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 much bigger picture and has a far reaching extension. Here are a few demonstrations of the old trick and then its generalization.

```
> restart;
```

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;
```

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

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;
```

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

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

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

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

  NormA := simplify(A*C);
```

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

$$NormA := -41 \quad \textbf{(6)}$$

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

$$\frac{B}{A} = \frac{13}{41} + \frac{1}{41}\sqrt{5} \quad \textbf{(7)}$$

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

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

$$\frac{13}{41} + \frac{1}{41}\sqrt{5} \quad \textbf{(8)}$$

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 $\mathbb{Q}\left(2^{\frac{1}{3}}, \omega \cdot 2^{\frac{1}{3}}, \omega^2 \cdot 2^{\frac{1}{3}}\right)$ where ω is a primitive 3rd root of unity. For convenience let's set $\alpha = 2^{\frac{1}{3}}$.

```
> solve(x^3-2=0);
```

$$2^{1/3}, -\frac{1}{2}2^{1/3} + \frac{1}{2}I\sqrt{3}\,2^{1/3}, -\frac{1}{2}2^{1/3} - \frac{1}{2}I\sqrt{3}\,2^{1/3} \quad (9)$$

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

$$\omega := -\frac{1}{2} + \frac{1}{2}I\sqrt{3} \quad (10)$$

```
> alpha := 2^(1/3);
```

$$\alpha := 2^{1/3} \quad (11)$$

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);
```

$$\alpha = 2^{1/3}, \omega\,\alpha = -\frac{1}{2}2^{1/3} + \frac{1}{2}I\sqrt{3}\,2^{1/3}, \omega^2\,\alpha = -\frac{1}{2}2^{1/3} - \frac{1}{2}I\sqrt{3}\,2^{1/3} \quad (12)$$

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. Before getting started on this, let's see what we're aiming for.

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

$$A := 2 + 3\,2^{1/3} + 2^{2/3} \quad (13)$$

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

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

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;
```

$$Ax := x^2 + 3x + 2 \quad (15)$$

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

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

$$2 + 3\,2^{1/3} + 2^{2/3} = 2 + 3\,2^{1/3} + 2^{2/3} \quad (16)$$

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);
```

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

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

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

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

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

$$A132 := \left(-\frac{1}{2} + \frac{1}{2}\,I\sqrt{3}\right)^4 2^{2/3} + 3\left(-\frac{1}{2} + \frac{1}{2}\,I\sqrt{3}\right)^2 2^{1/3} + 2 \qquad \textbf{(17)}$$

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 field. Thus the norm must be rational (in our case it's actually an integer).

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

$$NormA := 900 \qquad \textbf{(18)}$$

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)))
  ;
```

$$Ainverse := \frac{7}{30}\,2^{2/3} - \frac{2}{15}\,2^{1/3} - \frac{1}{15} \qquad \textbf{(19)}$$

Drum roll please...

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

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

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". :)

One final note: Notice that 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).