Galois Theory: The Conjugate Trick

Everyone learns the "conjugate trick" in highschool algebra. This allows one to compute inverses of complex numbers and to rationalize expressions of the form: $\frac{1+\sqrt{5}}{2+3\sqrt{5}}$.

It turns out that this "trick" is really part of a bigger picture and has a far reaching extension. Here are a few demonstrations of the old trick and then its generalization.

```
> # clear memory and load PolynomialTools so we have the
  MinimalPolynomial command.
  restart;
  with(PolynomialTools):
```

Example 1: Compute the inverse of $A = 3 + 4\,i$.

The Galois group of the complex numbers over the real numbers has two elements: the identity map and the conjugate map. Thus the element $3 + 4\,i$ has two conjugates: itself and $3 - 4\,i$.

```
> A := 3+4*I;
  B := 3-4*I;
```

$$A := 3 + 4\,\mathrm{I}$$
$$B := 3 - 4\,\mathrm{I} \qquad (1)$$

The norm of A is the product of itself and all of its conjugates.

```
> NormA := A*B;
```

$$NormA := 25 \qquad (2)$$

This means that $\frac{A\cdot(\textit{all the rest of A's conjugates})}{Norm(A)} = 1$. In other words, $\frac{1}{A} = \frac{\textit{all other conjugates}}{Norm(A)}$

```
> Ainverse := B/NormA;
```

$$Ainverse := \frac{3}{25} - \frac{4\,\mathrm{I}}{25} \qquad (3)$$

Let's check this out...

```
> A * Ainverse;
```

$$1 \qquad (4)$$

Example 2: Simplify $\frac{B}{A} = \frac{1+\sqrt{5}}{2+3\sqrt{5}}$.

To simplify $\frac{B}{A}$ (i.e. rationalize this expression) we are taught to multiply the top and bottom by the "conjugate" of A.

Why does this work?

Let $C = 2 - 3\sqrt{5}$ (the conjugate of A). Then $A \cdot C = Norm(A)$ since the only conjugates of A are itself and C. This is the case because the Galois group of $\mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$ has exactly two elements: the identity map and the map that sends $a + b\sqrt{5}$ to $a - b\sqrt{5}$. Since the norm of an element of a Galois extension (our extension is the splitting field of $x^2 - 5$ so it's Galois) lies in the base field, we must have that $Norm(A) = A \cdot C$ is a rational number (in fact it's an integer).

Therefore, $\frac{B}{A} = \frac{B \cdot C}{A \cdot C} = \frac{B \cdot C}{Norm(A)}$ is an element of $\mathbb{Q}(\sqrt{5})$ divided by a rational number (so B/A has been rationalized).

```
> B := 1+sqrt(5);
  A := 2+3*sqrt(5);

  'B'/'A' = B/A;
```

$$B := \sqrt{5} + 1$$

$$A := 2 + 3\sqrt{5}$$

$$\frac{B}{A} = \frac{\sqrt{5} + 1}{2 + 3\sqrt{5}} \quad \textbf{(5)}$$

```
> C := 2-3*sqrt(5);

  NormA := simplify(A*C);

  'B'/'A' = expand(simplify(B*C/NormA));
```

$$C := 2 - 3\sqrt{5}$$

$$NormA := -41$$

$$\frac{B}{A} = \frac{13}{41} + \frac{\sqrt{5}}{41} \quad \textbf{(6)}$$

We could use Maple's built in command "rationalize" to get the same result:

```
> expand(rationalize(B/A));
```

$$\frac{13}{41} + \frac{\sqrt{5}}{41} \quad \textbf{(7)}$$

Example 3: Let's compute the inverse of $A = 2 + 3 \cdot 2^{\frac{1}{3}} + 2^{\frac{2}{3}}$ using the Galois conjugate "trick". [Note: This is the same element we rationalized in our "factorization handout".]

