a linear combination of E_2^2, $E_2 W$ and W^2, and the explicit combination is easily deduced in a given example from (2.28). For instance, in the $\mathfrak{su}(2)$ case, the polynomial (2.17) and the division in the corresponding ideal give

$$\langle S \rangle = -\frac{(E_2 E_4 - E_6)W + E_2 E_6 - E_4^2}{3(W^2 - E_4)} = \frac{1}{6}(W^2 - W E_2 - 2E_4)\,. \tag{2.30}$$

It would be most interesting to complete the calculation of the vacuum expectation values of the chiral ring operators, including the vacuum expectation values of all three chiral fields Φ_i.

2.3.3 Domain wall kinematics in the quantum theory

There are also very direct uses of the superpotential values. To illustrate this aspect, we analyze the kinematical stability of BPS domain walls of the $\mathfrak{su}(2)$ $\mathcal{N} = 1^*$ theory in the quantum theory, at any value of the complexified gauge coupling τ. We will combine our results with those obtained in the classical theory [30], and the physics of confining gauge theories to propose a global picture of the existence of domain walls in the theory.

Firstly, we recall that half BPS domain walls in $\mathcal{N} = 1$ theories in four dimensions preserve two supercharges. The corresponding central charge is a complexified tension T, which relates to the tension M through the formula [31]

$$M \geq |T|\,, \tag{2.31}$$

with saturation for BPS domain walls. If a BPS domain wall composed of BPS domain walls with complexified tensions T_1 and T_2 exists, it then has mass

$$M_3 = |T_3| = |T_1 + T_2| \leq |T_1| + |T_2| = M_1 + M_2\,, \tag{2.32}$$

which is automatically stable. The wall is marginally stable if the phases of the central charges are equal. This will typically happen in a space of real co-dimension one in the space of couplings. A generic expectation would be then that BPS domain walls are stable or unstable on one or another side of such a wall of marginal stability [31, 32].

Let's reconsider the example of the $\mathfrak{su}(2)$ theory with superpotential values $W_{1,2,3}$ as in equation (2.17). We note that for τ purely imaginary, as well as in the semi-classical limit $\tau \to i\infty$, the critical values are real. We have available an existence analysis for classical domain walls [30]. In this limit, one has a full handle on the kinetic term, and therefore on the first order flow equation for a BPS domain wall [31]. One can then explicitly determine whether the BPS wall exists. In [30] it was found that a domain wall exists between two massive vacua if the superpotential on the left (say) is larger than the one on the right. Thus, for $\mathfrak{su}(2)$ for instance, we have a supersymmetric wall interpolating between the Higgs vacuum and the confining vacua. Indeed, the classical limits of the above superpotentials are $(W_1, W_2, W_3)_{\text{clas}} = (-1, -1, 2)$ respectively. The first two correspond to confining vacua and the last to the Higgs vacuum. The first two are degenerate in the classical regime. Thus, the classical limit suggests the existence of supersymmetric domain walls between vacua 1 and 3 and between 2 and 3. In the classical limit, the tension of the domain wall between the (quantum mechanically) confining vacua becomes zero. At finite and small coupling, the expectation from the pure $\mathcal{N} = 1$ theory is that the domain wall between the two confining vacua exists and is BPS. At finite and small coupling, these facts provide us with a full picture of the domain walls. We can ask whether this picture is accurate in the deep quantum regime.

Firstly, we check whether we have another point at which extremal values of the superpotential coincide (as they do in the classical point). According to (2.18), there are coinciding roots at values of τ where $D(\tau)$ vanishes, which happens only at the cusps.

Most importantly, we can also scan for walls of marginal stability, where the three roots of the characteristic polynomial are aligned. These may signal that BPS walls that exist near the classical regime decay at strong coupling. The sum of the roots of the characteristic polynomial always vanishes. If they are aligned, then there exists a phase θ such that the $e^{-i\theta}W_j$ are all real. Those are then the three real roots of $W^3 - 3e^{2i\theta}E_4 W - 2e^{3i\theta}E_6$. Hence the coefficients of this polynomial must be real, and the discriminant must be positive. In particular $(e^{2i\theta}E_4)^3/(e^{3i\theta}E_6)^2 = E_4^3/E_6^2$ is real. This is true on the lines $\tau_1 = 0$ and $\tau_1 = 1/2$. However on the line $\tau_1 = 1/2$, the discriminant $\eta(\tau)^{24}$ is negative. Therefore the three roots are aligned if and only if $\tau_1 = 0$ (in the fundamental domain). This potentially is a wall of marginal stability. In any event, since the classical regime near $\tau_2 = i\infty$, at non-zero θ angle extends towards strong coupling without crossing the only potential wall of marginal stability, we conclude that the existence of BPS domain walls in the deep quantum regime is fixed by the existence analysis of BPS domain walls in the classical regime at non-zero θ-angle. This conclusion illustrates that using our knowledge of the exact values of the superpotential, we can infer properties of the deep quantum regime of the $\mathcal{N} = 1^*$ theory.

3 The $\mathfrak{su}(N)$ theory

In this section, we generalize to the $\mathfrak{su}(N)$ theory the structures covered in the previous section in the case of $\mathfrak{su}(2)$. We will see that the Galois group is in general smaller than the full permutation group of vacua. The order N lattices of $\mathbb{Z}_N \times \mathbb{Z}_N$ play a classifying role [14], and we start by collecting useful properties of these lattices. These properties imply that all $\mathfrak{su}(N)$ $\mathcal{N} = 1^*$ theories belong to the class of theories that still display reduced modular invariance in any given vacuum. See also [28]. This can be thought off as a consequence of the toroidal geometries governing both the $\mathcal{N} = 2$ and the $\mathcal{N} = 1$ mass deformed theories [14]. We detail the reduced modular invariance in low-rank examples and highlight some salient features.

3.1 Order N lattices of $\mathbb{Z}_N \times \mathbb{Z}_N$ and dualities

An order N lattice of the group $\mathbb{Z}_N \times \mathbb{Z}_N$ is an order N subgroup of $\mathbb{Z}_N \times \mathbb{Z}_N$. There are $\sigma_1(N) = \sum_{d|N} d$ such lattices. We use the following parametrization:

$$L = L_{N,p,k} = \left\{ (pr + sk, sq) \in \mathbb{Z}_N^2 | r \in \mathbb{Z}_q,\, s \in \mathbb{Z}_p \right\} , \tag{3.1}$$

where p is a divisor of N, the integer q is defined by $pq = N$ and $k \in \mathbb{Z}_p$. Moreover, we define the *level* of the lattice $L_{N,p,k}$ to be $d = \gcd(p, k, N/p)$. Note that we always have $d^2|N$. The group $\mathrm{SL}(2, \mathbb{Z})$ acts on the set of lattices by left multiplication on the lattice points.

The motivation to study the modular transformation properties of these lattices is twofold. On the one hand, the lattices label the possible choices of line operators in a given theory [19], and hence label the theories with $\mathfrak{su}(N)$ gauge algebra. More details on this aspect can be found in appendix B.1.

More important to us here is the fact that the order N lattices of $\mathbb{Z}_N \times \mathbb{Z}_N$ are in bijection with the massive vacua of the $\mathcal{N} = 1^*$ $\mathfrak{su}(N)$ theory on $\mathbb{R}^4$ [14]. The superpotential in the vacuum corresponding to the lattice L is given by [11, 12]

$$W_L = \sum_{A \neq B \in L} \wp\left(\frac{A - B}{N}, \tau\right) , \tag{3.2}$$

where we identify a point $A = (x, y) \in L$ with the complex number $A = x + \tau y$. Using a re-parametrization of the sum, one obtains

$$Z_L = \frac{E_4}{E_6} W_L = N \frac{E_4}{E_6} \sum_{A \in L - \{(0,0)\}} \wp\left(\frac{A}{N}, \tau\right) . \tag{3.3}$$

Two questions are particularly relevant for our study of the permutation of the massive vacua:

- Which lattices can be related by a duality transformation?

- What are the duality transformations that leave a given lattice (respectively, the set of all lattices) invariant?

The answer to the above questions is given by the three following properties of the lattices (3.1).

1. The structure of T-multiplets is as follows: each divisor D of N gives $\gcd(D, \frac{N}{D})$ cycles of size $D/\gcd(D, \frac{N}{D})$.

2. Two lattices are related by a duality if and only if they have the same level. Hence the number of duality multiplets is the number of divisors of N that are squares.

3. Any lattice of level d is left invariant by $\alpha^{-1}\Gamma_0(N/d^2)\alpha$, where α is a coset representative of $\Gamma_0(N/d^2)$ in $\mathrm{SL}(2,\mathbb{Z})$, and this gives a bijection between level d lattices and $\mathrm{SL}(2,\mathbb{Z})/\Gamma_0(N/d^2)$.

The proofs of these properties are relegated to appendix B.2. Note that it is clear that $\Gamma(N)$ leaves all the lattices invariant (indeed, any matrix in $\Gamma(N)$ acts as the identity in $\mathbb{Z}_N^2$ by definition).

We give one example. For $N = 4$, property 1 tells us that we have three cycles of size one and one cycle of size four under T. As a result of property 2, these cycles organize themselves into two multiplets, which by property 3 have respectively size one and six.

3.2 The characteristic polynomial and the Galois group

The structure of the characteristic polynomial is deduced from the structure of the duality diagram of the vacua. According to property 2 in subsection 3.1, the number of connected components of this graph of dualities is exactly equal to the number of squares dividing N, and from property 3 the number of vertexes in each component is equal to the index of $\Gamma_0(N/d^2)$. This gives the following decomposition of the number of vacua[11]

$$\sigma_1(N) = \sum_{d^2|N} \frac{N}{d^2} \prod_{p|\frac{N}{d^2}} \left(1 + \frac{1}{p}\right) , \tag{3.5}$$

and this decomposition is reflected into the factorization of the degree $\sigma_1(N)$ characteristic polynomial (2.3) into factors of degrees $\frac{N}{d^2} \prod_{p|\frac{N}{d^2}} \left(1 + \frac{1}{p}\right)$. Each multiplet is characterized by its own permutation group, which is the Galois group of the associated factor in the polynomial. This is again reminiscent of the characterization of phases of $\mathcal{N} = 1$ theories through the Galois group associated to the chiral ring relations, advocated in [6]. In general the full Galois group is a subgroup of the product of the individual Galois groups. The physics in these multiplets (e.g. the spectrum of massive excitations) will be different, while in a given multiplet, it will be the same by duality.[12]

---

[11] A dual way of saying the same thing is

$$\sum_{P' \subset P(N)} (-1)^{|P'|} \sigma_1 \left(N \prod_{p \in P'} p^{-2}\right) = N \prod_{p|N} \left(1 + \frac{1}{p}\right) , \tag{3.4}$$

where $P(N)$ is the set of primes p whose square divides N.

[12] Similar remarks apply to the space of theories discussed in appendix B.1.

The identification between the roots of the polynomial and the order N subgroups of $\mathbb{Z}_N \times \mathbb{Z}_N$, on which there is a well-defined action of the modular group, indicates that $\sqrt{D}$ has no branch cut. Accordingly, we know that the field extension is a subfield of the field of modular functions of the modular curve of $\Gamma(N)$ [20]. In the next paragraph, we examine in detail the relation between these two fields, and use the Galois correspondence to learn about the structure of the Galois group.

To compute the Galois group, one follows the same steps as for the $\mathfrak{su}(2)$ example in section 2.2. We compute the intersection of the stabilizers of all the W_i. Let (α_j) be a family of coset representatives of $\Gamma_0(N)$ in $\mathrm{SL}(2, \mathbb{Z})$. We clearly have the inclusion inspired from (2.22)

$$\bigcap_j \alpha_j^{-1} \Gamma_0(N) \alpha_j \supseteq \Gamma(N). \tag{3.6}$$

The inclusion can be strict. To see this, we first prove that if α_i equals the matrix

$$\alpha_i = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, \tag{3.7}$$

then we have the coset

$$\alpha_j^{-1} \Gamma_0(N) \alpha_j = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \,\middle|\, g^2 b + gh(d - a) - h^2 c \equiv 0 \bmod N \right\}. \tag{3.8}$$

If $N \geq 2$, we always have at least the three coset representatives $1, S, ST^{-1}$ in the list (α_j), as can be read on the duality diagram. This shows that the left-hand side of (3.6) is included in

$$\Gamma_{\mathrm{Galois}}(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \,\middle|\, b \equiv c \equiv a - d \equiv a^2 - 1 \equiv 0 \bmod N \right\}, \tag{3.9}$$

but the general expression (3.8) shows that this group is a subgroup of all the $\alpha_j^{-1} \Gamma_0(N) \alpha_j$. Therefore we have proven that

$$\bigcap_j \alpha_j^{-1} \Gamma_0(N) \alpha_j = \Gamma_{\mathrm{Galois}}(N) \supseteq \Gamma(N), \tag{3.10}$$

and the index of the inclusion is the number $s(N)$ of solutions of the equation $a^2 - 1 \equiv 0 \bmod N$.[13] Using the index of $\Gamma(N)$ in $\mathrm{SL}(2, \mathbb{Z})$ (see figure 12 in the appendix) and the Galois correspondence, we deduce that

$$|G_{\mathfrak{su}(N)}| = [\mathrm{SL}(2, \mathbb{Z}) : \Gamma_{\mathrm{Galois}}(N)] = \frac{N^2 \phi(N)}{s(N)} \prod_{p | N} \left(1 + \frac{1}{p} \right). \tag{3.12}$$

---

[13]If $\omega(N)$ is the number of distinct prime divisors of N, we have

$$s(N) = \begin{cases} 2^{\omega(N)-1} & \text{for } N \equiv \pm 2 \bmod 8 \\ 2^{\omega(N)} & \text{for } N \equiv \pm 1, \pm 3, 4 \bmod 8 \\ 2^{\omega(N)+1} & \text{for } N \equiv 0 \bmod 8. \end{cases} \tag{3.11}$$
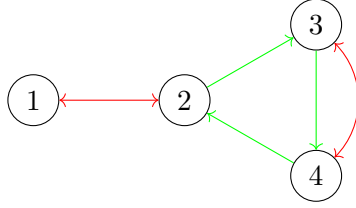
Figure 7. The duality group action on the four vacua of the $\mathfrak{su}(3)$ $\mathcal{N} = 1^*$ theory.

