Galois groups of multivariate Tutte polynomials

Adam Bohn\textsuperscript{1}, Peter J. Cameron\textsuperscript{1}, and Peter Müller\textsuperscript{2}

\textsuperscript{1}School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK.
\textsuperscript{2}Institut für Mathematik, Universität Würzburg, Campus Hubland Nord, 97074 Würzburg, Germany

November 15, 2011

Abstract

The multivariate Tutte polynomial $\hat{Z}_M$ of a matroid $M$ is a generalization of the standard two-variable version, obtained by assigning a separate variable $v_e$ to each element $e$ of the ground set $E$. It encodes the full structure of $M$. Let $v = \{v_e\}_{e \in E}$, let $K$ be an arbitrary field, and suppose $M$ is connected. We show that $\hat{Z}_M$ is irreducible over $K(v)$, and give three self-contained proofs that the Galois group of $\hat{Z}_M$ over $K(v)$ is the symmetric group of degree $n$, where $n$ is the rank of $M$. An immediate consequence of this result is that the Galois group of the multivariate Tutte polynomial of any matroid is a direct product of symmetric groups. Finally, we conjecture a similar result for the standard Tutte polynomial of a connected matroid.

Let $M$ be a finite matroid on the set $E$. The rank of $M$ is denoted by $r(M)$, and $r_M$ is the rank function on $M$. With this notation we have $r(M) = r_M(E)$. To avoid degenerate examples and exceptions a connected matroid will be assumed throughout to have positive rank (our results are trivial for a matroid having zero rank). Following the usual notation in matroid theory, we will write $E \setminus e$ instead of $E \setminus \{e\}$ for $e \in E$, and denote by $M|A$ the restriction of $M$ to some $A \subseteq E$.

For each $e \in E$ let $v_e$ be a variable, and let $v$ be the collection of these variables. If $A$ is a subset of $E$, we will denote by $v_A$ the set $\{v_e\}_{e \in A}$. In \cite{Sokal} Sokal defines the following multivariate version of the Tutte polynomial of a matroid $M$ \cite{Sokal}.

For another variable $q$ set

$$\hat{Z}_M(q, v) = \sum_{A \subseteq E} q^{-r_M(A)} \prod_{e \in A} v_e.$$ 

\footnote{The multivariate Tutte polynomial for matroids has in fact been discovered a number of times; it appears, for example, in \cite{Helm} as the “Tugger polynomial”.

1
Then $\hat{Z}_M(q,v)$ is a polynomial in $\frac{1}{q}$ with coefficients in $\mathbb{Z}[v]$.

For our purpose it is more convenient to use the following minor modification:

$$\hat{Z}_M(q,v) = \sum_{A \subseteq E} q^{r(M) - r_M(A)} \prod_{e \in A} v_e.$$ 

Then

$$\hat{Z}_M(q,v) = q^{r(M)} \hat{Z}_M(q,v),$$

and $\hat{Z}_M(q,v)$ is a polynomial of degree $r(M)$ in $q$, which is monic if $M$ contains no loops. In particular, if $M$ is connected then $\hat{Z}_M(q,v)$ is monic. Combinatorially, $\hat{Z}_M(q,v)$ is a generating function for the content and rank of the subsets of $E$, and thus encodes all of the information about $M$.

By making the substitutions

$$q \leftarrow (x - 1)(y - 1)$$

$$v_e \leftarrow y - 1$$

for each $e \in E$, and multiplying by a prefactor $(y - 1)^{-r(M)}$, we obtain the standard bivariate Tutte polynomial:

$$T_M(x,y) = \sum_{A \subseteq E} (x - 1)^{r(M) - r_M(A)}(y - 1)^{|A| - r_M(A)}.$$ 

Thus $T_M$ is essentially equivalent to a special case of $\hat{Z}_M$ in which the same variable is assigned to every element of $E$.

**Theorem 1.** Let $M$ be a finite connected matroid with positive rank $n = r(M)$, and let $\hat{Z}_M(q,v)$ be as defined above. Let $K$ be an arbitrary field. Then the Galois group of $\hat{Z}_M(q,v)$ over $K(v)$ is the symmetric group on the $n$ roots of $\hat{Z}_M(q,v)$.