This example is more complicated. We are now dealing with a root of $x^3 - 2$. We know that the splitting field (over the rationals) for this polynomial is $\mathbb{Q}(\alpha, \omega \cdot \alpha, \omega^2 \cdot \alpha)$ where ω is a primitive 3rd root of unity and $\alpha = 2^{\frac{1}{3}}$.

```
> A := 2+3*2^(1/3)+1*2^(2/3);

  "The roots of x^3-2 are ", solve(x^3-2=0);
```

```
omega := (-1+sqrt(-3))/2;
alpha := 2^(1/3);
```

$$A := 2 + 3\,2^{1/3} + 2^{2/3}$$

$$\text{"The roots of x^3-2 are "}, 2^{1/3}, -\frac{2^{1/3}}{2} + \frac{I\sqrt{3}\,2^{1/3}}{2}, -\frac{2^{1/3}}{2} - \frac{I\sqrt{3}\,2^{1/3}}{2}$$

$$\omega := -\frac{1}{2} + \frac{I\sqrt{3}}{2}$$

$$\alpha := 2^{1/3} \tag{8}$$

The roots of $x^3 - 2$ (consider these as roots 1, 2, and 3):

```
> 'alpha' = alpha;
  'omega'*'alpha' = expand(omega*alpha);
  'omega^2'*'alpha' = expand(omega^2*alpha);
```

$$\alpha = 2^{1/3}$$

$$\omega\,\alpha = -\frac{2^{1/3}}{2} + \frac{I\sqrt{3}\,2^{1/3}}{2}$$

$$\omega^2\,\alpha = -\frac{2^{1/3}}{2} - \frac{I\sqrt{3}\,2^{1/3}}{2} \tag{9}$$

The Galois group of this splitting field (over the rationals) is isomorphic to the symmetric group S_3. Thus our element A will have $|S_3| = 3! = 6$ conjugates (including itself).

We know that the Galois group permutes our 3 roots. Since all permutations are allowed, it's not too hard to write down what happens.

We are going to be permuting our roots. For example, we might send α to $\omega\cdot\alpha$, $\omega\cdot\alpha$ to α, and $\omega^2\cdot\alpha$ to itself. To aid with our computation, let's call the α root x, the $\omega\cdot\alpha$ root y, and the $\omega^2\cdot\alpha$ root z. This means that our element A is...

```
> Ax := 2+3*x+1*x^2;
```

$$Ax := x^2 + 3\,x + 2 \tag{10}$$

So in reality A is the result of plugging α into x in Ax.

```
> 'A' = subs(x=alpha,Ax);
```

$$A = 2 + 3\,2^{1/3} + 2^{2/3} \tag{11}$$

Now let's compute all 6 conjugates...

[I've labeled them according to how I've permuted the roots. For example: A123 is the result of sending root 1 to 2, 2 to 3, and 3 to 1.]

```
> A1   := subs(x=alpha,y=omega*alpha,z=omega^2*alpha, Ax);
  A12  := subs(y=alpha,x=omega*alpha,z=omega^2*alpha, Ax);
  A13  := subs(z=alpha,y=omega*alpha,x=omega^2*alpha, Ax);
  A23  := subs(x=alpha,z=omega*alpha,y=omega^2*alpha, Ax);
```

```
A123 := subs(z=alpha,x=omega*alpha,y=omega^2*alpha, Ax);
A132 := subs(y=alpha,z=omega*alpha,x=omega^2*alpha, Ax);
```

$$A1 := 2 + 3\,2^{1/3} + 2^{2/3}$$

$$A12 := \left(-\frac{1}{2} + \frac{I\sqrt{3}}{2}\right)^2 2^{2/3} + 3\left(-\frac{1}{2} + \frac{I\sqrt{3}}{2}\right) 2^{1/3} + 2$$

$$A13 := \left(-\frac{1}{2} + \frac{I\sqrt{3}}{2}\right)^4 2^{2/3} + 3\left(-\frac{1}{2} + \frac{I\sqrt{3}}{2}\right)^2 2^{1/3} + 2$$

$$A23 := 2 + 3\,2^{1/3} + 2^{2/3}$$

$$A123 := \left(-\frac{1}{2} + \frac{I\sqrt{3}}{2}\right)^2 2^{2/3} + 3\left(-\frac{1}{2} + \frac{I\sqrt{3}}{2}\right) 2^{1/3} + 2$$

$$A132 := \left(-\frac{1}{2} + \frac{I\sqrt{3}}{2}\right)^4 2^{2/3} + 3\left(-\frac{1}{2} + \frac{I\sqrt{3}}{2}\right)^2 2^{1/3} + 2 \quad \textbf{(12)}$$

