Computing Galois Groups in *Mathematica*

Mathematica can be used to compute and form Cayley tables of the Galois groups of polynomials in $\mathbb{R}$. In addition, Mathematica can actually define a field extension and directly produce the elements of the Galois Group.

By William Paulsen

The purpose of this paper is to demonstrate how *Mathematica* can be used to compute and form Cayley tables of the Galois groups of polynomials in $\mathbb{R}$. There have already been examples of using *Mathematica* in an abstract algebra course, but few have gone to the extent of actually defining a field extention and directly producing the elements of the Galois group. Such a presentation helps students to comprehend an otherwise difficult subject.

1. Introduction

In spite of the fact that *Mathematica* is making its way into the curriculum of most undergraduate mathematics programs, there is a shortage of applications available
for abstract algebra. *Mathematica* notebooks and courseware becoming available as a supplement to a modern algebra course,but most of them only work with finite groups, offering little aid to the students who go on to study rings and fields.

This is ironic, since the power of *Mathematica*'s **ReplaceAll** command allows students to study extention fields of Q. For example, consider the extention $\mathbb{Q}(2\cos(\pi/9))$. Using
trigonometric identities, we see that $2\cos(\pi/9)$ satisfies the polynomial equation $X^3 - 3X - 1 = 0$. *Mathematica* can verify that the polynomial is irreducible.

```
Factor[X^3 - 3 X - 1]
```

$-1 - 3X + X^3$

Suppose we were to create a root to this polynomial, z. This can be accomplished by defining z^3 to be $3z + 1$.

```
z /: z^3 := 3 z + 1
```

Using a **TagSetDelayed** avoids having to redefine the power function. Of course this only affects expressions containing z^3 directly---we would also like z^4 to simplify to $3z^2 + z$, and so on.

The module

```
UsedSymbols = {};
Define[a_Symbol^n_Integer, b_] := Module[{i, m},
        UsedSymbols = Union[UsedSymbols, {a}];
        a /: a^n := b;
        For[i = n + 1, i <= 2 n, i++,
            a /: a^i := Evaluate[FixedPoint[Expand, (a^(i - 1)) a]]];
        a /: a^m_ := FixedPoint[Expand, (a^(2 n)) (a^(m - 2 n))] /; m > 2 n]
```

allows us to create definitions with the command

```
Define[a^3, 3 a + 1]
```

which defines all powers of a recursively. Thus, *Mathematica* will quickly simplify a^9 to $27a^2 + 90a + 28$. In like manner we can define $\mathbb{Q}(a)$ for any algebraic number a.

In actuality, we have defined the field $\mathbb{Q}[X] \Big/ \left(X^3 - 3X - 1\right)$, where $\left(X^3 - 3X - 1\right)$ is the ideal generated be the polynomial. The isomorphism
$\mathbb{Q}(a) \approx \mathbb{Q}[X] \Big/ \left(X^3 - 3X - 1\right)$ becomes clear in this setting, which is a beautiful illustration of the first isomorphism theorem for rings.

Other patterns become evident from this example. We can describe any element
of this field in terms of $A_1 + A_2\, a + A_3\, a^2$, where A_1, A_2, and A_3 are rational numbers. It is clear that any higher power of a will be expressible in this form, hence the product
of any two numbers in this field evaluates to an expression in the field:

```
Expand[Expand[(A1 + A2 a + A3 a^2) (B1 + B2 a + B3 a^2)]]
```

```
A1 B1 + a A2 B1 + a^2 A3 B1 + a A1 B2 + a^2 A2 B2 +
  A3 B2 + 3 a A3 B2 + a^2 A1 B3 + A2 B3 + 3 a A2 B3 + a A3 B3 + 3 a^2 A3 B3
```

From this we can see that this new field is a three dimensional extension of $\mathbb{Q}$, which naturally comes from that fact that the polynomial we used, $X^3 - 3X - 1$, is a cubic polynomial.

But this raises another question. Since we have created this field so that $X^3 - 3X - 1$ will have a root, namely a, can we now use *Mathematica* to *factor* this polynomial? Certainly one factor would be $(X - a)$, and *Mathematica* can find the other factor with the command

```
g = PolynomialQuotient[X^3 - 3 X - 1, X - a, X]
```

```
-3 + a^2 + a X + X^2
```

yet the result does not factor over $\mathbb{Q}$:

```
Factor[g]
```

```
-3 + a^2 + a X + X^2
```

Yet this expression may very well factor in the field $\mathbb{Q}(a)$ that we have just defined. How can students determine whether this factors in $\mathbb{Q}(a)$?