This formula simplifies if $N \geq 3$ is prime: in this case, $\mathbb{Z}_N$ is a field where in addition $1 \neq -1$, so $s(N) = 2$, and we obtain

$$|G_{\mathfrak{su}(N)}|_{N \geq 3 \text{ prime}} = \frac{N^3 - N}{2} = [\text{PSL}(2, \mathbb{Z}) : \Gamma(N)]_{N \text{ prime}}. \tag{3.13}$$

Although it is difficult to characterize precisely the Galois group in general, it is clear that it is a group much smaller than $\mathfrak{S}_{\#\text{vacua}}$. For instance we have just seen that for the $\mathfrak{su}(N)$ theory with $N \geq 3$ prime, the ratio of orders of $\mathfrak{S}_{\#\text{vacua}}$ and G is $2(N-2)!$. For a given value of N, the Galois group can be computed explicitly as the group generated by the two transformations S and T acting on the order N subgroups of $\mathbb{Z}_N \times \mathbb{Z}_N$ as described in subsection 3.1.

3.3 The $\mathfrak{su}(3)$ example

Let us apply the general results to the $\mathfrak{su}(3)$ example. In this case, the result (3.12) gives immediately the congruence subgroup $\Gamma_{\text{Galois}} = \Gamma(3)$, the cardinality of the Galois group, $|G_{\mathfrak{su}(3)}| = 12 = \frac{1}{2}|\mathfrak{S}_4|$, and therefore the Galois group itself is

$$G_{\mathfrak{su}(3)} = \mathfrak{A}_4, \tag{3.14}$$

the alternating group $\mathfrak{A}_4$ of even permutations.

This is confirmed by an explicit computation based on order 3 sublattices of $\mathbb{Z}^2$, which gives the duality diagram of figure 7, that can also be interpreted as the coset graph of $\Gamma_0(3)$. Physically these are four isolated extrema that correspond to one Higgs vacuum and three confining vacua. The permutations $T = (234)$ and $S = (12)(34)$ indeed generate $\mathfrak{A}_4$.

The subgroup structure of $\mathfrak{A}_4$ is presented on the left of figure 8. The subgroups $\mathbb{Z}_2$ are generated by permutations of the form $(ab)(cd)$, and we have added a subscript $1, 2, 3$ to represent the three subgroups of this kind. Similarly, there are four subgroups isomorphic to $\mathbb{Z}_3$ corresponding to four independent three-cycles. Finally, we have the group $\mathbb{Z}_2^2 = \{1, (12)(34), (13)(24), (14)(23)\}$. Using the extremal values of the superpotential, we can compute the characteristic polynomial for the $\mathfrak{su}(3)$ quadruplet

$$P^{\mathfrak{su}(3)}(W) = W^4 - 8E_6 W - 6E_4 W^2 - 3E_4^2. \tag{3.15}$$

As a check, the discriminant

$$D = -2^{24} 3^9 \Delta^2 \tag{3.16}$$

is the square of a modular form, which confirms that $\sqrt{D}$ has no branch cut.
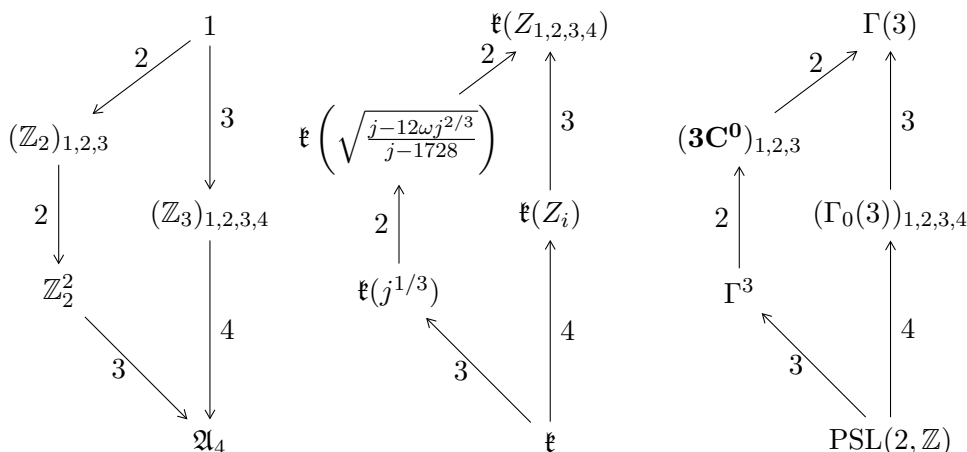
Figure 8. Summary of the Galois correspondence for gauge algebra $\mathfrak{su}(4)$. Here ω is a third root of unity.

The Galois correspondence relates the field extensions generated by polynomials of the roots Z_i to congruence subgroups that contain $\Gamma_{\text{Galois}}(3) = \Gamma(3)$. Those are represented on the right of figure 8, using the notations of [22]. The corresponding fields of modular functions are then engendered by polynomials of the roots left invariant by the associated subgroup of $\mathfrak{A}_4$. For instance, $\mathbb{C}(\mathbf{X}(\Gamma^3))$ is generated by polynomials left invariant by $\mathbb{Z}_2^2$, like

$$(Z_1 - Z_2)(Z_3 - Z_4) + (Z_1 - Z_3)(Z_2 - Z_4) + (Z_1 - Z_4)(Z_3 - Z_2) \sim \frac{j^{2/3}}{j - 1728}. \quad (3.17)$$

The extension of $\mathfrak{k}$ generated by this function is $\mathfrak{k}(j^{1/3})$, and the fact that is has degree three guarantees that it is the right extension. Similarly,

$$Z_1 + Z_2 - Z_3 - Z_4 \sim \sqrt{\frac{j - 12j^{2/3}}{j - 1728}} \quad (3.18)$$

is associated to the group $\mathbb{Z}_2 = \{1, (12)(34)\}$ and to one of the three congruence subgroups in the isomorphism class $\mathbf{3C^0}$.

3.4 The $\mathfrak{su}(4)$ example

The $\mathfrak{su}(4)$ example is the first one where we have two disjoint multiplets, according to property 2 of section 3.1. The cardinality of the Galois group is given by (3.12), $|G_{\mathfrak{su}(4)}| = 24 = [\text{PSL}(2, \mathbb{Z}) : \Gamma(4)]$, and we have $\Gamma_{\text{Galois}}(4) = \Gamma(4)$. In contrast with the situation encountered in the $\mathfrak{su}(3)$ example, the cardinality is not sufficient to determine the Galois group, because there are five conjugacy classes of cardinal 24 groups in $\mathfrak{S}_6$. However, using our correspondence with congruence subgroups, we can extract more information about the subgroups of $G_{\mathfrak{su}(4)}$. In particular, using the facts collected in [22], one can compute the diagram of congruence subgroups between $\text{PSL}(2, \mathbb{Z})$ and $\Gamma(4)$. There are 30 subgroups that can be organized into 11 classes up to conjugation. Moreover, we know from

subsection 3.1 that all the six vacua are permuted by the Galois group. These properties uniquely identify the Galois group,

$$G_{\mathfrak{su}(4)} \cong \mathfrak{S}_4 \,. \tag{3.19}$$

This result can be confirmed using the known duality permutations on massive vacua.

Let us show that the Galois correspondence leads to a complete understanding of the behavior of the vacua under dualities in figure 9. The diagram in figure 9 represents the subgroup structure of the Galois group $\mathfrak{S}_4$, the congruence groups contained between $\Gamma_{\mathrm{Galois}} = \Gamma(4)/\{\pm 1\}$ and $\mathrm{PSL}(2, \mathbb{Z})$, and the associated function field extensions.

For the singlet, the duality group is trivial. The characteristic polynomial $P^{\mathfrak{su}(4)}(W)$ defined in terms of the seven extremal values of the superpotential is equal to

$$P^{\mathfrak{su}(4)}(W) = \left(W^6 - 90E_4W^4 - 540E_6W^3 - 1215E_4^2W^2 - 972E_4E_6W + 108\left(E_4^3 - E_6^2\right)\right)W \,. \tag{3.20}$$

The sextuplet corresponds to the irreducible factor $P^{\mathfrak{su}(4)}(W)/W$.

Our method generalizes to higher rank gauge theories, although the computation complexity grows rapidly. As an illustration, for the smallest N such that $\Gamma_{\mathrm{Galois}}(N) \neq \Gamma(N)$, namely $N = 8$, we obtain one phase characterized by the order 96 Galois group

$$G_{\mathfrak{su}(8)} \cong (\mathbb{Z}_4 \times \mathbb{Z}_4) \rtimes \mathfrak{S}_3 \,. \tag{3.21}$$

4 The $\mathfrak{so}(8)$ theory

In the $\mathfrak{so}(8)$ $\mathcal{N} = 1^*$ theory, more of the power of our framework will come to bare. We will see that in this case, the square root $\sqrt{D}$ of the discriminant of the characteristic polynomial has branch cuts. Relatedly, the field extension lies beyond the theory of modular forms for congruent subgroups. The characteristic polynomial will provide us with a full analytic understanding of the vector valued modular objects described numerically in [13].

In [13], we determined the extrema of the $\mathfrak{so}(8)$ exact effective superpotential. We found twenty different extremal values that split into multiplets of one, three, four and twelve extrema — this last multiplet is called the duodecuplet. The smaller multiplets can be discussed in analogy with previous examples — the monodromy group is generated by the duality group. The duodecuplet however exhibits new features. The extrema in the duodecuplet were determined numerically in [13], and we computed a Fourier expansion for the value of the superpotential at small absolute value of q (amongst various other properties). We use this Fourier expansion to determine the characteristic polynomial with coefficients in the space of modular forms of $\mathrm{PSL}(2, \mathbb{Z})$.

The characteristic polynomial $P^{\mathrm{duod}}(W)$ has degree twelve, and the coefficient of W^k therefore has weight $24 - 2k$. The dimension of the relevant spaces of modular forms, obtained from (2.6), are

Weight	0	2	4	6	8	10	12	14	16	18	20	22	24
Dimension	1	0	1	1	1	1	2	1	2	2	2	2	3

$$\tag{4.1}$$

$\Gamma(4)$

3   2   2

4F⁰ $\Gamma_0(4) \cap \Gamma(2)$

4D⁰   3   2   2   2   2

2   4 $\Gamma(2)$ $\Gamma_0(4)$ **4C⁰**

4A⁰   2   2   2

4   3 $\Gamma_0(2)$

Γ^2

2   3

$\mathrm{PSL}(2,\mathbb{Z})$

c.c. of Γ	# c.c.	c.c. of Group
$\mathrm{PSL}(2,\mathbb{Z})$	1	$\mathfrak{S}_4 = \langle (abcd), (ab) \rangle$
4A⁰	4	$\mathfrak{S}_3 = \langle (abc), (ab) \rangle$
Γ^2	1	$\mathfrak{A}_4 = \langle (abc), (ab)(cd) \rangle$
$\Gamma_0(2)$	3	$D_8 = \langle (abcd), (ac) \rangle$
$\Gamma(2)$	1	$\mathbb{Z}_2^2 = \{1, (ab)(cd), (ac)(bd), (ad)(bc)\}$
$\Gamma_0(4)$	3	$\mathbb{Z}_2^2 = \langle (ab)(cd) \rangle$
4C⁰	3	$\mathbb{Z}_4 = \langle (abcd) \rangle$
4D⁰	4	$\mathbb{Z}_3 = \langle (abc) \rangle$
4F⁰	6	$\mathbb{Z}_2 = \langle (ab) \rangle$
$\Gamma_0(4) \cap \Gamma(2)$	3	$\mathbb{Z}_2 = \langle (ab)(cd) \rangle$
$\Gamma(4)$	1	1

Figure 9. Diagram of subgroups of $\mathfrak{S}_4$, and equivalently of congruence subgroups that contain $\Gamma(4)$. The symbols are defined in the table below, where in each class, we also indicate the number of conjugates. We use the nomenclature of [22] for congruence subgroups.