The $Norm(A)$ is the product of all of the conjugates. Since the norm is fixed by all of the Galois group elements, it must lie in the base (fixed) field. Thus the norm must be rational (in our case it's actually an integer).

```
> NormA := simplify(A1*A12*A13*A23*A123*A132);
```

$$NormA := 900 \quad \textbf{(13)}$$

Finally, $\frac{1}{A}$ must be the product of all of the conjugates of A (except itself) then divided by $Norm(A)$...

```
> Ainverse := expand(simplify(A12*A13*A23*A123*A132/simplify(NormA)));
```

$$Ainverse := -\frac{2\,2^{1/3}}{15} - \frac{1}{15} + \frac{7\,2^{2/3}}{30} \quad \textbf{(14)}$$

Drum roll please...

```
> simplify(A*Ainverse);
```

$$1 \quad \textbf{(15)}$$

It works!

Ok. That's a lot of work. And, no, I wouldn't want to do it by hand. But that maybe explains why your highschool algebra class doesn't cover the "conjugate of the cube root of 2 trick".

Of course, Maple can just do this for us with its built in command...

```
> 1/A = rationalize(1/A);
```

$$\frac{1}{2 + 3\,2^{1/3} + 2^{2/3}} = -\frac{2\,2^{1/3}}{15} - \frac{1}{15} + \frac{7\,2^{2/3}}{30} \quad \textbf{(16)}$$

One final note about this example: Our calculation leaves the realm of real numbers. But that's ok. We know that the answer $\frac{1}{A}$ lies in the field $\mathbb{Q}\left(2^{\frac{1}{3}}\right)$ so it must be real. Thus in the end all of our complex stuff **must** cancel out (as it does).

Example 4: Let's compute the inverse of $A = 5\sqrt{2+\sqrt{2}} - 3\sqrt{2-\sqrt{2}}$ using the Galois conjugate "trick".

```
> A := 5*sqrt(2+sqrt(2))-3*sqrt(2-sqrt(2));
```

$$A := 5\sqrt{2+\sqrt{2}} - 3\sqrt{2-\sqrt{2}} \quad \textbf{(17)}$$

These elements are roots of the polynomial:

```
> expand((x-sqrt(2+sqrt(2)))*(x+sqrt(2+sqrt(2)))*(x-sqrt(2-sqrt(2)))*(x+
  sqrt(2-sqrt(2))));
```

$$x^4 - 4x^2 + 2 \quad \textbf{(18)}$$

Deriving the Galois Group:

It shouldn't be difficult to see that $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt{2+\sqrt{2}}] = \mathbb{Q}[\sqrt{2+\sqrt{2}}, -\sqrt{2+\sqrt{2}}, \sqrt{2-\sqrt{2}}, -\sqrt{2-\sqrt{2}}]$ is a radical tower building up the splitting field of our above polynomial.

[Note: $\left(\sqrt{2+\sqrt{2}}\right)^2 - 2 = \sqrt{2}$ shows that $\mathbb{Q}[\sqrt{2}]$ is an intermediate field. Also while not obvious, it is the case that $\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = \sqrt{2-\sqrt{2}}$ and so once we have $\sqrt{2+\sqrt{2}}$ we have all of the roots.]

The extension $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ has 2 automorphisms: We can send $\sqrt{2}$ to $\pm\sqrt{2}$ (the roots of $x^2 - 2$). Let's call these maps $\varphi_{\pm}$.

These maps can then be extended to the splitting field. The identity, φ_+, can send $\sqrt{2+\sqrt{2}}$ to $\pm\sqrt{2+\sqrt{2}}$ (the roots of $x^2 - (2+\sqrt{2})$). Let's call these maps $\psi_{+,\pm}$.

The other map, φ_-, can also be extended in two ways. Here we need to be careful. We can send $\sqrt{2+\sqrt{2}}$ (a root of $x^2 - (2+\sqrt{2})$) to a root of $\varphi_-^*(x^2 - (2+\sqrt{2})) = x^2 - (2-\sqrt{2})$, so $\sqrt{2+\sqrt{2}}$ can map to $\pm\sqrt{2-\sqrt{2}}$. Let's call these maps $\psi_{-,\pm}$.