Although *Mathematica 3.0* has a factor command that allows coefficients of the polynomial to be rational combinations of algebriac numbers, these rational fuctions are limited to square roots and higher order roots. Since there is no way of declaring a to be algebriac, we must find another way
to factor polynomials in $\mathbb{Q}(a)$.

2. Factorization in $\mathbb{Q}(a)$

Students can easily define the extention $\mathbb{Q}(a)$ with one **Define** command, using the irreducible polynomial $f(X)$ for which a is a root. However, there will be other roots to the polynomial
$f(X)$ besides the root a. For example, the three roots of $X^3 - 3X - 1$ are as follows.

```
NSolve[X^3 - 3 X - 1 == 0, X]
```

```
{{X → -1.53209}, {X → -0.347296}, {X → 1.87939}}
```

We can use the roots of the irreducible polynomial to produce the next definition.

- **Definition 2.1**
  Given an irreducible polynomial $f(X)$ with roots $a_1, a_2, a_3, \ldots a_n$, we define the *norm* of a function $g(a)$ to be

$$N(g(a)) = g(a_1) \cdot g(a_2) \cdot g(a_3) \cdots g(a_n).$$

For example, the norm of $g(a)$ defined above can be computed in *Mathematica*.

```
Expand[(g /. a -> -1.53209) (g /. a -> -0.347296) (g /. a -> 1.87939)]
```

$$1.00003 + 6.00007\,X + 8.99996\,X^2 - 2.00004\,X^3 - 5.99999\,X^4 + 4.\times 10^{-6}\,X^5 + X^6$$

The fact that the coefficients are integers comes as no surprise, since $N(g)$ is a symetric function of the three roots. It is not difficult to have *Mathematica* determine how much precision is needed to find the coefficients to the nearest integer. The routine **Norm[g, a]** is included in the package

```
<< galois.m
```

Thus, we can use this routine to find the exact value of $N(g)$.

```
Define[a^3, 3 a + 1]
Norm[g, a]
```

$$1 + 6\,X + 9\,X^2 - 2\,X^3 - 6\,X^4 + X^6$$

Since we now have a standard polynomial in $\mathbb{Q}$, we can use *Mathematica* to factor this.

```
Factor[%]
```

$$\left(-1 - 3\,X + X^3\right)^2$$

We see that this factors! This suggests that $g(X)$ may factor as well. However, $N(g)$ may factor even if $g(X)$ does not. But if we make a slight modification to $g(X)$ before we take the norm, we can determine whether or not $g(X)$ factors in $\mathbb{Q}(a)$.

■ **Proposition 2.2**
Let $g(X, a)$ be a polynomial in $\mathbb{Q}(a)[X]$.
Let $h(X, \lambda, a) = g(X - \lambda a, a)$ be the polynomial formed by replacing X with $X - \lambda a$, where λ is introduced as a new variable.
Then $g(X, a)$ factors if, and only if, $N(h(X, \lambda, a))$ factors in $\mathbb{Q}[X, \lambda]$.

Proof:
If $g(X, a)$ factors into $p(X, a)\cdot q(X, a)$, then $h(X, \lambda, a) = p(X - \lambda a, a)\cdot q(X - \lambda a, a)$, and so $N(h(X, \lambda, a)) = N(p(X - \lambda a, a))\cdot N(q(X - \lambda a, a))$, and so $N(h(X, \lambda))$ factors in $\mathbb{Q}[X, \lambda]$.
Now suppose that $g(X, a)$ is an irreducible polynomial of degree r in $\mathbb{Q}(a)[X]$. We may assume without loss of generality that the leading coefficent of $g(X)$ is 1. Let us define
$j(X, \lambda, a) = h(\lambda X, \lambda, a) = g(\lambda X - \lambda a, a)$.
The norm of $j(X, \lambda, a)$ is given by

$$g(\lambda X - \lambda a_1, a_1)\cdot g(\lambda X - \lambda a_2, a_2)\cdot(\lambda X - \lambda a_3, a_3)\cdots g(\lambda X - \lambda a_n, a_n) \in \mathbb{Q}[X, \lambda] \quad (*)$$