For $e \in E$, let $M \setminus e$ be the deletion of $e$, and $M/e$ the contraction of $e$. Note that $M \setminus e$ and $M/e$ are matroids on the set $E \setminus e$. The essential tool for our first proof is a theorem of Tutte (see [6, Theorem 4.3.1]), which says that connectivity of $M$ implies that at least one of the matroids $M \setminus e$ or $M/e$ is connected. Since $M$ is connected, $e$ is not a coloop, so $r(M \setminus e) = r_M(E \setminus e) = r_M(E) = r(M)$. By [6, Prop. 3.1.6] we have that $r(M/e) = r_M(E) - r_M(e)$. Now $r_M(e) = 1$, since $e$ is not a loop. So $r(M/e) = r(M) - 1$.

The proof will be based on some lemmas.

**Lemma 2.** Let $M$ be a finite connected matroid and $e \in E$. Then

$$\hat{Z}_M = \hat{Z}_{M \setminus e} + v_e \hat{Z}_{M/e}.$$ 

**Proof.** Since $M$ is connected, $e$ is neither a loop nor a coloop. By [7, (4.18a)]

$$\hat{Z}_M = \hat{Z}_{M \setminus e} + \frac{v_e}{q} \hat{Z}_{M/e},$$

hence

$$\hat{Z}_M = q^{r(M) - r(M \setminus e)} \hat{Z}_{M \setminus e} + q^{r(M) - r(M/e)} \frac{v_e}{q} \hat{Z}_{M/e}.$$ 

The claim then follows from the previous determination of the ranks of $E \setminus e$ and $E/e$. 

\[\square\]
As an intermediate step in the proof of the theorem, we need to know that \( \hat{Z}_M \) is irreducible over \( K(v) \). As \( T_M \) is essentially a specialization of \( \hat{Z}_M \), this would follow from \( \text{[2]} \) in the case where \( K \) has characteristic zero. However, the multivariate case allows for a much simpler proof, and one which holds for any characteristic.

**Lemma 3.** Let \( M \) be a finite connected matroid. Then \( \hat{Z}_M \) is irreducible over \( K(v) \).

*Proof.* The induction proof is most conveniently formulated by considering a counterexample \( M \) where \( r(M) \) is minimal; among these counterexamples, we pick one where \( |E| \) is minimal. Clearly, the result holds for \( r(M) = 1 \), so \( r(M) \geq 2 \). Pick \( e \in E \). By Lemma \( \text{[2]} \), \( \hat{Z}_M = \hat{Z}_{M\setminus e} + v_e \hat{Z}_{M/e} \). Note that \( v_e \) does not appear in \( \hat{Z}_{M\setminus e} \) and \( \hat{Z}_{M/e} \). If \( M \setminus e \) is connected, then \( \hat{Z}_{M\setminus e} \) is irreducible by minimality of \( |E| \). As \( \hat{Z}_M \) and \( \hat{Z}_{M\setminus e} \) have the same degree, setting \( v_e = 0 \) shows that \( \hat{Z}_M \) is irreducible, a contradiction. So \( M \setminus e \) is not connected, which by Tutte’s theorem means that \( M/e \) is connected. So \( r(M/e) \geq 1 \) (because \( r(M) \geq 2 \)), and \( \hat{Z}_{M/e} \) is monic. Note also that because \( M \) is loopless, so too is \( M \setminus e \), and hence \( \hat{Z}_{M\setminus e} \) is also monic.

Now, consider a non-trivial factorization of \( \hat{Z}_M \). Since \( \hat{Z}_M \) is monic and linear in \( v_e \), we can write \( \hat{Z}_M = (U + v_e V)W \), where \( U, V, W \) are polynomials in \( K[v][q] \) in which \( v_e \) does not appear, and where each factor has positive degree in \( q \).

So \( (U + v_e V)W = \hat{Z}_{M\setminus e} + v_e \hat{Z}_{M/e} \). Comparing coefficients with respect to \( v_e \) gives \( UW = \hat{Z}_{M\setminus e} \) and \( VW = \hat{Z}_{M/e} \). By minimality of the counterexample, \( \hat{Z}_{M/e} \) is irreducible. But \( W \) has positive degree in \( q \), so \( V = 1 \) and \( W = \hat{Z}_{M/e} \).