Therefore, the Galois of group of $\mathbb{Q}[\sqrt{2+\sqrt{2}}]$ has 4 elements: $\psi_{\pm,\pm}$. Alternatively, we could note that $\mathbb{Q}[\sqrt{2+\sqrt{2}}]$ is a Galois extension (since it's a splitting field) of degree 4 and thus the Galois group has 4 elements.

At this point there are two possibilities: our Galois group is either the Klein 4-group or it is cyclic (order 4).

Let's label the roots: $\sqrt{2+\sqrt{2}}$, $-\sqrt{2+\sqrt{2}}$, $\sqrt{2-\sqrt{2}}$, and $-\sqrt{2-\sqrt{2}}$ as roots 1,2,3, and 4 and see what permutations our Galois group elements correspond to.

First, obviously $\psi_{+,+} = (1)$ is the identity. Next, we consider $\psi_{+,-}$. This map sends $\sqrt{2+\sqrt{2}}$ to -$\sqrt{2+\sqrt{2}}$ (i.e., root 1 to root 2). Likewise, it must send root 2 back to root 1. Next, notice that $-\sqrt{2+\sqrt{2}} \cdot \psi_{+,-}\left(\sqrt{2-\sqrt{2}}\right) = \psi_{+,-}\left(\sqrt{2+\sqrt{2}}\right)\psi_{+,-}\left(\sqrt{2-\sqrt{2}}\right) = \psi_{+,-}\left(\sqrt{2+\sqrt{2}} \cdot \sqrt{2-\sqrt{2}}\right) = \psi_{+,-}\left(\sqrt{(2+\sqrt{2})(2-\sqrt{2})}\right) = \psi_{+,-}\left(\sqrt{2}\right) = \sqrt{2}$. Thus $-\sqrt{2+\sqrt{2}} \cdot \psi_{+,-}\left(\sqrt{2-\sqrt{2}}\right) = \sqrt{2}$. This implies that $\psi_{+,-}\left(\sqrt{2-\sqrt{2}}\right) = -\sqrt{2-\sqrt{2}}$. Therefore, we have that root 3 maps to root 4. Likewise, root 4 must map to root 3. Therefore, $\psi_{+,-} = (12)(34)$.

Now consider the map $\psi_{-,+}$ where $\psi_{-,+}\left(\sqrt{2}\right) = -\sqrt{2}$ and $\psi_{-,+}\left(\sqrt{2+\sqrt{2}}\right) = \sqrt{2-\sqrt{2}}$. Thus we send root 1 to root 3. Keeping in mind that automorphisms are the identity map on rational numbers (or that they preserve additive inverses), we also have $\psi_{-,+}\left(-\sqrt{2+\sqrt{2}}\right) = -\sqrt{2-\sqrt{2}}$ so that root 2 maps to root 4. Now for a calculation similar to one we did for $\psi_{+,-}$. Notice that $-\sqrt{2-\sqrt{2}} \cdot \psi_{-,+}\left(\sqrt{2-\sqrt{2}}\right) = \psi_{-,+}\left(\sqrt{2+\sqrt{2}}\right)\psi_{-,+}\left(\sqrt{2-\sqrt{2}}\right) = \psi_{-,+}\left(\sqrt{2+\sqrt{2}} \cdot \sqrt{2-\sqrt{2}}\right) = \psi_{-,+}\left(\sqrt{(2+\sqrt{2})(2-\sqrt{2})}\right) = \psi_{-,+}\left(\sqrt{2}\right) = -\sqrt{2}$. Thus $-\sqrt{2-\sqrt{2}} \cdot \psi_{-,+}\left(\sqrt{2-\sqrt{2}}\right) = -\sqrt{2}$. Therefore, $\psi_{-,+}\left(\sqrt{2-\sqrt{2}}\right) = \sqrt{2+\sqrt{2}}$. Therefore, we have that root 3 maps to root 2. This then also implies that root 4 maps to root 1. We have just demonstrated that $\psi_{-,+}\left(\sqrt{2-\sqrt{2}}\right) = (1324)$.

Finally, a simliar argument shows that $\psi_{-,-} = (1423)$. Therefore, our Galois group is cyclic (order 4) and is represented by the permutation: {(1), (12)(34), (1324), (1423)}.