– 23 –

In [13], we determined more than enough[14] terms in the Fourier q-expansion to identify all these coefficients. The resulting polynomial is

$$
\begin{aligned}
P^{\mathrm{duod}}(W) = {} & W^{12} - 378 E_4 W^{10} - 4632 E_6 W^9 - 12951 E_4^2 W^8 \\
& + 153144 E_4 E_6 W^7 + \left(1172340 E_4^3 + 555708 E_6^2\right) W^6 + 8444160 E_4^2 E_6 W^5 \\
& + \left(5978880 E_4^4 + 18358272 E_4 E_6^2\right) W^4 + \left(26818560 E_4^3 E_6 + 16777216 E_6^3\right) W^3 \\
& \left(9621504 E_4^5 + 37748736 E_4^2 E_6^2\right) W^2 + 28311552 E_4^4 E_6 W + 7077888 E_4^6 \,.
\end{aligned}
\tag{4.2}
$$

For this high degree polynomial, we will perform a monodromy analysis only, without attempting to characterize the field extensions or Galois group entirely. We compute the polynomial $\tilde{P}^{\mathrm{duod}}$ defined in (2.7):

$$
\begin{aligned}
\tilde{P}^{\mathrm{duod}}(Z) = {} & \frac{7077888}{k^6} + \frac{28311552 Z}{k^5} + \frac{36864(1024k + 261)Z^2}{k^5} + \frac{2048(8192k + 13095)Z^3}{k^4} \\
& + \frac{6912(2656k + 865)Z^4}{k^4} + \frac{8444160 Z^5}{k^3} + \frac{12(46309k + 97695)Z^6}{k^3} \\
& + \frac{153144 Z^7}{k^2} - \frac{12951 Z^8}{k^2} - \frac{4632 Z^9}{k} - \frac{378 Z^{10}}{k} + Z^{12} \,,
\end{aligned}
\tag{4.3}
$$

where $k(\tau) = \frac{j(\tau) - 1728}{j(\tau)}$. Then the discriminant of (4.3) is

$$
\begin{aligned}
\tilde{D}^{\mathrm{duod}} = {} & -2^{166} 3^{99} j^{50} (125j - 488095744)^3 \left(14235529 j^3 - 253052536992000 j^2 \right. \\
& \left. - 4425564178752000000 j - 2401900062310400000000\right)^2 (j - 1728)^{-66} .
\end{aligned}
\tag{4.4}
$$

Crucially, we note the presence of the term $(125j - 488095744)^3$ which induces a branch cut in $\sqrt{\tilde{D}^{\mathrm{duod}}}$, thus spoiling the modular properties of the roots of the characteristic polynomials by introducing a point of monodromy inside the fundamental domain. Indeed, the equation

$$
j(\tau) = j_0 := \frac{488095744}{125} .
\tag{4.5}
$$

has exactly one solution in the fundamental domain, namely

$$
\tau_M = i \frac{{}_2F_1\left(\frac{1}{6}, \frac{5}{6}; 1; \frac{1}{2} + \frac{2761}{992\sqrt{31}}\right)}{{}_2F_1\left(\frac{1}{6}, \frac{5}{6}; 1; \frac{1}{2} - \frac{2761}{992\sqrt{31}}\right)} \approx 2.4155769875\ldots i \,.
\tag{4.6}
$$

This analytic result matches the prediction made in [13]. Let us consider more closely the pair $W_i(\tau)$, $W_j(\tau)$ of roots that coincide at $j(\tau) = j_0$. Around the value j_0 we have the behavior $(W_i(q) - W_j(q))^2 \sim (j - j_0)^3$, and then $W_i(q) - W_j(q) \sim (j - j_0)^{3/2}$. Thus when j turns once around j_0, the superpotential extrema W_i and W_j are exchanged, realizing a monodromy of order two in the space of couplings.

The $\mathfrak{so}(8)$ discriminant (4.4) also has a degree three polynomial factor that can vanish. It has one real root and two complex conjugate roots. More precisely, its roots are

$$
j(\tau) = j_k := \mu^k a + \mu^{-k} b + c
\tag{4.7}
$$

---

[14]Each additional coefficient can be considered as a check of the validity of this computation. We have several dozens such checks.
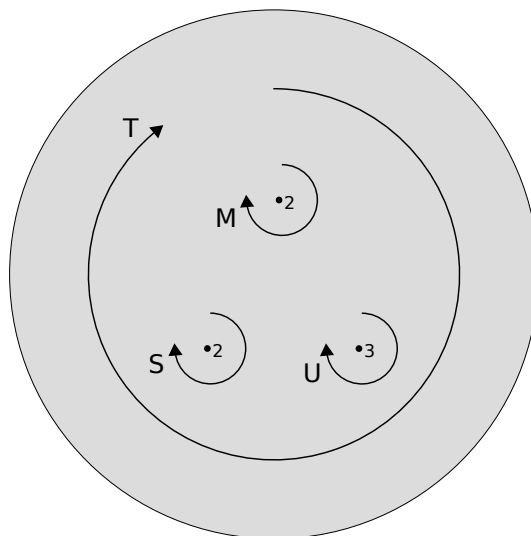
Figure 10. The orbifold $\bar{C}$ for the $\mathcal{N} = 1^*$ theory with gauge algebra $\mathfrak{so}(8)$.

where $\mu = \exp(2\pi i/3)$ and $k = 1, 2, 3$ and a, b and c are the real numbers

$$a = \frac{24000 \sqrt[3]{4360686193219190553684990 4418 - 36140966112133424721 00883\sqrt{229}}}{14235529}$$

$$b = \frac{24000 \sqrt[3]{4360686193219190553684990 4418 + 36140966112133424721 00883\sqrt{229}}}{14235529}$$

$$c = \frac{84350845664000}{14235529} \, .$$

These are order two roots of (4.4), meaning that exactly two superpotentials become equal when $j(\tau) = j_k$. We can write explicit formulas for τ in the fundamental domain that solve (4.7). Numerical estimations of these exact values are:

$$\tau_3 \approx 2.65698i \qquad \tau_{1,2} \approx \pm 0.43207 + 1.47209i \, . \tag{4.8}$$

Around these singular values of τ, the pair of superpotentials that coincide satisfies $W_i(q) - W_j(q) \sim (j - j_k)$, and there is no monodromy around these points. This shows that the numerical analysis performed in [13] was indeed exhaustive in identifying points of monodromy.

We can then describe the space $\bar{C}$ in which the complexified gauge coupling lives as an orbifold with the topology of a disk and three elliptic points of orders two, two and three, as pictured in figure 10. Accordingly the fundamental group is the free product $\pi_1(\bar{C}) = \mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_3$ with generators M, S and U, which contains a $\mathrm{PSL}(2, \mathbb{Z}) = \mathbb{Z}_2 * \mathbb{Z}_3$ group as a subgroup.

In [13], we determined how each generator of $\pi_1(\bar{C})$ is associated to a permutation of the massive vacua, thus giving the explicit realization of the map $\bar{\sigma}$ (1.2). Using those results, we can compute e.g. the order of the Galois group. In the duodecuplet, the basic duality transformations were determined to be the following permutations of the twelve

vacua:[15]

$$\bar{\sigma}(M) = (5,8)$$
$$\bar{\sigma}(S) = (1,2)(3,7)(4,12)(5,8)(6,11)(9,10) \tag{4.9}$$
$$\bar{\sigma}(U) = (1,2,7)(3,12,6)(4,5,11)(8,10,9)\,.$$

The cardinality of the Galois group $G = \langle \bar{\sigma}(M), \bar{\sigma}(S), \bar{\sigma}(U) \rangle$ generated by these permutations is $|G| = 82944$, which uniquely determines the group to be

$$G = \mathfrak{S}_4 \wr \mathfrak{S}_3 \tag{4.10}$$

where $\wr$ denotes the regular wreath product.

We can also introduce the transformation T which refers to the shift of the θ-angle at weak coupling, or equivalently the monodromy around the point $\tau = i\infty$. This transformation should be identified with the product MSU, as represented in figure 10, so that $\bar{\sigma}(T) = \bar{\sigma}(MSU) = (2,3,4,5,6,7)(8,9)(11,12)$. It is clear from the figure, and it can be explicitly checked, that those S and T dualities do not satisfy the defining relation of the modular group, $(ST)^3 \neq 1$, as discussed in [13]. This explains why the appearance of the additional monodromy M spoils irremediably all modular properties in a given vacuum of the duodecuplet with respect to these S and T actions, in contrast with the analysis of section 3 where there was a residual modular covariance. As we mentioned previously, the modular group does appear as a subgroup of $\pi_1(\bar{C})$, although with a different interpretation regarding the complexified coupling constant. For instance, defining $T' = MT = SU$ we have $(ST')^3 = U^3 = 1$. This opens the possibility that the actions of the permutations S and T' be trivial for some congruence subgroup. If this is the case, there exists an integer N such that all the generators of $\Gamma(N)$ are trivial in this representation. Looking at small values of N, we observe that this situation indeed occurs for $N = 8$ (and not below), as can be checked by expressing the 33 generators of $\Gamma(8)$ using the Farey algorithm. It should be kept in mind though that it is the T-transformation that determines the properties of the q-expansion at $\tau = i\infty$.

Conclusion. We understand the modular covariant vectors as roots of a characteristic polynomial with coefficients that are modular forms. This provides an analytic understanding of all the integers appearing in the Fourier decomposition of the extrema generated numerically in [13]. The superpotential values are modular algebraic, i.e. the superpotential values live in non-analytical extensions of the field of weight two modular forms. More generally, observables in duality covariant quantum field theory invoke non-analytic modular vectors that live in extensions of the graded ring of modular forms.

In summary, we have realized the two modular group breaking patterns previewed in our introduction. The next section will serve to illustrate that it is the full breaking pattern that is generic.

---

[15]Here we shift for convenience the labeling numbers of the twelve vacua of the duodecuplet in [13] by minus eight so that they run from 1 to 12.

5 Mass deformed $\mathcal{N} = 2$ superconformal QCD

In this section, we focus on the $\mathfrak{su}(N_c)$, $\mathcal{N} = 2$ theory with $N_f = 2N_c$ massive quarks. Again, we analyze the characteristic polynomial and the permutation group of its roots and its relation to the duality group. We concentrate on the case of two colors. The Seiberg-Witten analysis for this theory was performed in [33] for $N_c = 2$, and in [34] for $N_c > 2$. The integrable system associated to these theories is the XXX spin chain [35]. Moreover, this integrable system is equivalent to the Gaudin integrable system [36].

We break $\mathcal{N} = 2$ supersymmetry to $\mathcal{N} = 1$ by adding a mass term for the chiral multiplets to the Lagrangian. In other words, we add a quadratic superpotential $W(\Phi) = \frac{\mu}{2}\Phi^2$ for the adjoint chiral field Φ. A semi-classical analysis gives the number of massive vacua

$$\sum_{r=0}^{N_c-1} (N_c - r) \binom{2N_c}{r}. \tag{5.1}$$

In the literature, there are few results on matching the semi-classical predictions with the results of analyzing the integrable system description of the quantum effective action. In [37], the theory with $N_c = 2$ was studied using the XXX spin chain prescription and the number of vacua and their semi-classical behavior was reproduced from the integrable system.[16]

Our main interest is in the monodromies of the massive vacua that arise after breaking $\mathcal{N} = 2$ to $\mathcal{N} = 1$ by mass deformation, in the case of the gauge algebra $\mathfrak{su}(2)$. We denote the four $\mathcal{N} = 2$ masses of the fundamental chiral multiplets by $m_{1,2,3,4}$. In this theory, there are generically six massive vacua. Two vacua arise from the confined dynamics in the $\mathfrak{su}(2)$ low-energy theory when the gauge group is unbroken and $\langle\Phi\rangle = 0$, and the four other vacua are Higgs vacua, associated to the four expectation values, $\langle\Phi\rangle \propto m_{1,2,3,4}\mathrm{diag}(1,-1)$. We wish to describe the quantum effective superpotential that captures these six vacua, and the permutation of massive vacua under monodromy.

5.1 The Gaudin integrable system

In order to more easily capture the duality action on the $\mathcal{N} = 1$ massive vacua, it is natural to start from the description of the $\mathcal{N} = 2$ curves adapted to these dualities [38]. These curves in turn are more easily interpreted in terms of the Gaudin integrable system. (See also e.g. [39].) The Gaudin integrable system at hand is a four-punctured two-sphere S with an $\mathfrak{sl}(2)$ valued Hitchin Higgs field Φ. Up to a conformal transformation, the punctures can be located at $z_0 = 0$, $z_1 = 1$, $z_\lambda = \lambda$ and $z_\infty = \infty$. The Seiberg-Witten curve Σ is a double cover of the sphere S with four branch points at the four punctures. The curve Σ is a torus

---

[16]We have studied the XXX spin chain prescription of the massive vacua for $N_c = 3, 4$. The expectation from semi-classics is that the number of vacua is respectively 30 and 140. We found the same number of extremal values of the superpotential through a random numerical search algorithm, run for a number of hours on a desktop computer. The technique follows the analysis in [37], with more variables, and reverting to numerics for determining the zeroes of the resulting high degree polynomials.