Thus \( U \hat{Z}_{M/e} = \hat{Z}_{M\setminus e} \). Now, \( \hat{Z}_{M/e} \) and \( \hat{Z}_{M\setminus e} \) are monic of degrees \( r(M) - 1 \) and \( r(M) \) respectively. So \( U = q + \beta \) for some \( \beta \in K[v] \). Let \( \bar{v} = v \setminus \{v_e\} \), and note that

\[
\hat{Z}_{M\setminus e}(1, \bar{v}) = \prod_{i \in E \setminus e} (1 + v_i) = \hat{Z}_{M/e}(1, \bar{v})
\]

so \( \beta = 0 \). Now setting \( q = 0 \) gives \( \hat{Z}_{M\setminus e}(0, \bar{v}) = 0 \). This means that there are no bases in \( M \setminus e \), which is only possible if every element of \( E \setminus e \) is a loop. So we have a contradiction. \( \square \)

In order to prove the theorem, we need more precise information about how Galois groups behave under specializations of parameters. The next result is well-known, it follows for instance from \( \text{[1]} \) Theorem IX.2.9.

**Proposition 4.** Let \( R \) be an integral domain which is integrally closed in its quotient field \( F \). Let \( f \in R[X] \) be monic and irreducible over \( F \). Let \( R \rightarrow k, r \mapsto \bar{r} \) be a homomorphism to a field \( k \). If \( f \in k[X] \) is separable, then \( \text{Gal}(f/k) \) is a subgroup of \( \text{Gal}(f/F) \).

The following two lemmas can be obtained through applications of this proposition.
Lemma 5. Let \( A \) be a subset of \( E \). Then \( \text{Gal}(\hat{Z}_{M|A}/K(\mathbf{v}_A)) \) is a subgroup of \( \text{Gal}(\hat{Z}_M/K(\mathbf{v})) \).

Proof. Let \( B \) be such that \( A \subset B \subseteq E \), and let \( e \) be an element of \( B \setminus A \). Note that removing \( e \) from \( B \) corresponds to specializing \( \mathbf{v}_e \) to zero in \( \hat{Z}_{M|B} \). Let \( R = K(\mathbf{v}_{B \setminus A})[\mathbf{v}_e], \) and let \( I \) be the maximal ideal of \( R \) generated by \( \mathbf{v}_e \). The image of \( \hat{Z}_M \) in the canonical homomorphism \( R \to R/I \) is either \( q\hat{Z}_{M|B(e)} \) or \( \hat{Z}_{M|B(e)} \), depending on whether or not \( e \) is a coloop. In both cases we have a separable polynomial, as the presence of a repeated irreducible factor would contradict the fact that \( \hat{Z}_{M|B(e)} \) is linear in the elements of \( \mathbf{v}_{B\setminus e} \). Furthermore, \( R \) is integrally closed in its quotient field \( K(\mathbf{v}) \). So we have that \( \text{Gal}(\hat{Z}_{M|B(e)}/K(\mathbf{v}_{B\setminus e})) \) is transitive on the \( n \) roots of \( \hat{f} \), and the result follows by induction.

Lemma 6. Let \( y \) be a variable over the field \( k \), and \( U, V \in k[X] \) with \( \deg V = n - 1 \), and \( U \) monic of degree \( n \) (where \( n \geq 2 \)). Suppose that \( f(X) = U(X) + yV(X) \) is irreducible over \( k(y) \) (which is equivalent to \( U \) and \( V \) being relatively prime). If \( \text{Gal}(U/k) = S_n \) or \( \text{Gal}(V/k) = S_{n-1} \), then \( \text{Gal}(f/k(y)) = S_n \).

Proof. First suppose that \( \text{Gal}(U/k) = S_n \). Then the assertion follows immediately from Proposition 4 by setting \( R = k[y] \) and considering the homomorphism \( R \to k, h(y) \mapsto h(0) \).

Now assume that \( \text{Gal}(V/k) = S_{n-1} \). Set \( t = 1/y \) and replace \( f(X) = U(X) + yV(X) = U(X) + tV(X) \) with \( t \) times the reciprocal of \( f(X) \), that is set \( f(X) = X^n(tU(1/X) + V(1/X)) \). Clearly, \( k(t) = k(y) \) and \( \text{Gal}(f/k(y)) = \text{Gal}(f/k(t)) \). The coefficient of \( X^n \) in \( \hat{f} \) is \( tu + v \), where \( u \) and \( v \) are the constant terms of \( U \) and \( V \). If \( v = 0 \), then \( V \) has the root 0. However, \( V \) is irreducible since \( \text{Gal}(V/k) = S_{n-1} \). So \( n = 2 \). The result clearly holds in this case because \( f \) is then irreducible of degree 2.