We now compute the conjugates of A. As before we will label roots 1, 2, 3, and 4 by x, y, z, and w. Then we create an "abstract" version of A called Ax. Finally, we apply all elements of the Galois group in order to compute the conjugates of A. For example, the permutation (1324) applied to A will be called "A1324".

```
> Ax := 5*x-3*z;

  R1 :=  sqrt(2+sqrt(2));
  R2 := -sqrt(2+sqrt(2));
  R3 :=  sqrt(2-sqrt(2));
  R4 := -sqrt(2-sqrt(2));

  A1 := subs(x=R1, y=R2, z=R3, w=R4, Ax);
  A1234 := subs(x=R2, y=R1, z=R4, w=R3, Ax);
  A1324 := subs(x=R4, y=R3, z=R1, w=R2, Ax);
  A1423 := subs(x=R3, y=R4, z=R2, w=R1, Ax);

  NormA := simplify(A1*A1234*A1324*A1423);

  Ainverse := simplify(A1234*A1324*A1423/NormA);
```

$$Ax := 5x - 3z$$

$$R1 := \sqrt{2+\sqrt{2}}$$

$$R2 := -\sqrt{2+\sqrt{2}}$$

$$R3 := \sqrt{2-\sqrt{2}}$$

$$R4 := -\sqrt{2-\sqrt{2}}$$

$$A1 := 5\sqrt{2+\sqrt{2}} - 3\sqrt{2-\sqrt{2}}$$

$$A1234 := -5\sqrt{2+\sqrt{2}} + 3\sqrt{2-\sqrt{2}}$$

$$A1324 := -5\sqrt{2-\sqrt{2}} - 3\sqrt{2+\sqrt{2}}$$

$$A1423 := 5\sqrt{2-\sqrt{2}} + 3\sqrt{2+\sqrt{2}}$$

$$NormA := 4232$$

$$Ainverse := \frac{(4\sqrt{2}+3)\sqrt{2-\sqrt{2}}}{46} \quad \textbf{(19)}$$

We get that $\frac{1}{A} = \frac{1}{5\sqrt{2+\sqrt{2}} - 3\sqrt{2-\sqrt{2}}} = \frac{3}{46}\sqrt{2-\sqrt{2}} + \frac{2}{23}\sqrt{2}\cdot\sqrt{2-\sqrt{2}}$

Consider that $\left\{1, \sqrt{2}, \sqrt{2+\sqrt{2}}, \sqrt{2}\cdot\sqrt{2+\sqrt{2}}\right\}$ is a basis for our splitting fields over the rationals (this basis can be built from multiplying bases coming from the radical tower used to build our automorphisms). To rewrite A's inverse in terms of our basis we simply notice that $\sqrt{2}\cdot\sqrt{2-\sqrt{2}} = 2\sqrt{2+\sqrt{2}} - \sqrt{2}\cdot\sqrt{2+\sqrt{2}}$ and $\sqrt{2-\sqrt{2}} = -\sqrt{2+\sqrt{2}} + \sqrt{2}\cdot\sqrt{2+\sqrt{2}}$.

Thus

$$\frac{1}{A} = \frac{1}{5\sqrt{2+\sqrt{2}} - 3\sqrt{2-\sqrt{2}}} = \frac{3}{46}\left(-\sqrt{2+\sqrt{2}} + \sqrt{2}\cdot\sqrt{2+\sqrt{2}}\right) + \frac{2}{23}\left(2\sqrt{2+\sqrt{2}} - \sqrt{2}\cdot\sqrt{2+\sqrt{2}}\right) = \frac{5}{46}\sqrt{2+\sqrt{2}} - \frac{1}{46}\sqrt{2}\cdot\sqrt{2+\sqrt{2}}$$

```
> Ainv := 5/46*sqrt(2+sqrt(2))-1/46*sqrt(2)*sqrt(2+sqrt(2));
  simplify(A*Ainv);
```

$$Ainv := \frac{5\sqrt{2+\sqrt{2}}}{46} - \frac{\sqrt{2}\sqrt{2+\sqrt{2}}}{46}$$

$$1 \quad \textbf{(20)}$$

Maple's rationalize function succeeds in rationalizing A's inverse. However, it gives a quite different (but equivalent) answer:

```
> simplify(rationalize(1/A));
```

$$\frac{\left(3\sqrt{2-\sqrt{2}} + 5\sqrt{2+\sqrt{2}}\right)\left(-16+17\sqrt{2}\right)}{644} \quad \textbf{(21)}$$