where $a_1, a_2, a_3, \ldots a_n$ are the n roots of the irreducible polynomial $f(X)$.
Since $g(X, a)$ irreducible in $\mathbb{Q}(a)[X, \lambda]$, so is $g(\lambda X - \lambda a_i, a_i)$ for each $1 \le i \le n$. Thus, (*) is the factorization of $N(j(X, \lambda, a))$ in $\mathbb{Q}(a)[X, \lambda]$. If $N(j(X, \lambda, a))$ should factor in $\mathbb{Q}[X, \lambda]$, then a non-trivial subset of factors in (*) must produce a polynomial in $\mathbb{Q}$[X,λ]. That is, there is a subset of roots $\{a_{k_1}, a_{k_2}, \ldots, a_{k_m}\}$ such that

$$g(\lambda X - \lambda a_{k_1}, a_{k_1})\cdot g(\lambda X - \lambda a_{k_2}, a_{k_2})\cdots g(\lambda X - \lambda a_{k_m}, a_{k_m}) \in \mathbb{Q}[X, \lambda]. \quad (**)$$

Let us now consider the terms in (**) with the highest power of λ.The highest coefficient of $g(X, a)$ is 1, and it is apparent that the other terms in $g(X, a)$ will not contribute to the highest power of λ. Thus, the terms with the largest power of λ will be

$\lambda^{r\,m} \cdot (X - a_{k_1})^r \cdot (X - a_{k_2})^r \cdots (X - a_{k_m})^r$.

Thus, $[(X - a_{k_1})(X - a_{k_2}) \cdots (X - a_{k_m})]^r \in \mathbb{Q}[X]$. But since $\mathbb{Q}$ is of characteristic 0, we can say that $(X - a_{k_1})(X - a_{k_2}) \cdots (X - a_{k_m}) \in \mathbb{Q}[X]$. But $f(X)$ is an irreducible polynomial of degree n containing the same roots. Thus, $m = n$, and so $N(j(X, \lambda, a))$ is irreducible in $\mathbb{Q}[X, \lambda]$. Since $N(h(X, \lambda, a))$ is merely $N(j(X, \lambda, a))$, replacing X with X/λ, we have that $N(h(X, \lambda, a))$ is also irreducible in $\mathbb{Q}[X, \lambda]$.

□

Let us use this proposition to see whether the polynomial $g(X) = -3 + a^2 + a\,X + X^2$ factors in $\mathbb{Q}(a)[X]$.

```
g /. X -> X - L a
```

$$-3 + a^2 + a\,(-a\,L + X) + (-a\,L + X)^2$$

```
h = Norm[%, a]
```

$$1 - 3\,L - 21\,L^2 + 47\,L^3 - 21\,L^4 - 3\,L^5 + L^6 + 6\,X - 15\,L\,X + 6\,L^2\,X + 6\,L^3\,X - 15\,L^4\,X + 6\,L^5\,X + 9\,X^2 - 18\,L\,X^2 + 27\,L^2\,X^2 - 18\,L^3\,X^2 + 9\,L^4\,X^2 - 2\,X^3 + 3\,L\,X^3 + 3\,L^2\,X^3 - 2\,L^3\,X^3 - 6\,X^4 + 6\,L\,X^4 - 6\,L^2\,X^4 + X^6$$

```
Factor[h]
```

$$\left(1 + 3\,L - 6\,L^2 + L^3 + 3\,X - 3\,L\,X + 3\,L^2\,X - X^3\right)\left(1 - 6\,L + 3\,L^2 + L^3 + 3\,X - 3\,L\,X + 3\,L^2\,X - X^3\right)$$

We find that $-3 + a^2 + a\,X + X^2$ indeed factors in $\mathbb{Q}(a)[X]$. Is there a way to use this factorization to find the original factors of$g(X)$? In a sense we must "un-norm" each of the factors of $h(X)$. Because we left λ unspecified, not only is this doable, but it can be done by solving linear equations. The key lies in penultimate powers of λ in equation (**). The package "galois.m" contains a function **UnNorm** which can quickly determine what the original factorization must be.

```
UnNorm[%, L, X, a]
```

$$\left(2 + a - a^2 + X\right)\left(-2 + a^2 + X\right)$$

Indeed, this gives us a way of factoring any polynomial in $\mathbb{Q}$(a). The package "galois.m" expands the **Factor** command to allow factoring in the field $\mathbb{Q}$(a). For example, we can factor the polynomial $X^3 - 3\,X - 1$ in $\mathbb{Q}(a)$ as follows:

```
Factor[X^3 - 3 X - 1, a]
```