So assume \( v \neq 0 \). Let \( R \subset k(t) \) be the localization of \( k[t] \) with respect to the ideal \( (t) \), so \( R \) consists of the fractions \( p(t)/q(t) \) with \( q(0) \neq 0 \). Note that \( \frac{1}{v+tu} \hat{f} \) is monic with coefficients in \( R \). Also, \( R \) (as a local ring) is integrally closed in \( k(t) \). Let \( R \to k \) be the homomorphism given by \( p(t)/q(t) \mapsto p(0)/q(0) \). Proposition 4 then gives \( \text{Gal}(\hat{f}/k(t)) \geq \text{Gal}(X^nV(1/X)/k) = S_{n-1} \). Because \( \text{Gal}(\hat{f}/k(t)) \) is transitive on the \( n \) roots of \( \hat{f} \), we must have \( \text{Gal}(\hat{f}/k(t)) = S_n \).

We are now ready to prove Theorem 1.

First proof of Theorem 1. Again assume that the matroid \( M \) is a counterexample with \( r_M(E) \) minimal, and among these cases pick one with \( |E| \) minimal. Note that the statement is trivially true if \( r(M) = 1 \), thus \( r(M) \geq 2 \) in the minimal counterexample.

Pick \( e \in E \). By Lemma 2 \( \hat{Z}_M = \hat{Z}_M|e + v_e\hat{Z}_M|e \). Let \( \mathbf{v} = \mathbf{v} \setminus \{v_e\} \), and set \( k = K(\mathbf{v}) \). Recall that \( \hat{Z}_M \) is irreducible over \( k(\mathbf{v}_e) \) by Lemma 3. We have seen above that \( r(M\setminus e) = r(M) = n \) and \( r(M/e) = n - 1 \). As established previously, either \( M \setminus e \) or \( M/e \) is connected. By assuming a minimal counterexample we
have \( \text{Gal}(\hat{Z}_{M|C}/k) = S_n \) or \( \text{Gal}(\hat{Z}_{M|C}/k) = S_{n-1} \). Theorem \( \square \) then follows from Lemma \( \square \)

We will now present an alternative proof of Theorem \( \square \). While it is less efficient than the above proof, it uses a group-theoretical inductive process which is perhaps more intuitive. We will need to first prove that the theorem holds for circuits.

**Lemma 7.** Let \( C \subseteq E \) be a circuit of a finite matroid \( M \). Then \( \text{Gal}(\hat{Z}_{M|C}/K(v_C)) = S_{r_M(C)} \).

**Proof.** The rank of any proper subset of \( C \) is the same as its cardinality, and \( r_M(C) = |C| - 1 \), so:

\[
\hat{Z}_{M|C}(q,v) = q^n + \sigma_1 q^{n-1} + \sigma_2 q^{n-2} + \ldots + \sigma_{n-1}q + (\sigma_n + \sigma_{n+1}),
\]

where \( \sigma_i \) is the \( i \)th elementary symmetric polynomial in the \( \{v_e\}_{e \in C} \) for each \( i \). The elementary symmetric polynomials are algebraically independent, and thus so too are the coefficients of \( \hat{Z}_{M|C}(q,v) \). It is well known that the Galois group of a polynomial with algebraically independent coefficients is the full symmetric group. \( \square \)

**Second proof** of Theorem \( \square \). Let \( C \) be a circuit of maximum cardinality in \( M \). By Lemma \( \square \), \( \text{Gal}(\hat{Z}_{M|C}/K(v_C)) = S_{r_M(C)} \). This will serve as the base case for the induction.

Now, let \( A \) be any proper subset of \( E \) such that \( C \subseteq A \) and \( M|A \) is connected, and suppose that \( \text{Gal}(\hat{Z}_{M|A}/K(v_A)) = S_{r_M(A)} \). Identify a non-empty independent set \( B \subseteq E \setminus A \) of minimal size such that \( M|(A \cup B) \) is connected, and let \( A' = (A \cup B) \). We will show that \( \text{Gal}(\hat{Z}_{M|A'}/K(v_{A'})) = S_{r_M(A')} \).

By Lemma 1.3.1 \( r_M(A') \leq r_M(A) + r_M(B) \). By maximality of \( C \), any circuit of \( M|A' \) has rank at most \( r_M(C) \). By minimality of \( B \), any circuit of \( M|A' \) not contained in \( M|A \) must include at least one element of \( A \), so \( r_M(B) \leq r_M(C) - 1 \), and we have \( r_M(A') \leq r_M(A) + r_M(C) - 1 \).