Elliptic point of order 2	$\tau \in \mathrm{SL}(2,\mathbb{Z}) \cdot i$	$j = 1728$	$\lambda = -1, \frac{1}{2}, 2$
Elliptic point of order 3	$\tau \in \mathrm{SL}(2,\mathbb{Z}) \cdot e^{2\pi i/3}$	$j = 0$	$\lambda = e^{2\pi i/3}, e^{-2\pi i/3}$
Cusps	$\tau \in \mathrm{SL}(2,\mathbb{Z}) \cdot i\infty = \{i\infty\} \cup \mathbb{Q}$	$j = \infty$	$\lambda = 0, 1, \infty$

Table 1. Cusps and elliptic points.

with modular parameter τ which is related to the cross ratio, or modular λ-function by

$$\lambda(\tau) = 16 e^{\pi i \tau} \prod_{n=1}^{\infty} \left(\frac{1 + e^{2\pi i n \tau}}{1 + e^{2\pi i \tau (n-1/2)}} \right)^8 = \frac{\theta_2^4(\tau)}{\theta_3^4(\tau)}. \tag{5.2}$$

This relation implies that the (infrared) duality transformation $\tau \to -1/\tau$ corresponds to the transformation of the (UV) parameter $\lambda \to 1 - \lambda$, and that the T-duality operation $\tau \to \tau + 1$ corresponds to $\lambda \to \frac{\lambda}{\lambda - 1}$. The cross ratio λ is invariant under $T^2 : \tau \to \tau + 2$. In fact, it is invariant under the subgroup $\Gamma(2) \subset \mathrm{SL}(2, \mathbb{Z})$.

As before, we are interested in the map from the fundamental group of the space of couplings to the permutation group of the six massive vacua. Let us first describe the space of couplings. It can be parametrized by

$$(\lambda, m_i) \in C = (\mathbb{C} - \{0, 1\}) \times (\bar{\mathbb{C}})^4, \tag{5.3}$$

where we have excluded the cusp values $0, 1, \infty$ for the cross ratio λ. See table 1 for a reminder of the cusp and elliptic points and the associated values of the cross ratio. We still have to quotient by the dualities, which provide an equivalence relation:

$$(\lambda, m_{0,1,\lambda,\infty}) \sim (1 - \lambda, m_{1,0,\lambda,\infty}) \sim \left(\frac{1}{\lambda}, m_{0,\lambda,1,\infty} \right). \tag{5.4}$$

The group generated by those dualities is isomorphic to the permutation group $\mathfrak{S}_3$, and it acts on C as indicated above. The parameter space is then the orbifold quotient

$$\bar{C} = C / \mathfrak{S}_3. \tag{5.5}$$

The fundamental group includes generators of infinite order corresponding to looping the coupling around two of the special points $\lambda \in \{0, 1, \infty\}$, as well as generators of order two around the points fixed by a non-trivial element of $\mathfrak{S}_3$.

5.2 The analysis of the integrable system extrema

The Gaudin integrable model has rank one. We can expect the superpotential to be determined in terms of the quadratic Hamiltonians of the Gaudin integrable system. Let's describe the Hamiltonians in some detail. We introduce the Gaudin integrable system through the Higgs field Φ of the Hitchin system

$$\Phi(z) = \sum_{c=0,1,\lambda,\infty} \frac{A^c}{z - z_c}, \tag{5.6}$$

where A^c are $\mathfrak{sl}(2)$ matrices, and the adjoint $\mathfrak{sl}(2)$ action is gauged. We moreover impose the constraint:

$$\sum_c A^c = 0 \,. \tag{5.7}$$

We further demand that these matrices lie on a particular orbit,

$$\operatorname{tr} A_i^2 = m_i^2$$
$$\operatorname{tr} (A_0 + A_1 + A_\lambda)^2 = m_\infty^2 \,. \tag{5.8}$$

Combining these constraints yields

$$\operatorname{tr}(A_0 A_1 + A_1 A_\lambda + A_\lambda A_0) = \frac{1}{2}(m_\infty^2 - m_0^2 - m_1^2 - m_\lambda^2) := M^2 \,. \tag{5.9}$$

The model has five parameters, namely one that defines the geometry of the punctured curve (i.e the gauge coupling) and four (masses) that specify the double pole residues of the quadratic differential ϕ_2 [38]

$$\phi_2 = \operatorname{tr} \left[\Phi(z)^2 \right] \mathrm{d}z^2 \,. \tag{5.10}$$

The quadratic Hamiltonians (which are residues of $\operatorname{tr} \Phi^2$ at the punctures) are, for $c = 0, 1, \lambda$,

$$H_{2,c} = \sum_{d \neq c} \frac{\operatorname{tr}(A^c A^d)}{z_c - z_d} \,. \tag{5.11}$$

We will place the fourth singularity at $z = \infty$. A good coordinates at infinity is $\tilde{z} = \frac{1}{z}$, so that $\mathrm{d}z^2 = \tilde{z}^{-4} \mathrm{d}\tilde{z}^2$, and we have the singularity structure

$$\phi_2 = \frac{m_\infty^2}{\tilde{z}^2} \mathrm{d}\tilde{z}^2 + \frac{H_{2,\infty}}{\tilde{z}} \mathrm{d}\tilde{z}^2 + \text{finite terms} \,, \tag{5.12}$$

with

$$H_{2,\infty} = \sum_{c,d=0,1,\lambda} (z_c + z_d) \operatorname{tr} (A^c A^d) \,. \tag{5.13}$$

While the second order residues at the punctures are specified by our boundary conditions, the first order residues give us four quadratic Hamiltonians (5.11) and (5.13). A crucial point is that extremizing one of them is equivalent to extremizing any other, up to an affine transformation. This leads to the duality covariance of the $\mathcal{N} = 1$ theory. We will concentrate on the three Hamiltonians (5.11) and the duality transformations implemented by exchanging the points $0, 1, \lambda$. The sum of the three Hamiltonians (5.11) is zero. Upon the exchange of the points 0 and 1, we have the interchange of Hamiltonians $H_{2,0} \leftrightarrow H_{2,1}$, and under $1 \leftrightarrow \lambda$ we have $H_{2,\lambda} \leftrightarrow \lambda H_{2,1}$. Under the constraints (5.8), we note the affine relations:

$$H \equiv H_{2,0} = (\lambda - 1)H_{2,\lambda} - M^2 = \frac{1 - \lambda}{\lambda} H_{2,1} - \frac{M^2}{\lambda} \,. \tag{5.14}$$

In appendix C.1, we introduce an explicit parametrization of the Gaudin integrable system, and compute the equations governing the six massive vacua and their superpotential values. We introduce a Lagrange parameter α for the constraint (5.7), and after some calculation (see appendix C.1) the extremization procedure reduces to solving a sixth degree polynomial in this variable, namely

$$\alpha^2 \left((\alpha - 1)^2 \lambda \left(m_\infty^2(\alpha\lambda - 1)^2 + m_1^2(\lambda - 1)\right) - m_\lambda^2(\lambda - 1)(\alpha\lambda - 1)^2\right) \tag{5.15}$$
$$-(\alpha - 1)^2 m_0^2(\alpha\lambda - 1)^2 = 0 \,.$$

We can write down the Hamiltonians at the extrema as a function of α alone. For instance for $H \equiv H_{2,0}$ we find

$$H = \frac{(\alpha - 1)^2 m_0^2(\alpha\lambda - 1)^2(\alpha\lambda + \alpha - 2) - \alpha^3(\lambda - 1)\left(m_\lambda^2(\alpha\lambda - 1)^2 - (\alpha - 1)^2 m_1^2\lambda^2\right)}{2(\alpha - 1)^2\alpha\lambda(\alpha\lambda - 1)^2} \,.$$
$$\tag{5.16}$$

The value of H in each vacuum is a function of λ and the masses $m_{0,1,\lambda,\infty}$ that we call

$$H_i(\lambda, m_{0,1,\lambda,\infty}) = H(\alpha_i(\lambda, m_{0,1,\lambda,\infty}), \lambda, m_{0,1,\lambda,\infty}) \,, \tag{5.17}$$

where the $\alpha_i(\lambda, m_{0,1,\lambda,\infty})$ are the roots of the polynomial (5.15). We can define a characteristic polynomial

$$P_H(H; \lambda, m_{0,1,\lambda,\infty}) = \prod_{i=1}^{6}(H - H_i(\lambda, m_{0,1,\lambda,\infty})) \,. \tag{5.18}$$

The coefficients of this polynomial are invariant under any permutation acting on the index i, so they depend only on the coefficients of the polynomial (5.15) and can be computed without knowing the roots $H_i(\lambda, m_{0,1,\lambda,\infty})$. Details about this computation and the resulting polynomial P_H are presented in appendix C.2. With this polynomial at hand, we can observe the action of various dualities. Firstly, the fact that P_H depends only on the function $\lambda(\tau)$ and not directly on τ shows that the polynomial P_H is invariant under $\Gamma(2)$. Secondly, the polynomial P_H is invariant under transformations such as $\tau \to \tau + 1$ or $\tau \to -1/\tau$ when combined with the appropriate permutation of the masses. More precisely, all dualities are obtained from the two identities:

$$P_H(H; \lambda, m_{0,1,\lambda,\infty}) = \left(\frac{1}{\lambda}\right)^6 P_H\left(\lambda H; \frac{1}{\lambda}, m_{0,\lambda,1,\infty}\right) \,, \tag{5.19}$$
$$= \left(\frac{\lambda - 1}{\lambda}\right)^6 P_H\left(\frac{\lambda H + M^2}{\lambda - 1}; 1 - \lambda, m_{1,0,\lambda,\infty}\right) \,.$$

This shows that knowing a root of the polynomial $P(H; \lambda, m_{0,1,\lambda,\infty})$ is equivalent to knowing the root of the polynomials obtained after duality as illustrated in figure 11. A vacuum is therefore characterized by the six values represented in figure 11, or equivalently by the six symmetric functions $\mathcal{O}_k$ of these values. The sum $\mathcal{O}_1$ evaluates to $-3M^2$ and is independent of λ and H. But the other observables $\mathcal{O}_k$ for $k = 2, 3, 4, 5, 6$ are non-trivial and characterize the vacua entirely. We have for instance

$$\mathcal{O}_2 = \frac{-H^2(\lambda^2 - \lambda + 1)^2 - H\left(\lambda^3 + 1\right)M^2 + (\lambda(3\lambda - 7) + 3)M^4}{(\lambda - 1)^2} \,, \tag{5.20}$$
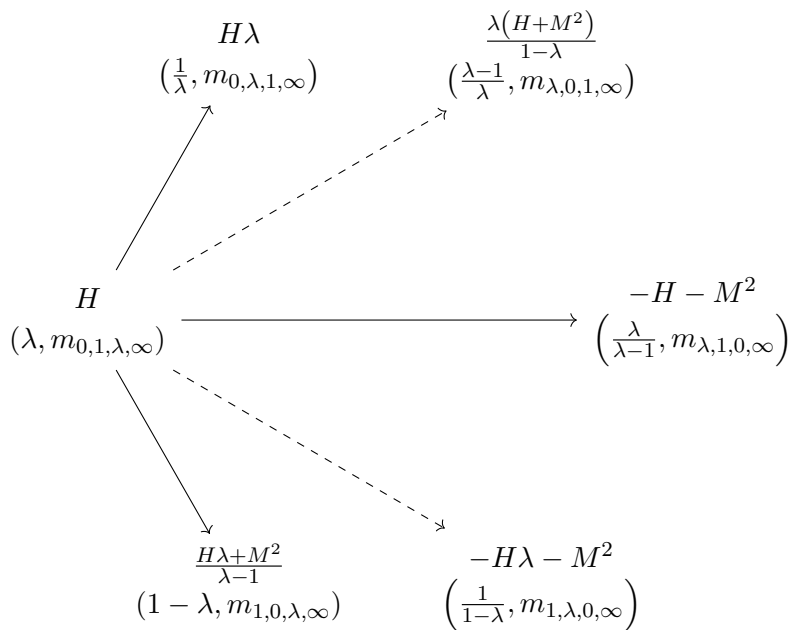
Figure 11. Action of the orbifold group $\mathfrak{S}_3$ on the λ, the masses and the Hamiltonian $H = H_{2,0}$. The plain arrows correspond to the transpositions, also presented in table 2, while the dashed arrows represent the three-cycles. To each fixed point of the $\mathfrak{S}_3$ action on the parameter space is associated a monodromy.

and for generic masses, this operator is generic in the sense of section 1. By construction, the operators $\mathcal{O}_k$ are defined on the space $\bar{C}$, and the dualities can be reformulated in terms of the Galois theory associated to their characteristic polynomials $P_{\mathcal{O}_k}$, which we can compute explicitly from the polynomial P_H (5.18) — see appendix C.2 for the result.

5.3 Dualities and monodromies

Armed with those polynomials, we can read how the six massive vacua transform along loops in $\bar{C}$, and construct the map $\bar{\sigma}$. The fundamental group $\pi_1(\bar{C})$ contains four types of elements:

1. elements associated to the monodromies around the excised points $\lambda = 0, 1, \infty$,

2. elements of order two, associated to the three transpositions in $\mathfrak{S}_3$,

3. elements of order three associated to the two three-cycles of $\mathfrak{S}_3$,

4. cycles around additional points of monodromy, if any.