$$(-a + X)\left(2 + a - a^2 + X\right)\left(-2 + a^2 + X\right)$$

3. Splitting Fields

We can try the same procedure on other polynomials to see if they behave the same way. Let us consider the polynomial $X^3 - 2$, whose extension field would be $\mathbb{Q}\left(\sqrt[3]{2}\right)$.

```
ClearDefs
```

```
Define[a^3, 2]
```

```
Factor[X^3 - 2, a]
```

$$(-a + X)\left(a^2 + a\,X + X^2\right)$$

The **ClearDefs** command erases the definition of the variables in **UsedSymbols**, allowing us to reuse the variable a. Notice that the polynomial $X^3 - 2$ did not factor completely as $X^3 - 3\,X - 1$ did. The explanation is that $X^3 - 2$ has complex roots, while $\mathbb{Q}\left(\sqrt[3]{2}\right)$ contains only real numbers. But we can fix this problem by defining a new variable b to be a root of the quadratic factor $a^2 + a\,X + X^2$.

```
Define[b^2, - a^2 - a b]
```

We now have defined an "extention of an extention." In order to factor the polynomial in the field $\mathbb{Q}(a, b)$, we

will apply a shortcut. We will use the following theorem found in many abstract algebra books.

- **Theorem 3.1**
  Let F be a field of characteristic 0 (such as $\mathbb{Q}$). Then if $K = F(a_1, a_2, \ldots, a_n)$ is an algebraic extension of F, then $K = F(c)$ for some c in K.

See [2, p. 297] or [3, p. 479] for a detailed proof. The basic idea behind the proof is to show that there are only a finite number of values of λ for which $\mathbb{Q}(\lambda a + b) \neq \mathbb{Q}(a, b)$. Thus, *Mathematica* can use a trial and error method to find a suitable value of λ. The function **SimpleExtension** selects a value c which fulfills theorem 3.1.

```
SimpleExtension[a, b]
```

```
2 a + b
```

Mathematica can now factor a polynomial in the field $\mathbb{Q}(a, b) = \mathbb{Q}(2a + b)$ using the same procedure as with a simple extention.

```
Factor[X^3 - 2, a, b]
```

```
(-a + X) (-b + X) (a + b + X)
```

Thus, we see that by defining an extention of an extention, we have succeeded in getting the polynomial to factor completely. We define the *splitting field* of a polynomial to be the smallest extention of $\mathbb{Q}$ for which the polynomial "splits completely" in this mannor. Therefore,
the splitting field of $X^3 - 2$ is $\mathbb{Q}(a, b)$, which is a six dimensional extension of $\mathbb{Q}$.

Let us try a more complicated example, $X^5 - X + 1$, which demonstrates*Mathematica*'s capacity and speed.

```
ClearDefs
```

```
Define[a^5, a - 1]
```

```
Factor[X^5 - X + 1, a]
```

```
(-a + X) (-1 + a^4 + a^3 X + a^2 X^2 + a X^3 + X^4)
```

```
Define[b^4, 1 - a^4 - a^3 b - a^2 b^2 - a b^3]
```

```
Factor[X^5 - X + 1, a, b]
```

```
(-a + X) (-b + X) (a^3 + a^2 b + a b^2 + b^3 + a^2 X + a b X + b^2 X + a X^2 + b X^2 + X^3)
```

```
Define[c^3, - a^3 - a^2 b - a b^2 - b^3 - a^2 c - a b c - b^2 c - a c^2 - b c^2]
```

```
Factor[X^5 - X + 1, a, b, c]
```

```
(-a + X) (-b + X) (-c + X) (a^2 + a b + b^2 + a c + b c + c^2 + a X + b X + c X + X^2)
```

```
Define[d^2, -a^2 - a b - b^2 - a c - b c - c^2 - a d - b d - c d]
```

```
Factor[X^5 - X + 1, a, b, c, d]
```

```
(-a + X) (-b + X) (-c + X) (-d + X) (a + b + c + d + X)
```

Notice we had to make four extentions before the polynomial finally split. Thus, the splitting field for this polynomial has $5 \cdot 4 \cdot 3 \cdot 2 = 120$ dimensions. This is obviously the maximum number of dimensions for a splitting field of a fifth degree polynomial.