By Lemma \( \square \), \( S_{r_M(A)} = \text{Gal}(\hat{Z}_{M|A}/K(v_A)) \leq \text{Gal}(\hat{Z}_{M|A'}/K(v_{A'})) \). So \( \text{Gal}(\hat{Z}_{M|A'}/K(v_{A'})) \) must contain at least one transposition. Let \( H \) be the group generated by all of the transpositions in \( \text{Gal}(\hat{Z}_{M|A'}/K(v_{A'})) \); then \( H \) is a direct product of symmetric groups. As \( \text{Gal}(\hat{Z}_{M|A'}/K(v_{A'})) \) is transitive, each of these symmetric groups must have the same degree \( i \), which must therefore divide the degree of \( \text{Gal}(\hat{Z}_{M|A'}/K(v_{A'})) \). By Lemma \( \square \), \( \hat{Z}_{M|A'} \) is irreducible, and its Galois group must therefore be transitive of degree \( r_M(A') \). So we have that \( ji = r_M(A') \) for some positive integer \( j \).

Now, \( S_{r_M(A)} \) contains at least one of the transpositions of \( H \), so must be a subgroup of one of the \( S_i \), which means \( r_M(A) \leq i \). So we have:

\[
jr_M(A) \leq ji = r_M(A') \leq r_M(A) + r_M(C) - 1.
\]

Suppose that \( j \geq 2 \). Then \( 2r_M(A) \leq r_M(A) + r_M(C) - 1 \), and so \( r_M(A) \leq r_M(C) - 1 \). This is impossible, as \( C \subseteq A \). So \( j = 1 \), and hence \( i = r_M(A') \). This
means that $H$ is a direct product of symmetric groups of degree $r_M(A')$. But $H$ is a subgroup of $\Gal(\hat{Z}_{M,A'}/K(\mathbf{v}_{A'}))$, which is transitive of degree $r_M(A')$, and so $\Gal(\hat{Z}_{M,A'}/K(\mathbf{v}_{A'})) = H = S_{r_M(A')}$. □

Now, in view of the proof of Lemma\textsuperscript{7} one might wonder if the coefficients of $\hat{Z}_M(q, \mathbf{v})$ are algebraically independent for any finite connected matroid. This does indeed turn out to be the case, leading us to our third and final proof of Theorem\textsuperscript{1}.

**Third proof of Theorem\textsuperscript{1}**. Let $M$ be a finite connected matroid of rank $r(M) = n \geq 1$, and write $\hat{Z}_M(q, \mathbf{v}) = q^n + a_{n-1}q^{n-1} + \cdots + a_1q + a_0 \in K[\mathbf{v}][q]$, where $K$ is an arbitrary field. It suffices to show that the coefficients $a_0, a_1, \ldots, a_{n-1}$ are algebraically independent over $K$.

If $n = 1$, then $\hat{Z}_M(q, \mathbf{v}) = q - 1 + \prod_{e \in E}(v_e + 1)$, so the claim clearly holds. Thus we may assume $n \geq 2$.

Assume that $M$ is a counterexample in which $|E|$ is minimal. We will use the deletion-contraction identity $\hat{Z}_M = \hat{Z}_{M\setminus e} + v_e \hat{Z}_{M/e}$ of Lemma\textsuperscript{2}. First consider the case that $M \setminus e$ is connected. By the assumption of a minimal counterexample, the coefficients of $\hat{Z}_{M\setminus e}$ (excluding the leading coefficient 1) are algebraically independent over $K$. However, these coefficients arise from the coefficients $a_0, a_1, \ldots, a_{n-1}$ upon setting $v_e = 0$. Of course, an algebraic dependency relation of $a_0, a_1, \ldots, a_{n-1}$ over $K$ remains an algebraic dependency relation upon setting $v_e = 0$, a contradiction.

Thus $M \setminus e$ is not connected, so we may assume that $M/e$ is connected. For each $0 \leq i \leq n - 1$, write $a_i = b_i + v_ec_i$, where $b_i$ and $c_i$ are polynomials in the elements of $\mathbf{v}_{E\setminus e}$. Each $c_j$ is then the coefficient of $q^j$ in $\hat{Z}_{M/e}$, so $c_{n-1} = 1$ (as $r(M/e) = n-1$) and $c_0, c_1, \ldots, c_{n-2}$ are algebraically independent over $K$. As $a_0, a_1, \ldots, a_{n-1}$ are algebraically dependent, there is a non-zero polynomial $P$ in $n$ variables over $K$ such that