Since the three-cycles are the products of two transpositions, it is enough to describe the image by $\bar{\sigma}$ of the elements of type 1 and type 2. The relevant data concerning the corresponding fixed points is summarized in table 2. Using the global symmetry of the problem, we note that it is sufficient to focus on one transposition, and to study the

Transposition	Equation	Orbifold fixed point	Excised fixed point
$0 \leftrightarrow 1$	$\lambda = 1 - \lambda$	$\lambda = \frac{1}{2}$	$\lambda = \infty$
$1 \leftrightarrow \lambda$	$\lambda = \frac{1}{\lambda}$	$\lambda = -1$	$\lambda = 1$
$0 \leftrightarrow \lambda$	$\lambda = \frac{\lambda}{\lambda - 1}$	$\lambda = 2$	$\lambda = 0$

Table 2. For each transposition in $\mathfrak{S}_3$, we give the fixed point equation and its two solutions.

permutation of the vacua around the two fixed points in the λ space — one is an orbifold point, the other is one of the excised points, as summarized in the table.

We focus on the third line of the table. Let us consider first the excised fixed point, namely $\lambda = 0$. The fact that this point is not in C is reflected in the fact that the polynomials $P_{\mathcal{O}_2}$ is singular in the limit $\lambda \to 0$. However, we can define the rescaled polynomial $\tilde{P}_{\mathcal{O}_2}(\mathcal{O}_2; \lambda, m_{0,1,\lambda,\infty}) = \lambda^{12} P_{\mathcal{O}_2}(\lambda^{-2}\mathcal{O}_2; \lambda, m_{0,1,\lambda,\infty})$ which is regular in this limit. Plugging in $\lambda = 0$, the polynomial $\tilde{P}_{\mathcal{O}_2}(\mathcal{O}_2; 0, m_{0,1,\lambda,\infty})$ factorizes and the roots can be found analytically. Perturbing those roots, we obtain a small λ expansion for the values of $\mathcal{O}_2$ in the six vacua after scaling back to the original polynomial:

$$(\mathcal{O}_2)_1 = -\frac{m_0^2 m_\lambda^2}{\lambda^2} + \frac{2 m_0^3 m_\lambda^2}{\lambda(m_0 - m_\lambda)} + \dots$$

$$(\mathcal{O}_2)_2 = -\frac{m_0^2 m_\lambda^2}{\lambda^2} + \frac{2 m_0^3 m_\lambda^2}{\lambda(m_0 + m_\lambda)} + \dots$$

$$(\mathcal{O}_2)_3 = -\frac{\left(m_0^2 + m_\lambda^2\right)^2}{4\lambda^2} - \frac{\sqrt{(m_0 - m_\lambda)(m_0 + m_\lambda)}\left(m_0^2 + m_\lambda^2\right)^{3/2}}{\lambda^{3/2}} + \dots$$

$$(\mathcal{O}_2)_4 = -\frac{\left(m_0^2 + m_\lambda^2\right)^2}{4\lambda^2} + \frac{\sqrt{(m_0 - m_\lambda)(m_0 + m_\lambda)}\left(m_0^2 + m_\lambda^2\right)^{3/2}}{\lambda^{3/2}} + \dots$$

$$(\mathcal{O}_2)_5 = \frac{-2\sqrt{m_1^6\left(m_0^2 + m_1^2 + m_\lambda^2\right)} - m_1^2\left(m_0^2 + 2m_1^2 + m_\lambda^2\right)}{\lambda^2} \tag{5.21}$$
$$+ \frac{2\left(m_0^2 m_1^2 + \sqrt{m_1^6\left(m_0^2 + m_1^2 + m_\lambda^2\right)} + m_1^4\right)}{\lambda} + \dots$$

$$(\mathcal{O}_2)_6 = \frac{2\sqrt{m_1^6\left(m_0^2 + m_1^2 + m_\lambda^2\right)} - m_1^2\left(m_0^2 + 2m_1^2 + m_\lambda^2\right)}{\lambda^2}$$
$$+ \frac{2\left(m_0^2 m_1^2 - \sqrt{m_1^6\left(m_0^2 + m_1^2 + m_\lambda^2\right)} + m_1^4\right)}{\lambda} + \dots$$

We can deduce from these expressions that the vacua labeled by 3 and 4 are exchanged under $\lambda \mapsto \frac{\lambda}{\lambda - 1}$, $m_0 \leftrightarrow m_\lambda$ while the others are left invariant.

We now consider the order two permutation around the orbifold point $\lambda = 2$. In order to be at a fixed point of the orbifold action, we also need to impose $m_0 = m_\lambda$. Plugging in those values in the characteristic polynomials for the invariant operators, we find that they factorize as

$$P_{\mathcal{O}_k}(\mathcal{O}_k) = \left(Q_k(\mathcal{O}_k)\right)^2, \tag{5.22}$$

where Q_k is a degree three polynomial, whose roots are distinct for generic masses. As a consequence, the image by the map $\bar{\sigma}$ of this orbifold cycle is an element of $\mathfrak{S}_2 \times \mathfrak{S}_2 \times \mathfrak{S}_2$. One can show, using either numerical computations or exact perturbation theory, that the element is a product of three transpositions.

Finally, we turn to possible additional points of monodromy. Let us first consider a simple and interesting situation in which $M = 0$ and $m_0 = m_1 = m_\lambda \equiv m$. We then find the discriminant

$$
\begin{aligned}
\operatorname{disc} P_{\mathcal{O}_2} &= -\frac{282429536481}{4(\lambda-1)^{52}\lambda^{52}}(\lambda-2)^6(\lambda+1)^6(2\lambda-1)^6\left(\lambda^2-\lambda+1\right)^{60} \\
&\quad \times \left(\lambda^6 - 3\lambda^5 + 60\lambda^4 - 115\lambda^3 + 60\lambda^2 - 3\lambda + 1\right)^3 m^{120} \\
&= -3^{24}2^{-204}m^{120}j^{20}(j-1728)^3(j+13824)^3 .
\end{aligned}
\tag{5.23}
$$

We used the relation between the λ function and the j invariant,

$$
j(\tau) = \frac{256\left(\lambda^2 - \lambda + 1\right)^3}{(1-\lambda)^2\lambda^2} .
\tag{5.24}
$$

Because we concentrated on the mass configuration $m_0 = m_1 = m_\lambda$, the discriminant (5.23) vanishes at the elliptic points and diverges at the cusps, see table 1. The discriminant also has additional zeros. They correspond to a complexified coupling constant τ that satisfies $j(\tau) = -13824$.[17] Let us concentrate on the additional root

$$
\lambda_M = \frac{1}{2}\left(1 - i\sqrt{3\left(25 + 20\sqrt[3]{2} + 16\,2^{2/3}\right)}\right) .
\tag{5.25}
$$

Plugging this value into the polynomial $P_{\mathcal{O}_2}$, we find a double root $\mathcal{O}_2 = 27m^4$, and we can then compute the evolution of these two roots for $\lambda \neq \lambda_M$ perturbatively,

$$
m^{-4}\mathcal{O}_2 = 27 + 45i\sqrt{6\left(12 - 7\sqrt[3]{2} - 2\,2^{2/3}\right)}(\lambda - \lambda_M)
\tag{5.26}
$$

$$
\pm 12i\sqrt[4]{-4539 + 4986\sqrt[3]{2} - 1098\,2^{2/3}}(\lambda - \lambda_M)^{3/2} + O((\lambda - \lambda_M)^2) .
\tag{5.27}
$$

The non-zero coefficient in front of $(\lambda - \lambda_M)^{3/2}$ proves that the two vacua are exchanged when λ circles once around the additional point of monodromy λ_M. In this very symmetric configuration we have thus been able to demonstrate the existence of additional points of monodromy. Because of their topological character, these points must survive when going away from this symmetric configuration. We deduce that the phenomenon of additional monodromies is generic. This conclusion is confirmed by numerical computations.

As a final remark, let us note that we can also connect the quantum behavior of massive vacua to our semi-classical intuition. The monodromy around the point $\lambda = 0$ can be interpreted as T-duality. The expansions (5.21) prove that two vacua admit an expansion in $\lambda^{1/2}$, and can be identified with the two confining vacua, while the four other have an expansion in integer powers of λ and are the Higgs vacua.

---

[17]We note that $1728 = 12^3$ and $13824 = 24^3$.

Conclusions. We conclude that the SU(2) $N_f = 4$ theory with $\mathcal{N} = 1$ supersymmetric mass deformation has a Galois group that includes monodromies that do not descend from $\mathcal{N} = 2$ dualities, and that the superpotential expectation values fully break the duality group. While the duality covariance of the $\mathcal{N} = 2$ theory governs the coefficients of the characteristic polynomials, the choice of massive $\mathcal{N} = 1$ vacuum breaks duality. After mass deformation, it is the Galois permutation group that classifies quantum vacua connected by interpolation in the coupling space.

6 Closing section

The vacuum and chiral ring structure of $\mathcal{N} = 1$ theories is a rich subject. The mere enumeration of the massive vacua gives rise to intriguingly rich counting problems. In this paper, we determined the permutation of massive vacua under completing a loop in the space of couplings. This quest lead us into the Galois theory of field extensions. In the case of the $\mathcal{N} = 1$ theories that inherit duality covariance properties from their $\mathcal{N} = 2$ parents, we argued that the Galois group takes over the role of the duality group in classifying multiplets of massive vacua.

It is clear that many open problems remain. It would be interesting to promote our results on the permutations of vacua into a study of the full Berry connection associated to $\mathcal{N} = 1$ vacuum states. Tackling the problem of determining the full chiral ring vacuum expectation values in some low rank examples with duality covariance, in the spirit of [6, 7], should be worthwhile. An efficient derivation of the characteristic polynomials from scratch would also be most welcome. In short, if we promote our generic grasp of the physics of $\mathcal{N} = 1$ theories to a much more detailed understanding of an ever larger class of theories, we are bound to unearth more beautiful treasures.

A Congruence subgroups, automorphic forms and Galois theory

In this appendix, we first collect useful facts about congruence subgroups and the associated fields of functions, which are the basic ingredients of the Galois correspondence. We also explain how these fields are related to the graded ring of modular forms, using the encompassing concept of automorphic form.

A.1 Congruence subgroups

A subgroup of $\mathrm{SL}(2,\mathbb{Z})$ is called a congruence subgroup if there exists an integer $N \geq 1$ such that it contains the group

$$\Gamma(N) := \left\{ \begin{pmatrix} a\ b \\ c\ d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) | b \equiv c \equiv 0 \text{ and } a \equiv d \equiv 1 \bmod N \right\}. \tag{A.1}$$

Common congruence subgroups are

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a\ b \\ c\ d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) | c \equiv 0 \bmod N \right\}, \tag{A.2}$$

and

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a\ b \\ c\ d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) | c \equiv 0 \text{ and } a \equiv d \equiv 1 \bmod N \right\}. \tag{A.3}$$

We give the inclusion structure of these groups and the associated indices in figure 12. In particular, the index of $\Gamma(N)$ is

$$[\mathrm{PSL}(2,\mathbb{Z}), \Gamma(N)] = \begin{cases} \frac{N^2}{2}\phi(N) \prod\limits_{p|N} \left(1 + \frac{1}{p}\right) & \text{for } N > 2 \\ 6 & \text{for } N = 2, \end{cases} \tag{A.4}$$

where ϕ is the Euler totient function. A useful relation is, for all $N \geq 2$,

$$[\mathrm{SL}(2,\mathbb{Z}), \Gamma(N)] = |\mathrm{SL}(2,\mathbb{Z}_N)| = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right) = N^2 \phi(N) \prod_{p|N} \left(1 + \frac{1}{p}\right). \tag{A.5}$$

A.2 Galois correspondence

Now that we have described the classical congruence subgroup and their inclusions, we recall how to attach a field to each of them and describe those fields explicitly. All of this is summarized in figure 13.