4. Field Automorphisms

Once we have defined the splitting field for a polynomial, we can ask what automorphisms exist on this field. It is not hard to prove that the automorphisms must send one root of the polynomial to another root. (See [1, p. 282].) Furthermore, the automorphism will be completely determined by where the automorphism sends the roots of the polynomial. Thus, we can view any automorphism on the splitting field as a permutation of

the roots of the polynomial.

How can we determine whether a given permutation of the roots represents an automorphism? We can have *Mathematica* help us! Let us choose the polynomial $X^5 - 5X + 12$ to illustrate the process.

```
ClearDefs
```

```
Define[a^5, 5 a - 12]
```

```
Factor[X^5 - 5 X + 12, a]
```

$$(-a+X)\left(2-\frac{5a}{4}-\frac{a^2}{4}-\frac{a^3}{4}-\frac{a^4}{4}+X+\frac{3aX}{4}-\frac{a^2X}{4}-\frac{a^3X}{4}-\frac{a^4X}{4}+X^2\right)$$
$$\left(-1-\frac{a}{2}-\frac{a^3}{2}-X+\frac{aX}{4}+\frac{a^2X}{4}+\frac{a^3X}{4}+\frac{a^4X}{4}+X^2\right)$$

We can let *b* be a root of the last factor, and try the factorization again.

```
Define[b^2, 1 + a / 2 + a^3 / 2 + b - a b / 4 - a^2 b / 4 - a^3 b / 4 - a^4 b / 4]
```

```
Factor[X^5 - 5 X + 12, a, b]
```

$$(-a+X)\,(-b+X)\left(-1+\frac{a}{4}+\frac{a^2}{4}+\frac{a^3}{4}+\frac{a^4}{4}+b+X\right)$$
$$\left(\frac{3}{2}+\frac{a}{4}-\frac{a^2}{4}-\frac{a^3}{4}-\frac{a^4}{4}-\frac{b}{2}-\frac{ab}{2}+X\right)\left(-\frac{1}{2}+\frac{a}{2}+\frac{b}{2}+\frac{ab}{2}+X\right)$$

It is natural to label the three other roots of this polynomial as *c*, *d*, and *e*.

```
c = 1 - a / 4 - a^2 / 4 - a^3 / 4 - a^4 / 4 - b;
```

```
d = -3 / 2 - a / 4 + a^2 / 4 + a^3 / 4 + a^4 / 4 + b / 2 + a b / 2;
```

```
e = 1 / 2 - a / 2 - b / 2 - a b / 2;
```

In order to define an automorphism on this splitting field, we only have to define where *a* and *b* are sent to, and the other three roots will follow suit. It is easy to define a homomorphism in *Mathematica*. The following creates the command **Homomorph[F]** which defines *F* to be a homomorphism.

```
Homomorph[F_Symbol] := Module[{a, b},
        UsedSymbols = Union[UsedSymbols, {F}];
        ClearAll[F];
        F[a_ b_] := FixedPoint[Expand, F[a] F[b]];
        F[a_ + b_] := F[a] + F[b];
        F[a_^b_Integer] := FixedPoint[Expand, F[a]^b];
        F[a_Integer] := a;
        F[a_Rational] := a;]
```

For example, we can easily define a homomorphism which sends *a* to *b*, and sends *b* back to *a*.

```
Homomorph[F]
```

```
F[a] := b
```

```
F[b] := a
```

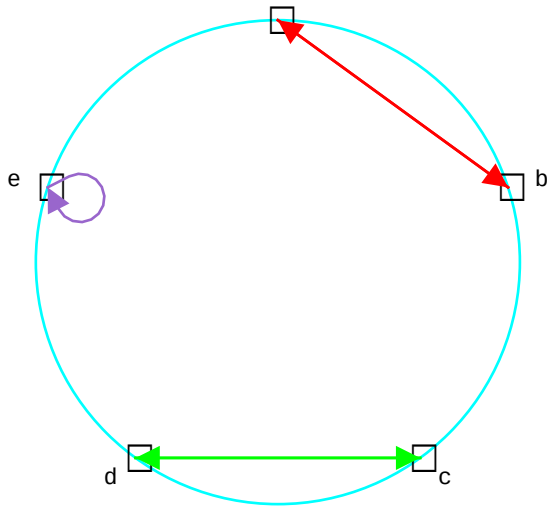
The command **CheckHomo** in the package "galois.m" can confirm for us that this is indeed a homomorphism on $\mathbb{Q}(a, b)$.

```
CheckHomo[F, {a, b}]
```

```
True
```