$$P(b_0 + v_c_0, \ldots, b_{n-2} + v_c_{n-2}, b_{n-1} + v_e) = 0.$$ 

Let $Q$ be the expansion of $P$ with respect to $v_e$, so that $Q$ is a polynomial in $v_e$ with coefficients in $K[\mathbf{v}_{E\setminus e}]$. As the elements of $\mathbf{v}$ are algebraically independent, these coefficients must be identically zero. Let $d$ be the total degree of $P$. Then $Q$ has degree $d$ in $v_e$, and the $v_e^d$ term must arise from a $K$-linear sum of products of the form:

$$(b_0 + v_e c_0)^{d_0} \cdots (b_{n-2} + v_e c_{n-2})^{d_{n-2}}(b_{n-1} + v_e)^{d_{n-1}},$$

where $d_0, \ldots, d_{n-1}$ are non-negative integers which sum to $d$. This means that the coefficient of $v_e^d$ in $Q$ is a $K$-linear combination of monomials of the form $c_0^{d_0} \cdots c_{n-2}^{d_{n-2}}$, where $d_i \geq 0$ for each $i$, and $d_0 + \cdots + d_{n-2} \leq d$. The vanishing of this coefficient then implies that the set of such monomials is linearly dependent over $K$, which contradicts our assertion that $c_0, \ldots, c_{n-2}$ are algebraically dependent over $K$. □
Remark 8. Sokal showed that the the multivariate Tutte polynomial for matroids factorizes over summands (see [7, (4.4)]). That is, if $M$ is the direct sum of connected matroids $M_1, M_2$ on the sets $E_1, E_2$ respectively (where $E_1$ and $E_2$ are disjoint and $E = E_1 \cup E_2$) then:

$$\tilde{Z}_M(q, v) = \tilde{Z}_{M_1}(q, v_{E_1}) \tilde{Z}_{M_2}(q, v_{E_2}).$$

As $v_{E_1}$ and $v_{E_2}$ are disjoint, there are clearly no algebraic dependencies between the roots of $\tilde{Z}_{M_1}$ and $\tilde{Z}_{M_2}$, so we have that

$$\text{Gal}(\tilde{Z}_M/K(v)) = \text{Gal}(\tilde{Z}_{M_1}/K(v_{E_1})) \times \text{Gal}(\tilde{Z}_{M_2}/K(v_{E_2})).$$

Theorem 1 then implies that the Galois group of the multivariate Tutte polynomial of any matroid is a direct product of symmetric groups corresponding to the connected direct summands.

Finally, we computed the Galois group of the bivariate Tutte polynomial $T_G(x, y)$ over $Q(y)$ for every biconnected graph $G$ of order $n \leq 10$, and found that all were the symmetric group of degree $n - 1$. As the Tutte polynomial of any connected matroid is irreducible over fields of characteristic zero (as noted in [2], this is not necessarily the case for fields of positive characteristic), this would seem to suggest the following:

Conjecture 9. Let $M$ be a finite connected matroid with positive rank $n = r(M)$, and let $K$ be a field of characteristic zero. Then the Galois group of the Tutte polynomial $T_M(x, y)$ over $K(y)$ is the symmetric group of degree $n$.

As remarked previously, the bivariate Tutte polynomial is essentially a specialization of the multivariate version. This means that Theorem 1 would follow from a proof of Conjecture 9 for fields of characteristic zero.

Interestingly, specializing the Tutte polynomial further produces a range of different Galois groups. For example, it was shown in [1] that all of the transitive permutation groups of degree at most 5 apart from $C_5$ appear as Galois groups of just one family of chromatic polynomials. Furthermore, Morgan [5] showed that a range of transitive groups of higher degree occur for chromatic polynomials of graphs on up to 10 vertices.

References

[1] Peter J. Cameron and Kerri Morgan. Algebraic properties of chromatic roots. Submitted.

[2] C. Merino, A. de Mier and M. Noy. Irreducibility of the Tutte polynomial of a connected matroid. Journal of Combinatorial Theory, 83:298–304, 2001.

[3] J.P.S. Kung. Twelve views of matroid theory. Combinatorial & computational mathematics: present and future: Pohang, the Republic of Korea, 15-17 February 2000, page 56, 2001.
[4] Serge Lang. *Algebra*. Addison–Wesley, Menlo Park, 1984.

[5] Kerri Morgan. *Algebraic aspects of the chromatic polynomial*. PhD thesis.

[6] James G. Oxley. *Matroid theory*. Oxford Science Publications. The Clarendon Press Oxford University Press, New York, 1992.

[7] Alan D. Sokal. The multivariate Tutte polynomial (alias Potts model) for graphs and matroids. *Surveys in Combinatorics*, 327:173–226, 2005.