From any congruence subgroup Γ we can construct a compact Riemann surface, called the *modular curve* $\mathbf{X}(\Gamma)$, which is a compactification [23, 24] of $\Gamma \backslash \mathfrak{H}$. We denote by $\mathbb{C}(\mathbf{X}(\Gamma))$ the field of meromorphic functions on this curve. If the genus of $\mathbf{X}(\Gamma)$ is zero, then the field can be generated by a single function (sometimes called the Hauptmodul), and otherwise more generators are needed.[18]

Let us describe these fields for the classical congruence subgroups introduced in the previous subsection. For $(a,b) \in \mathbb{Z}_N^2 - \{(0,0)\}$, we define the functions

$$\mathbf{f}_N^{a,b}(\tau) = \frac{E_4(\tau)}{E_6(\tau)} \wp\left(\frac{a\tau + b}{N}; \tau\right). \tag{A.6}$$

---

[18]In fact, two generators always suffice, but the fields can be more easily described using more generators, as we do here for $\mathbb{C}(\mathbf{X}(\Gamma(N)))$.
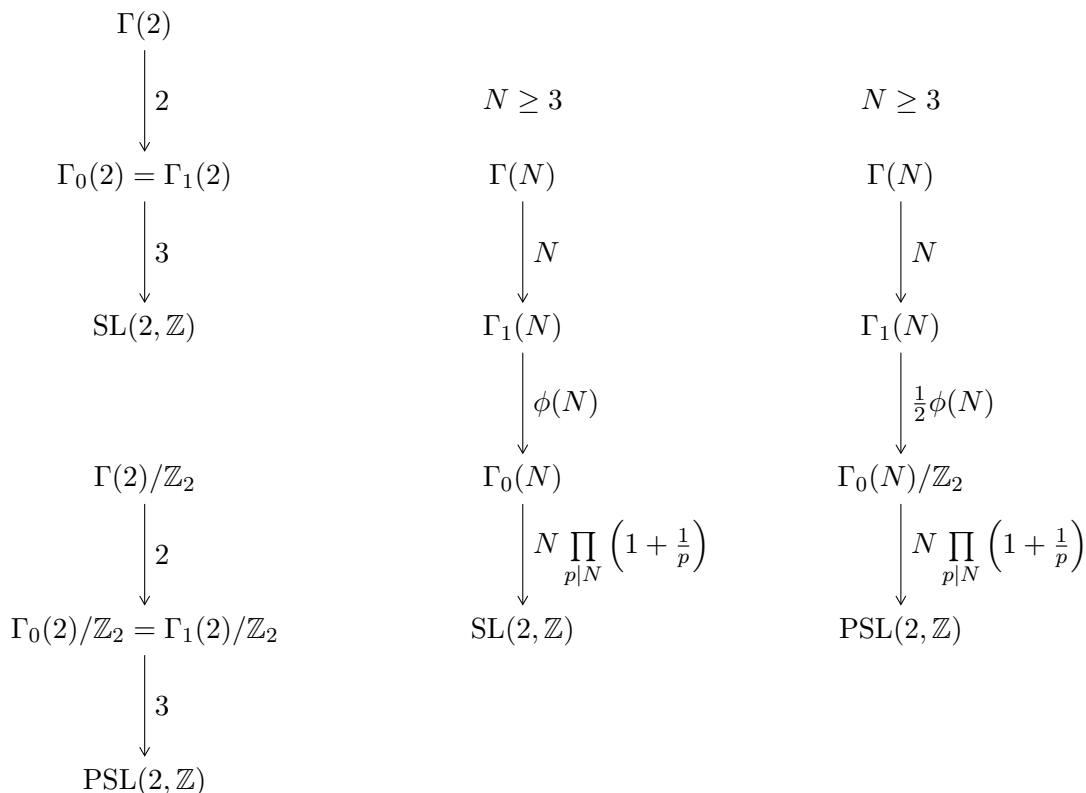
$$
\begin{array}{ccc}
\Gamma(2) & & \\
\Big\downarrow 2 & N \geq 3 & N \geq 3 \\
\Gamma_0(2) = \Gamma_1(2) & \Gamma(N) & \Gamma(N) \\
\Big\downarrow 3 & \Big\downarrow N & \Big\downarrow N \\
\mathrm{SL}(2,\mathbb{Z}) & \Gamma_1(N) & \Gamma_1(N) \\
 & \Big\downarrow \phi(N) & \Big\downarrow \tfrac{1}{2}\phi(N) \\
\Gamma(2)/\mathbb{Z}_2 & \Gamma_0(N) & \Gamma_0(N)/\mathbb{Z}_2 \\
\Big\downarrow 2 & \Big\downarrow N\prod_{p|N}\left(1+\tfrac{1}{p}\right) & \Big\downarrow N\prod_{p|N}\left(1+\tfrac{1}{p}\right) \\
\Gamma_0(2)/\mathbb{Z}_2 = \Gamma_1(2)/\mathbb{Z}_2 & \mathrm{SL}(2,\mathbb{Z}) & \mathrm{PSL}(2,\mathbb{Z}) \\
\Big\downarrow 3 & & \\
\mathrm{PSL}(2,\mathbb{Z}) & &
\end{array}
$$

Figure 12. Some congruence subgroups of level N with the indices of the group inclusions. On the right are congruence subgroups of $\mathrm{PSL}(2,\mathbb{Z})$ of level N.

These are $\frac{1}{2}(N^2 - 1)$ (for $N \geq 3$, and three for $N = 2$) distinct functions that satisfy $\mathbf{f}_N^{a,b} = \mathbf{f}_N^{-a,-b}$, and the dualities act via $T : \mathbf{f}_N^{a,b} \to \mathbf{f}_N^{a,a+b}$ and $S : \mathbf{f}_N^{a,b} \to \mathbf{f}_N^{-b,a}$. Define also

$$
j_N(\tau) = j(N\tau). \tag{A.7}
$$

We then have [23]

$$
\mathbb{C}(\mathbf{X}(\Gamma_0(N))) = \mathbb{C}(j, j_N) \tag{A.8}
$$

$$
\mathbb{C}(\mathbf{X}(\Gamma_1(N))) = \mathbb{C}(j, \mathbf{f}_N^{1,0}) \tag{A.9}
$$

$$
\mathbb{C}(\mathbf{X}(\Gamma(N))) = \mathbb{C}(j, \mathbf{f}_N^{1,0}, \mathbf{f}_N^{0,1}). \tag{A.10}
$$

The fields of meromorphic functions on the modular curves $\mathbf{X}(\Gamma)$ are fairly well understood. In order to translate this knowledge into information about modular forms, we introduce the unifying concept of automorphic form. A function $f : \mathfrak{H} \to \hat{\mathbb{C}}$ is an automorphic form of weight k for Γ, which we denote by $f \in \mathcal{A}_k(\Gamma)$, if

1. f is meromorphic on $\mathfrak{H}$ and at the cusps

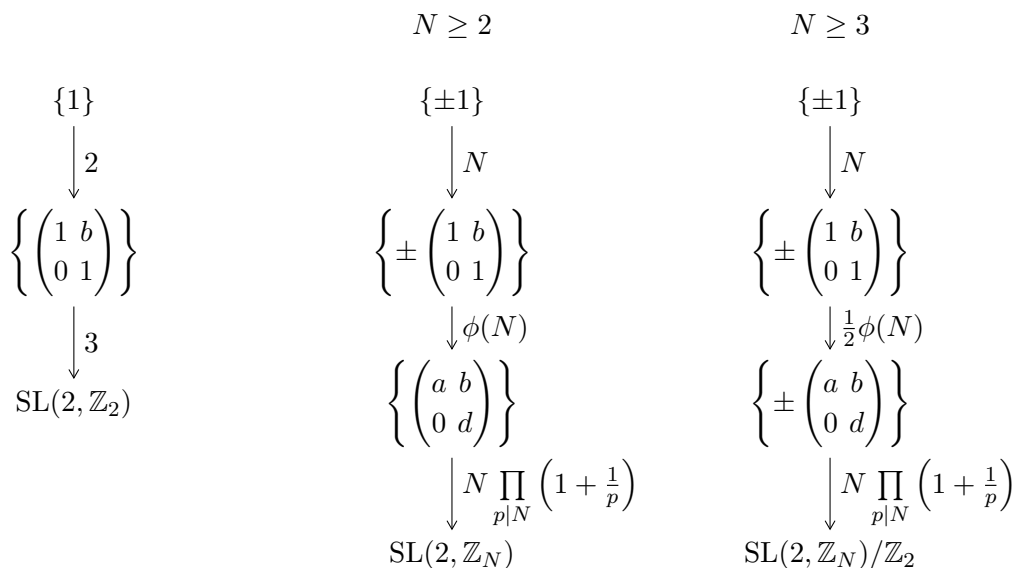2. f is weight-k invariant under Γ.

Figure 13. Galois Groups associated to the congruence subgroups of figure 12. The group denoted $\{\pm 1\}$ at the top is the trivial group (of cardinality 1) inside $\mathrm{SL}(2, \mathbb{Z}_N)/\mathbb{Z}_2$. The letters a, b, d denote generic elements in $\mathbb{Z}_N$, and all matrices have unit determinant.

Note that $f \in \mathcal{A}_k(\Gamma)$ is well defined on $\mathbf{X}(\Gamma)$ when $k = 0$, but not when $k \neq 0$ unless $f = 0$. The fundamental property is

$$\forall f \in \mathcal{A}_k(\Gamma) - \{0\}, \qquad \mathcal{A}_k(\Gamma) = \mathbb{C}(\mathbf{X}(\Gamma)) f \,. \tag{A.11}$$

Thus knowing $\mathcal{A}_0(\Gamma) = \mathbb{C}(\mathbf{X}(\Gamma))$ and a non-trivial element of $\mathcal{A}_k(\Gamma)$ gives a full description of $\mathcal{A}_k(\Gamma)$. We recall that if $k \geq 0$ is even, then

$$(E_6/E_4)^{k/2} \in \mathcal{A}_k(\Gamma) - \{0\} \,, \tag{A.12}$$

The modular forms $\mathcal{M}_k(\Gamma)$ are those automorphic forms that are holomorphic on $\mathfrak{H}$ and at the cusps. Applying the Riemann-Roch theorem, one can deduce that this regularity condition restricts $\mathcal{A}_k(\Gamma)$ to a finite-dimensional subspace whose dimension is given by the formula quoted in (2.13).

B   Properties of $\mathcal{N} = 4$ $\mathfrak{su}(N)$ theories

We collect in this appendix two related analyses. The first is an analysis of the space of $\mathcal{N} = 4$ super Yang-Mills theories with $\mathfrak{su}(N)$ gauge algebra. The second part contains proofs of properties of lattices.

B.1   The $\mathcal{N} = 4$ theories with $\mathfrak{su}(N)$ gauge algebra

The authors of [19] have shown that the number of different $\mathcal{N} = 4$ theories with gauge algebra $\mathfrak{su}(N)$ is given by $\sigma_1(N)$, since we have to make a choice of center $\mathbb{Z}_d \in \mathbb{Z}_N$ of the gauge group, and one among d possible tilts in the spectrum of dyonic line operators. The

structure of the set of $\mathfrak{su}(N)$ $\mathcal{N} = 4$ (and $\mathcal{N} = 1^*$) theories is therefore in bijection with the lattices (3.1), which are in this context interpreted as the electric and magnetic charges of line operators of the theory.

The space of parameters for a theory of level d is $\Gamma_0(N/d^2)\backslash\mathfrak{H}$. Indeed, a given theory, characterized by a lattice $L_{N,p,k}$, is left invariant under a group of the form $\alpha^{-1}\Gamma_0(N/d^2)\alpha$, which is isomorphic to $\Gamma_0(N/d^2)$. For instance, the $SU(N)$ theory is associated with the lattice $L_{N,1,0}$ which is left invariant by $\Gamma_0(N)$.[19] If N is square-free, then all lattices have level one, and we recover the results of [19].

Note however that for the local physics we describe in the rest of the paper, the global aspects we discussed in this appendix will play second fiddle, and we may then simply refer to $\mathrm{PSL}(2,\mathbb{Z})$ as the duality group.

B.2 Proofs of the properties of section 3.1

We prove the three properties stated in section 3.1 that are useful in appendix B.1 as well. We keep the convention that when p is a divisor of N, we set $q = \frac{N}{p}$.

1. For a divisor p of N, consider the p lattices $L_{N,p,k}$, with $k \in \mathbb{Z}_p$. The action of T on this set of lattices is $k \mapsto k + q$, so the size of an orbit is the smallest positive solution of $xq \equiv 0$ modulo p. This solution satisfies $xq = \mathrm{lcm}\,(p, q)$, so the orbit has length $p/\gcd\,(p, q)$. Since all orbits in $\mathbb{Z}_p$ have the same length, we conclude there are $\gcd\,(p, q)$ of them.

2. We prove the two implications separately.

   - Firstly, let us prove that the level is preserved by any duality operation. We remark that the level of a lattice is equal to the greatest common divisor of the coordinates of all the points in the lattice. Indeed, since d divides p, k and q in (3.1), it divides all the coordinates, and reciprocally a divisor of all the coordinates will divide the coordinates of the points $(p, 0)$ and (k, q). Now let $L_{N,p,k}$ be a lattice of level d. Left multiplication by a matrix with integer coefficients can not decrease the level. If the matrix is in $\mathrm{SL}(2, \mathbb{Z})$, the operation is invertible, hence the level is preserved.

   - Now we prove that conversely, if two lattices have the same level, they are related by a duality. Without loss of generality, we can focus on lattices of level 1, dividing if necessary by the level of the initial lattice. Let us then consider $L_{N,p,k}$ with $\gcd\,(p, q, k) = 1$. Under this assumption, there exists an integer[20] l such that $\gcd\,(p, ql + k) = 1$. This means that $T^l L_{N,p,k} = L_{N,p,k'}$ with $\gcd(p, k') = 1$.

---

[19]The associated lattice $L_{N,1,0}$ contains points of the form $(r, 0)$ for $r \in \mathbb{Z}_N$, and therefore acting with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ gives $(ar, cr) = (r', 0)$ with $r' \in \mathbb{Z}_N$ since necessarily $\gcd(a, N) = 1$. The proof of the statement given in [19] is based on the incorrect assumption that the group $\Gamma_0(N)$ is generated by T and $ST^N S$. The statement, however, is correct.

[20]One such integer l can be constructed explicitly along the lines of the proof of Lemma B.1 in [18], as the product of all prime numbers that divide p but that don't divide k nor q.

Taking the S-dual of this lattice, one obtains $ST^l L_{N,p,k} = L_{N,N,k''}$ for some integer k'', and finally $ST^{-k''} ST^l L_{N,p,k} = L_{N,1,0}$. We have proven that any lattice of level 1 is related by a sequence of dualities to $L_{N,1,0}$, so any two such lattices are related by a duality sequence as well.