We can also have *Mathematica* graph this homomorphism on the set of five roots.

```
CircleGraph[{a, b, c, d, e}, F];
```



Not every choice of $F[a]$ and $F[b]$ will produce an automorphism;

```
Homomorph[F]
```

```
F[a] := b
```

```
F[b] := c
```

```
CheckHomo[F, {a, b}]
```

```
f[b] * f[b] is not equal to f[b*b]
```

```
False
```

yet it is not hard to find automorphisms that do work. These become theelements of the Galois group. Thus, *Mathematica* allows us to visualize the different automorphisms of the Galois group of the polynomial. Here is another example.

```
Homomorph[F]
```

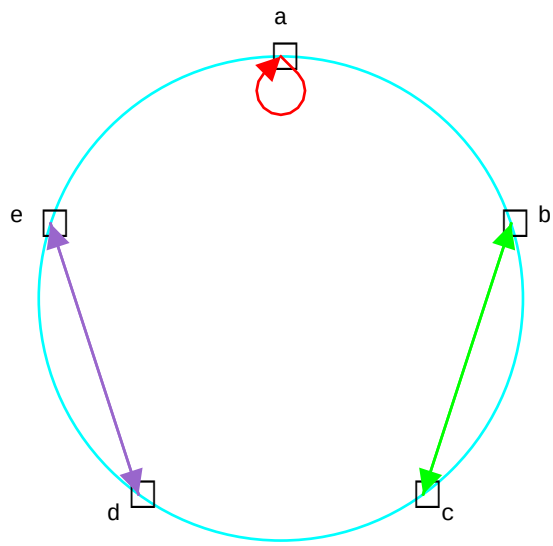
```
F[a] := a
```

```
F[b] := c
```

```
CheckHomo[F, {a, b}]
```

```
True
```

```
CircleGraph[{a, b, c, d, e}, F];
```



From these two elements of the Galois group, we can actually produce the entire Galois group of $X^5 - 5X + 12$. We will develop a quick way to produce these elements in the next section.

5. The Galois Group of a Polynomial

Now that we are able to discover some of the elements of the Galois group, the natural step would be to use these elements to produce the whole Galois group of a polynomial. If we number the roots of the polynomial, we can view each element of the Galois group as a standard permutation.

For example, the roots of the polynomial $X^5 - 5X + 12$ can be numbered $a = 1$, $b = 2$, $c = 3$, $d = 4$, and $e = 5$. Then the two automorphisms discovered in the last section could be viewed as the permutations]

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}.$$

These permutations can be entered into *Mathematica* using only the bottom row of the permutation.

```
P[2, 1, 4, 3, 5]
```

```
P[2, 1, 4, 3]
```

```
P[1, 3, 2, 5, 4]
```

```
P[1, 3, 2, 5, 4]
```

Here, the **P** stands for "permutation." Notice that if the last number is sent to itself in the permutation, it is omitted to save space. We can multiply two permutations using `CenterDot` for the non-commutative multiplication.

```
P[2, 1, 4, 3] · P[1, 3, 2, 5, 4]
```

```
P[2, 4, 1, 5, 3]
```

The **Group** command, which was described in [4], is also in the "galios.m" package. Thus, we can find the subgroup of S_5 generated by these two permutations as follows:

```
Group[{P[2, 1, 4, 3], P[1, 3, 2, 5, 4]}]
```

```
{P[], P[2, 1, 4, 3], P[1, 3, 2, 5, 4], P[3, 1, 5, 2, 4], P[2, 4, 1, 5, 3],
 P[4, 2, 5, 1, 3], P[3, 5, 1, 4, 2], P[5, 3, 4, 1, 2], P[4, 5, 2, 3, 1], P[5, 4, 3, 2, 1]}
```

Since the splitting field of $X^5 - 5X + 12$ is 10 dimensional, we would expect the Galois group to have 10 elements. Since *Mathematica* has found 10 elements in the Galois group, we have found all of them.

Which group is this isomorphic to? It is obvious that none of these elements is of order 10. Thus, the group cannot be isomorphic to Z_{10}. The only other group of order 10 is D_5, so this group is isomorphic to D_5. Note that [5] claims the Galois group is F_{20}, which is wrong.

Let us try one more example---the polynomial $X^8 - 24X^6 + 144X^4 - 288X^2 + 144$. We can first note that this polynomial is irreducible over the rational numbers.

```
ClearDefs
```

```
Factor[X^8 - 24 X^6 + 144 X^4 - 288 X^2 + 144]
```

$$144 - 288\,X^2 + 144\,X^4 - 24\,X^6 + X^8$$

We can define a to be a root of this polynomial, and factor it over $\mathbb{Q}(a)$.

```
Define[a^8, 24 a^6 - 144 a^4 + 288 a^2 - 144]
```

```
Factor[X^8 - 24 X^6 + 144 X^4 - 288 X^2 + 144, a]
```

$$(-a + X)\,(a + X)\left(-3\,a + \frac{3\,a^3}{2} - \frac{a^5}{12} + X\right)\left(3\,a - \frac{3\,a^3}{2} + \frac{a^5}{12} + X\right)\left(10\,a - \frac{17\,a^3}{2} + \frac{11\,a^5}{6} - \frac{a^7}{12} + X\right)$$
$$\left(-a - \frac{5\,a^3}{2} + \frac{5\,a^5}{6} - \frac{a^7}{24} + X\right)\left(a + \frac{5\,a^3}{2} - \frac{5\,a^5}{6} + \frac{a^7}{24} + X\right)\left(-10\,a + \frac{17\,a^3}{2} - \frac{11\,a^5}{6} + \frac{a^7}{12} + X\right)$$

As we can see, the polynomial factors completely in $\mathbb{Q}(a)$. The roots can be given as $\pm a$, $\pm b$, $\pm c$, and $\pm d$, where

```
b = a + 5 a^3 / 2 - 5 a^5 / 6 + a^7 / 24;
```

```
c = 3 a - 3 a^3 / 2 + a^5 / 12;
```

```
d = 10 a - 17 a^3 / 2 + 11 a^5 / 6 - a^7 / 12;
```

which are all expressed in terms of a. Thus, an automorphism of the splitting field will be completely determined by which root a is sent to. Suppose that a is sent to b.

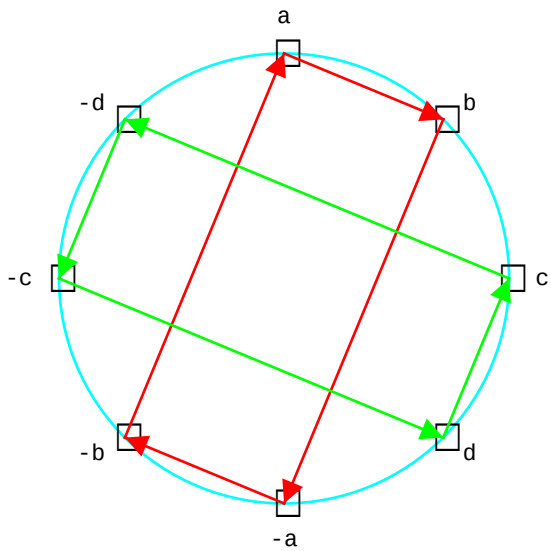
```
Homomorph[F]
```

```
F[a] := b
```

```
CheckHomo[F, {a}]
```

```
True
```

```
CircleGraph[{a, b, c, d, -a, -b, -c, -d}, F];
```



We can also consider a homomorphism which sends *a* to *c*.

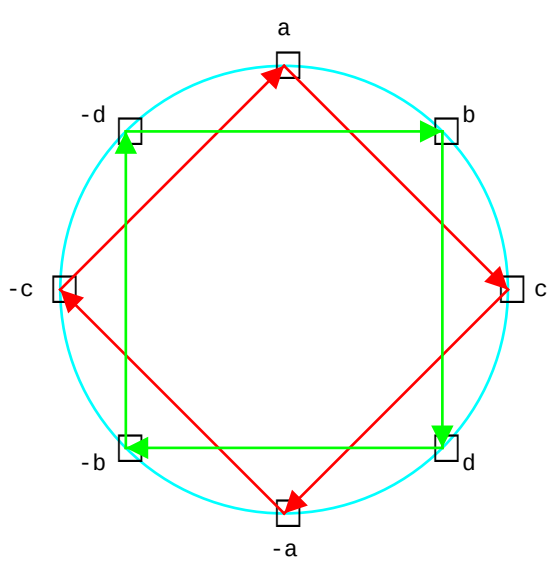
```
Homomorph[F]
```

```
F[a] := c
```

```
CheckHomo[F, {a}]
```

```
True
```

```
CircleGraph[{a, b, c, d, -a, -b, -c, -d}, F];
```