3. Again we focus on lattices of level 1. Let $L_{N,p,k}$ be such a lattice. According to the previous paragraph, it can be related by a chain of dualities to $L_{N,1,0}$. Let us denote α the corresponding SL$(2, \mathbb{Z})$ matrix, so that $L_{N,1,0} = \alpha L_{N,p,k}$. The lattice $L_{N,1,0}$ is left invariant by $\Gamma_0(N)$, so $L_{N,p,k}$ is left invariant by $\alpha^{-1} \Gamma_0(N) \alpha$.

C   Appendices to section 5

We gather a number of technical results relevant to section 5.

C.1   The parametrization of the Gaudin model

In this subsection, we provide a few technical details of the analysis of the Gaudin integrable system extrema exploited in section 5.2. Firstly, we parameterize the $\mathfrak{sl}(2)$ valued matrices A_i $(i = 0, 1, \lambda)$ using complex numbers a_i, c_i as follows

$$A_i = \frac{m_i}{\sqrt{2}} \begin{pmatrix} 2a_i c_i + 1 & 2c_i(a_i c_i + 1) \\ -2a_i & -2a_i c_i - 1 \end{pmatrix}. \tag{C.1}$$

The conditions $Tr A_i = 0$ and $Tr A_i^2 = m_i^2$ are then automatically enforced. The constraint $\sum_c A_c = 0$ fixes the matrix A_∞. We exploit the gauge freedom of conjugating all three remaining matrices by SL$(2, C)$ which is of dimension three. Firstly, we can use conjugation to diagonalize A_λ, which amounts to setting $c_\lambda = a_\lambda = 0$. We can then still conjugate by a diagonal matrix and put A_1 in the form

$$\begin{pmatrix} 2b + 1 & 2b(b + 1) \\ -2 & -2b - 1 \end{pmatrix}, \tag{C.2}$$

where $a_1 = 1$ and $c_1 = b$. To simplify notation further, we also set $a_0 = a$, $c_0 = c$. We then define a functional W_0 to be extremized, with a Lagrange multiplier α that imposes the last constraint

$$W_0(a, b, c, \alpha) = H_{2,0} + \alpha \left(\sum_{k<j} Tr(A_k A_j) - M^2 \right). \tag{C.3}$$

The explicit expression reads

$$\frac{\lambda}{m^2} W_0 = -2a \left(c(-2b\alpha\lambda + 2b\lambda - 2\alpha\lambda + \lambda + 1) + b(b+1)(\alpha - 1)\lambda + c^2(\alpha - 1)\lambda \right)$$
$$+ \lambda(4b\alpha - 2b - 2c\alpha + 2c + 4\alpha - 1) - 1. \tag{C.4}$$

We extremize this system with respect to a, b, c and α and after elimination obtain a sixth order polynomial in α that governs the positions of the extrema. The extremal values are then given by evaluating the potential W_0 in equation (C.3) at the roots of the sixth order polynomial. The final equations are recorded in section 5.2.

C.2 Explicit polynomials

In section 5.2, in order to construct the polynomials P_H and $P_{\mathcal{O}_k}$ we face the problem of finding a polynomial Q whose roots are the images by some function f of the roots of another polynomial $P = \prod_i (X - \alpha_i)$. If the function f is a ratio of polynomials in α, $f(\alpha) = \frac{f_{\mathrm{num}}(\alpha)}{f_{\mathrm{den}}(\alpha)}$, this problem can be solved without knowing explicitly the roots α_i. Indeed, we can consider

$$Q(X) = \prod_i \left(f_{\mathrm{den}}(\alpha) X - f_{\mathrm{num}}(\alpha) \right) \tag{C.5}$$

whose coefficients are symmetric polynomials of the α_i. Using a reduction algorithm for symmetric polynomials, these coefficients can be expressed in terms of the elementary symmetric functions in the α_i, which in turn can be identified up to a sign to the coefficients of the polynomial P.

We catalogue below explicit expressions for the polynomials that feature in section 5.2, obtained using this algorithm. Although we can compute the polynomials in full generality, for simplicity we provide them here only in the situation where the masses satisfy the constraint $M = 0$, or equivalently $m_\infty^2 = m_0^2 + m_1^2 + m_\lambda^2$.

The characteristic polynomial for H is

$$P_H(H; \lambda, m_{0,1,\lambda}) = H^6 + \sum_{j=0}^{5} r_j(\lambda, m_{0,1,\lambda}) H^j \tag{C.6}$$

where the functions $r_j(\lambda, m_{0,1,\lambda,\infty})$ are

$$
\begin{aligned}
r_0 =\ & \frac{m_0^2 m_1^2 m_\lambda^2}{4\lambda^6} \Big(3(\lambda-1)^4 m_1^4 \left(\lambda^2 m_0^2 + m_\lambda^2 \right) + \left(\lambda^2 m_0^2 + m_\lambda^2 \right)^3 \\
& + 3(\lambda-1)^2 m_1^2 \left(\lambda^4 m_0^4 - 7\lambda^2 m_0^2 m_\lambda^2 + m_\lambda^4 \right) + (\lambda-1)^6 m_1^6 \Big) \\
r_1 =\ & -\frac{3 m_0^2 m_1^2 m_\lambda^2}{2\lambda^5} \left(\lambda^2 m_0^2 + (\lambda-1)^2 m_1^2 + m_\lambda^2 \right) \\
& \times \left((\lambda-2)\lambda^2 m_0^2 + (\lambda-1)^2(\lambda+1) m_1^2 + (1-2\lambda) m_\lambda^2 \right) \\
r_2 =\ & -\frac{1}{4\lambda^4} \Big(\lambda^4 m_0^6 \left(m_1^2 + m_\lambda^2 \right) - \lambda^2 m_0^4 \left(-2(\lambda-1)^2 m_1^4 + \left(9\lambda^2 - 26\lambda + 26 \right) m_1^2 m_\lambda^2 - 2 m_\lambda^4 \right) \\
& + m_0^2 \left((\lambda-1)^4 m_1^6 - (\lambda-1)^2 \left(9\lambda^2 + 8\lambda + 9 \right) m_1^4 m_\lambda^2 + \left(-26\lambda^2 + 26\lambda - 9 \right) m_1^2 m_\lambda^4 + m_\lambda^6 \right) \\
& + m_1^2 m_\lambda^2 \left((\lambda-1)^2 m_1^2 + m_\lambda^2 \right)^2 \Big) \\
r_3 =\ & \frac{1}{2\lambda^3} \Big(\lambda^2 m_0^4 \left((2\lambda-5) m_1^2 + (3\lambda-5) m_\lambda^2 \right) \\
& + m_0^2 \left((\lambda-1)^2(2\lambda+3) m_1^4 + \left(2\lambda^3 - 3\lambda^2 - 3\lambda + 2 \right) m_1^2 m_\lambda^2 + (3-5\lambda) m_\lambda^4 \right) \\
& + m_1^2 m_\lambda^2 \left((\lambda-1)^2(3\lambda+2) m_1^2 + (2-5\lambda) m_\lambda^2 \right) \Big) \\
r_4 =\ & \frac{1}{4\lambda^2} \Big(\lambda^2 m_0^4 - 2 m_0^2 \left(\left(\lambda^2 - \lambda + 6 \right) m_1^2 + \left(6\lambda^2 - 11\lambda + 6 \right) m_\lambda^2 \right) + (\lambda-1)^2 m_1^4 \\
& - 2 \left(6\lambda^2 - \lambda + 1 \right) m_1^2 m_\lambda^2 + m_\lambda^4 \Big) \\
r_5 =\ & \frac{1}{\lambda} \left(-(\lambda-2) m_0^2 - (\lambda+1) m_1^2 + (2\lambda-1) m_\lambda^2 \right) .
\end{aligned}
$$

The characteristic polynomial for $\mathcal{O}_2$ is

$$P_{\mathcal{O}_2}(\mathcal{O}_2; \lambda, m_{0,1,\lambda}) = \mathcal{O}_2^6 + \sum_{j=0}^{5} s_j(\lambda, m_{0,1,\lambda})\mathcal{O}_2^j \tag{C.7}$$

where

$$
\begin{aligned}
s_0 =\ & \frac{(\lambda^2 - \lambda + 1)^{12} m_p^4 m_1^4 m_\lambda^4}{16(\lambda-1)^{12}\lambda^{12}}\Big(3(\lambda-1)^4 m_1^4\left(\lambda^2 m_p^2 + m_\lambda^2\right) + \left(\lambda^2 m_p^2 + m_\lambda^2\right)^3 \\
& + 3(\lambda-1)^2 m_1^2\left(\lambda^4 m_p^4 - 7\lambda^2 m_p^2 m_\lambda^2 + m_\lambda^4\right) + (\lambda-1)^6 m_1^6\Big)^2
\end{aligned}
$$

$$
\begin{aligned}
s_1 =\ & \frac{\left(\lambda^2 - \lambda + 1\right)^{10} m_p^2 m_1^2 m_\lambda^2}{8(\lambda-1)^{10}\lambda^{10}}\Big(18 m_p^2 m_1^2 m_\lambda^2\left((\lambda-2)\lambda^4 m_p^4\right. \\
& -(\lambda-1)^2 m_1^2\left((1-2\lambda)\lambda^2 m_p^2 + (\lambda-2)m_\lambda^2\right) \\
& -\lambda^2(\lambda+1)m_p^2 m_\lambda^2 + (\lambda-1)^4(\lambda+1)m_1^4 + (1-2\lambda)m_\lambda^4\big)^2 \\
& + \Big(3(\lambda-1)^4 m_1^4\left(\lambda^2 m_p^2 + m_\lambda^2\right) + \left(\lambda^2 m_p^2 + m_\lambda^2\right)^3 \\
& + 3(\lambda-1)^2 m_1^2\left(\lambda^4 m_p^4 - 7\lambda^2 m_p^2 m_\lambda^2 + m_\lambda^4\right) \\
& + (\lambda-1)^6 m_1^6\Big)\Big((\lambda-1)^4 m_1^6\left(m_p^2 + m_\lambda^2\right) + m_p^2 m_\lambda^2\left(\lambda^2 m_p^2 + m_\lambda^2\right)^2 \\
& + (\lambda-1)^2 m_1^4\left(2\lambda^2 m_p^4 - \left(9\lambda^2 + 8\lambda + 9\right)m_p^2 m_\lambda^2 + 2m_\lambda^4\right) + m_1^2\left(\lambda^4 m_p^6\right. \\
& + \lambda^2\left(-9\lambda^2 + 26\lambda - 26\right)m_p^4 m_\lambda^2 + \left(-26\lambda^2 + 26\lambda - 9\right)m_p^2 m_\lambda^4 + m_\lambda^6\big)\Big)\Big)
\end{aligned}
$$

$$
\begin{aligned}
s_2 =\ & \frac{\left(\lambda^2 - \lambda + 1\right)^8}{16(\lambda-1)^8\lambda^8}\Big(24 m_p^2 m_1^2 m_\lambda^2\left((\lambda-2)\lambda^4 m_p^4 - (\lambda-1)^2 m_1^2\left((1-2\lambda)\lambda^2 m_p^2 + (\lambda-2)m_\lambda^2\right)\right. \\
& -\lambda^2(\lambda+1)m_p^2 m_\lambda^2 + (\lambda-1)^4(\lambda+1)m_1^4 + (1-2\lambda)m_\lambda^4\big)\left((\lambda-1)^2 m_1^4\left((2\lambda+3)m_p^2\right.\right. \\
& + (3\lambda+2)m_\lambda^2\big) + m_p^2 m_\lambda^2\left(\lambda^2(3\lambda-5)m_p^2 + (3-5\lambda)m_\lambda^2\right) + m_1^2\left(\lambda^2(2\lambda-5)m_p^4\right. \\
& + \left(2\lambda^3 - 3\lambda^2 - 3\lambda + 2\right)m_p^2 m_\lambda^2 + (2-5\lambda)m_\lambda^4\big)\Big) \\
& + 2 m_p^2 m_1^2 m_\lambda^2\Big(3(\lambda-1)^4 m_1^4\left(\lambda^2 m_p^2 + m_\lambda^2\right) + \left(\lambda^2 m_p^2 + m_\lambda^2\right)^3 \\
& + 3(\lambda-1)^2 m_1^2\left(\lambda^4 m_p^4 - 7\lambda^2 m_p^2 m_\lambda^2 + m_\lambda^4\right) + (\lambda-1)^6 m_1^6\Big)\left(\lambda^2 m_p^4\right. \\
& -2m_p^2\left(\left(\lambda^2 - \lambda + 6\right)m_1^2 + \left(6\lambda^2 - 11\lambda + 6\right)m_\lambda^2\right) + (\lambda-1)^2 m_1^4 \\
& -2\left(6\lambda^2 - \lambda + 1\right)m_1^2 m_\lambda^2 + m_\lambda^4\big) + \Big((\lambda-1)^4 m_1^6\left(m_p^2 + m_\lambda^2\right) + m_p^2 m_\lambda^2\left(\lambda^2 m_p^2 + m_\lambda^2\right)^2 \\
& + (\lambda-1)^2 m_1^4\left(2\lambda^2 m_p^4 - \left(9\lambda^2 + 8\lambda + 9\right)m_p^2 m_\lambda^2 + 2m_\lambda^4\right) \\
& + m_1^2\left(\lambda^4 m_p^6 + \lambda^2\left(-9\lambda^2 + 26\lambda - 26\right)m_p^4 m_\lambda^2 + \left(-26\lambda^2 + 26\lambda - 9\right)m_p^2 m_\lambda^4 + m_\lambda^6\right)\big)^2\Big)
\end{aligned}
$$

$$
\begin{aligned}
s_3 =\ & \frac{\left(\lambda^2 - \lambda + 1\right)^6}{8(\lambda-1)^6\lambda^6}\Big((\lambda-1)^6 m_1^{10}\left(m_p^2 + m_\lambda^2\right) + (\lambda-1)^4 m_1^8\left(\left(8\lambda^2 + 26\lambda + 6\right)m_p^4\right. \\
& + \left(21\lambda^2 + 104\lambda + 21\right)m_p^2 m_\lambda^2 + 2\left(3\lambda^2 + 13\lambda + 4\right)m_\lambda^4\big) \\
& + (\lambda-1)^2 m_1^6\left(\lambda^2\left(14\lambda^2 - 14\lambda - 83\right)m_p^6 + \left(74\lambda^4 + 4\lambda^3 - 99\lambda^2 + 176\lambda + 72\right)m_p^4 m_\lambda^2\right. \\
& + \left(72\lambda^4 + 176\lambda^3 - 99\lambda^2 + 4\lambda + 74\right)m_p^2 m_\lambda^4 + \left(-83\lambda^2 - 14\lambda + 14\right)m_\lambda^6\big) \\
& + m_1^4\left(2\lambda^4\left(4\lambda^2 - 21\lambda + 20\right)m_p^8 + \lambda^2\left(74\lambda^4 - 300\lambda^3 + 357\lambda^2 - 286\lambda + 227\right)m_p^6 m_\lambda^2\right. \\
& + 2\left(82\lambda^6 - 246\lambda^5 + 249\lambda^4 - 88\lambda^3 + 249\lambda^2 - 246\lambda + 82\right)m_p^4 m_\lambda^4
\end{aligned}
$$

$$+ \left(227\lambda^4 - 286\lambda^3 + 357\lambda^2 - 300\lambda + 74\right) m_p^2 m_\lambda^6 + 2\left(20\lambda^2 - 21\lambda + 4\right) m_\lambda^8\big)$$
$$+ m_p^2 m_\lambda^2 \left(\lambda^6 m_p^8 + 2\lambda^4 \left(3\lambda^2 - 19\lambda + 20\right) m_p^6 m_\lambda^2 + \lambda^2 \left(-83\lambda^2 + 180\lambda - 83\right) m_p^4 m_\lambda^4\right.$$
$$+ 2\left(20\lambda^2 - 19\lambda + 3\right) m_p^2 m_\lambda^6 + m_\lambda^8\big) + m_1^2 \left(\lambda^6 m_p^{10} + \lambda^4 \left(21\lambda^2 - 146\lambda + 146\right) m_p^8 m_\lambda^2\right.$$
$$+ \lambda^2 \left(72\lambda^4 - 464\lambda^3 + 861\lambda^2 - 622\lambda + 227\right) m_p^6 m_\lambda^4$$
$$+ \left(227\lambda^4 - 622\lambda^3 + 861\lambda^2 - 464\lambda + 72\right) m_p^4 m_\lambda^6 + \left(146\lambda^2 - 146\lambda + 21\right) m_p^2 m_\lambda^8 + m_\lambda^{10}\big)\big)$$

$$s_4 = \frac{\left(\lambda^2 - \lambda + 1\right)^4}{16(\lambda - 1)^4 \lambda^4} \big(\lambda^4 m_p^8 + 4\lambda^2 \left(4\lambda^2 - 33\lambda + 34\right) m_p^6 m_\lambda^2$$
$$+ 2\left(24\lambda^4 - 160\lambda^3 + 299\lambda^2 - 160\lambda + 24\right) m_p^4 m_\lambda^4$$
$$+ 4(\lambda - 1)^2 m_1^6 \left(\left(5\lambda^2 + 25\lambda + 4\right) m_p^2 + \left(4\lambda^2 + 25\lambda + 5\right) m_\lambda^2\right)$$
$$+ 4\left(34\lambda^2 - 33\lambda + 4\right) m_p^2 m_\lambda^6 + 2 m_1^4 \left(\left(27\lambda^4 - 54\lambda^3 - 37\lambda^2 + 64\lambda + 24\right) m_p^4\right.$$
$$+ 2\left(28\lambda^4 - 39\lambda^3 + 78\lambda^2 - 39\lambda + 28\right) m_p^2 m_\lambda^2$$
$$+ \left(24\lambda^4 + 64\lambda^3 - 37\lambda^2 - 54\lambda + 27\right) m_\lambda^4\big) + 4 m_1^2 \left(\lambda^2 \left(5\lambda^2 - 35\lambda + 34\right) m_p^6\right.$$
$$+ \left(28\lambda^4 - 73\lambda^3 + 129\lambda^2 - 112\lambda + 56\right) m_p^4 m_\lambda^2$$
$$+ \left(56\lambda^4 - 112\lambda^3 + 129\lambda^2 - 73\lambda + 28\right) m_p^2 m_\lambda^4$$
$$+ \left(34\lambda^2 - 35\lambda + 5\right) m_\lambda^6\big) + (\lambda - 1)^4 m_1^8 + m_\lambda^8\big)$$

$$s_5 = \frac{\left(\lambda^2 - \lambda + 1\right)^2}{2(\lambda - 1)^2 \lambda^2} \left(\left(\lambda^2 - 8\lambda + 8\right) m_p^4 + m_p^2 \left(\left(6\lambda^2 - 6\lambda + 4\right) m_1^2 + 2\left(2\lambda^2 - \lambda + 2\right) m_\lambda^2\right)\right.$$
$$+ \left(\lambda^2 + 6\lambda + 1\right) m_1^4 + 2\left(2\lambda^2 - 3\lambda + 3\right) m_1^2 m_\lambda^2 + \left(8\lambda^2 - 8\lambda + 1\right) m_\lambda^4\right) .$$

References

[1] E. Witten, *Supersymmetric index in four-dimensional gauge theories*, *Adv. Theor. Math. Phys.* **5** (2002) 841 [`hep-th/0006010`] [INSPIRE].

[2] R. Dijkgraaf and C. Vafa, *A Perturbative window into nonperturbative physics*, `hep-th/0208048` [INSPIRE].

[3] F. Cachazo, N. Seiberg and E. Witten, *Chiral rings and phases of supersymmetric gauge theories*, *JHEP* **04** (2003) 018 [`hep-th/0303207`] [INSPIRE].

[4] A. Baker, *An Introduction to Galois Theory*, http://www.maths.gla.ac.uk/~ajb/dvi-ps/Galois.pdf.

[5] I. Stewart, *Galois Theory*, Chapman and Hall, London, U.K. (1989).

[6] F. Ferrari, *On the Geometry of Super Yang-Mills Theories: Phases and Irreducible Polynomials*, *JHEP* **01** (2009) 026 [`arXiv:0810.0816`] [INSPIRE].

[7] F. Ferrari, *Galois symmetries in Super Yang-Mills Theories*, *JHEP* **03** (2009) 128 [`arXiv:0901.4079`] [INSPIRE].

[8] V. Naik, *The Group Properties Wiki*, http://groupprops.subwiki.org.

[9] G. Pfeiffer, http://schmidt.nuigalway.ie/subgroups.

[10] The Sage Developers, *SageMath, the Sage Mathematics Software System*, http://www.sagemath.org (2016).

[11] N. Dorey, *An Elliptic superpotential for softly broken $N = 4$ supersymmetric Yang-Mills theory*, *JHEP* **07** (1999) 021 [hep-th/9906011] [INSPIRE].

[12] J. Polchinski and M.J. Strassler, *The String dual of a confining four-dimensional gauge theory*, hep-th/0003136 [INSPIRE].

[13] A. Bourget and J. Troost, *Duality and modularity in elliptic integrable systems and vacua of $\mathcal{N} = 1^*$ gauge theories*, *JHEP* **04** (2015) 128 [arXiv:1501.05074] [INSPIRE].

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

[15] S.P. Kumar and J. Troost, *Geometric construction of elliptic integrable systems and $N = 1^*$ superpotentials*, *JHEP* **01** (2002) 020 [hep-th/0112109] [INSPIRE].

[16] A. Bourget and J. Troost, *Counting the Massive Vacua of $\mathcal{N} = 1^*$ Super Yang-Mills Theory*, *JHEP* **08** (2015) 106 [arXiv:1506.03222] [INSPIRE].

[17] A. Bourget and J. Troost, *On the $\mathcal{N} = 1^*$ gauge theory on a circle and elliptic integrable systems*, *JHEP* **01** (2016) 097 [arXiv:1511.03116] [INSPIRE].

[18] A. Bourget and J. Troost, *The Arithmetic of Supersymmetric Vacua*, *JHEP* **07** (2016) 036 [arXiv:1606.01022] [INSPIRE].

[19] O. Aharony, N. Seiberg and Y. Tachikawa, *Reading between the lines of four-dimensional gauge theories*, *JHEP* **08** (2013) 115 [arXiv:1305.0318] [INSPIRE].

[20] A. Ritz, *Central charges, S-duality and massive vacua of $N = 1^*$ super Yang-Mills*, *Phys. Lett.* **B 641** (2006) 338 [hep-th/0606050] [INSPIRE].

[21] T. Hsu, *Identifying congruence subgroups of the modular group*, *P. Am. Math. Soc.* **124** (1996) 1351.

[22] C.J. Cummins and S. Pauli, *Congruence subgroups of PSL (2, Z) of genus less than or equal to 24*, *Exp. Math.* **12** (2003) 243.

[23] F. Diamond and J. Shurman, *A first course in modular forms*, in *Springer Science and Business Media*, volume 228, (2006).

[24] G. Shimura, *Introduction to the arithmetic theory of automorphic functions. Vol. 1*, Princeton University Press, Princeton, U.S.A. (1971).

[25] A. Landesman, P. Ruhm and R. Zhang, *Spin canonical rings of log stacky curves*, arXiv:1507.02643.

[26] R. Dijkgraaf and C. Vafa, *Matrix models, topological strings and supersymmetric gauge theories*, *Nucl. Phys.* **B 644** (2002) 3 [hep-th/0206255] [INSPIRE].

[27] N. Dorey and A. Sinkovics, *N=1* vacua, fuzzy spheres and integrable systems*, *JHEP* **07** (2002) 032 [hep-th/0205151] [INSPIRE].

[28] O. Aharony, N. Dorey and S.P. Kumar, *New modular invariance in the $N = 1^*$ theory, operator mixings and supergravity singularities*, *JHEP* **06** (2000) 026 [hep-th/0006008] [INSPIRE].

[29] N. Dorey, T.J. Hollowood, S.P. Kumar and A. Sinkovics, *Exact superpotentials from matrix models*, *JHEP* **11** (2002) 039 [hep-th/0209089] [INSPIRE].

[30] C. Bachas, J. Hoppe and B. Pioline, *Nahm equations, $N = 1^*$ domain walls and D strings in $AdS_5 \times S^5$*, *JHEP* **07** (2001) 041 [hep-th/0007067] [INSPIRE].

[31] E.R.C. Abraham and P.K. Townsend, *Intersecting extended objects in supersymmetric field theories*, *Nucl. Phys.* **B 351** (1991) 313 [INSPIRE].

[32] A. Ritz, *A Note on domain walls and the parameter space of $N = 1$ gauge theories*, *JHEP* **10** (2003) 021 [hep-th/0308144] [INSPIRE].

[33] N. Seiberg and E. Witten, *Monopoles, duality and chiral symmetry breaking in $N = 2$ supersymmetric QCD*, *Nucl. Phys.* **B 431** (1994) 484 [hep-th/9408099] [INSPIRE].

[34] P.C. Argyres, M.R. Plesser and N. Seiberg, *The Moduli space of vacua of $N = 2$ SUSY QCD and duality in $N = 1$ SUSY QCD*, *Nucl. Phys.* **B 471** (1996) 159 [hep-th/9603042] [INSPIRE].

[35] A. Gorsky, S. Gukov and A. Mironov, *Multiscale $N = 2$ SUSY field theories, integrable systems and their stringy/brane origin. 1.*, *Nucl. Phys.* **B 517** (1998) 409 [hep-th/9707120] [INSPIRE].

[36] A. Mironov, A. Morozov, B. Runov, Y. Zenkevich and A. Zotov, *Spectral Duality Between Heisenberg Chain and Gaudin Model*, *Lett. Math. Phys.* **103** (2013) 299 [arXiv:1206.6349] [INSPIRE].

[37] T.J. Hollowood and K. Ohta, *Vacua of $N = 1$ supersymmetric QCD from spin chains and matrix models*, *JHEP* **02** (2005) 042 [hep-th/0405051] [INSPIRE].

[38] D. Gaiotto, *N=2 dualities*, *JHEP* **08** (2012) 034 [arXiv:0904.2715] [INSPIRE].

[39] G. Bonelli, S. Giacomelli, K. Maruyoshi and A. Tanzini, *N=1 Geometries via M-theory*, *JHEP* **10** (2013) 227 [arXiv:1307.7703] [INSPIRE].