If we lable the roots of the polynomial in the order that they appear in these circle graphs, we find that the first permutation of the roots corresponds to the permutation **P[2,5,8,3,6,1,4,7]**, while the second automorphism can be expressed by the permutation **P[3,4,5,6,7,8,1,2]**. Hence, we can find more automorphisms by considering the group generated by these two elements.

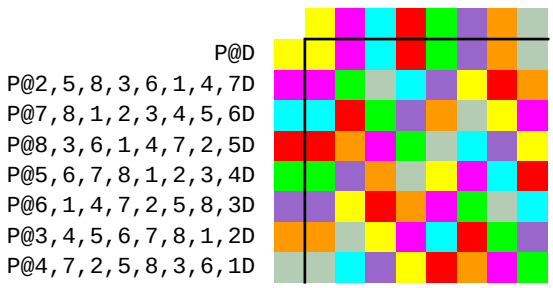
```
G = Group[{P[2, 5, 8, 3, 6, 1, 4, 7], P[3, 4, 5, 6, 7, 8, 1, 2]}]
```

```
{P[], P[2, 5, 8, 3, 6, 1, 4, 7], P[7, 8, 1, 2, 3, 4, 5, 6],
 P[8, 3, 6, 1, 4, 7, 2, 5], P[5, 6, 7, 8, 1, 2, 3, 4],
 P[6, 1, 4, 7, 2, 5, 8, 3], P[3, 4, 5, 6, 7, 8, 1, 2], P[4, 7, 2, 5, 8, 3, 6, 1]}
```

The package "galois.m" also includes a command **MultTable** which allows us to see the Cayley table of this

group of permutations.

```
MultTable[G];
```



Mathematica uses a color code for the elements, which is shown here as shading. By comparing this table with the 5 known groups of order 8, we see that the Galois group of $X^8 - 24\,X^6 + 144\,X^4 - 288\,X^2 + 144$ is
isomorphic to the quaternionic group, Q_8. Hence, we can use *Mathematica* to find the Galois groups of fairly complicated polynomials.

By having a visualization of the Galois groups, students have an easier time grasping the fundemental theorem of Galois theory. From this point, it is not hard for the students to learn the many consequences of Galois theory, such as the insolvability of fifth degree polynomials in terms of radicals.

6. References

[1] Goldstein, L. J., Abstract Algebra, a first course,
(Prentice-Hall, Englewood Cliffs, New Jersey), 1973.

[2] Hungerford, T. W., Abstract Algebra, An Introduction,
(Saunders College Publishing, Philadelphia), 1990.

[3] Malik, Mordeson, and Sen, Fundamentals of Abstract Algebra,
(McGraw-Hill, New York), 1997.

[4] Paulsen, William H., Group Presentations Using *Mathematica*,
Mathematica in Education and Research, **4** :4 (Fall 1995), pp.21-24.

[5] Wolfram Reseach, Inc., *Solving the Quintic with Mathematica*, Poster, December, 1994,
¬http://www.mathsource.com/cgi-bin/MathSource/Applications/Mathematics/0207-122.

■ ABOUT THE AUTHOR

William Paulsen is an associate professor at Arkansas State University. He earned his Ph.D. from Washington University in St. Louis. Although his main field of research is applied mathematics, he has used *Mathematica* for a variety of unusual applications. He has recently completed a two volume text, "Interactive Group Theory" and "Interactive Ring Theory" which uses a set of *Mathematica* courseware to cover a two semester modern algebra course. In fact, this paper demonstrates how the last chapter on Galois groups

was implemented into *Mathematica*. The two volume text has yet to be accepted for publication.

William Paulsen
Department of Mathematics and Computer Science
P. O. Box 70
State University, AR 72467
wpaulsen@caddo.astate.edu

■ ELECTRONIC SUBSCRIPTIONS

Included in the distribution for each electronic subscription are the files `galois.m` and `GalComp.nb` containing *Mathematica* code for the material described in this article.