Mathematics 466 **Proving a weird root identity** A. Hulpke

To illustrate what one can do with quotient rings, consider the following famous[1] identity. We let

$$A = \sqrt{5} + \sqrt{22 + 2\sqrt{5}}, \qquad B = \sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}}.$$

Numerical evaluation of A and B yields that they are equal to 25 places (to 7.38117594089565797098726 69), so one might suspect that they are in fact equal, but proving this through high school algebra seems daunting, but here is a way of doing it. (I am using GAP to help with the calculations. Once could do so in principle by hand, but factoring polynomials is hard.)
The toold are part of a technique, called *radical denesting*, that is used inside computer algebra systems such as Maple or WolframAlpha.

We start by constructing a suitable field that contains all the roots we need, namely $F = \mathbb{Q}(\sqrt{5}, \sqrt{22 + 2\sqrt{5}}, \sqrt{29})$. It is a subfield of the complex numbers.
We want to construct this field as quotient of the polynomial ring $\mathbb{Q}[x]$ modulo a suitable irreducible polynomial, since this allows us to represent the elements of this field exactly as cosets. Such a polynomial will be built iteratively (not all details show, the method uses a tool called *Resultants*).
The idea is that we first construct a polynomial that has root $\sqrt{5} + \sqrt{29}$, since

$$\sqrt{5} = \frac{1}{48}(\sqrt{5} + \sqrt{29})^3 - \frac{11}{12}(\sqrt{5} + \sqrt{29}), \qquad \sqrt{29} = -\frac{1}{48}(\sqrt{5} + \sqrt{29})^3 + \frac{11}{12}(\sqrt{5} + \sqrt{29}),$$

and $\mathbb{Q}(\sqrt{5} + \sqrt{29})$ thus is a field containing both $\sqrt{5}$ and $\sqrt{29}$.
A suitable polynomial (namely $x^4 - 68x^2 + 576$) can be obtained using the fact that $(\sqrt{5} + \sqrt{29})^2 = 5 + 29 + 2\sqrt{5 \cdot 29}$.
A further (technical, not shown here) iteration gives the polynomial $pol = x^8 - 8x^7 - 196x^6 + 1208x^5 + 8742x^4 - 43224x^3 - 41476x^2 + 227880x + 8609$. We verify that it is irreducible and construct the quotient ring $\mathbb{Q}[x]/(pol)$, which will be a field:

```
gap> x:=X(Rationals,"x");; # create a variable
gap> pol:=x^8-8*x^7-196*x^6+1208*x^5+8742*x^4-43224*x^3-41476*x^2+227880*x+8609;;
gap> Factors(pol);
[ x^8-8*x^7-196*x^6+1208*x^5+8742*x^4-43224*x^3-41476*x^2+227880*x+8609 ]
gap> e:=AlgebraicExtension(Rationals,pol);
<algebraic extension over the Rationals of degree 8>
```

Now (working in `e` will automatically work with cosets) we work in this quotient ring. Since it is a field all arithmetic will work as expected.
We get values of the root expressions through factoring polynomials. All results withh be given as polynomials in a new variable `a`, that will be the coset $(pol) + x$. We start with $\sqrt{5}$:

```
gap> y:=X(e,"y");; # variable over the quotient ring
gap> RootsOfUPol(y^2-5);
[ -609/61755136*a^7+2095/30877568*a^6+133959/61755136*a^5-326101/30877568*a^4-\
7625627/61755136*a^3+12216013/30877568*a^2+92459893/61755136*a-67326631/30877568,
  609/61755136*a^7-2095/30877568*a^6-133959/61755136*a^5+326101/30877568*a^4+7\
625627/61755136*a^3-12216013/30877568*a^2-92459893/61755136*a+67326631/30877568 ]
gap> r5:=RootsOfUPol(y^2-5)[1]; # root 5
-609/61755136*a^7+2095/30877568*a^6+133959/61755136*a^5-326101/30877568*a^4-76\
25627/61755136*a^3+12216013/30877568*a^2+92459893/61755136*a-67326631/30877568
```

We similarly get $\sqrt{22 + 2\sqrt{5}}$, and thus calculate A. Since we work in the quotient ring all objects are represented by polynomials of degree ≤ 7.

[1] D. Shanks, *Incredible Identities*, Fibonacci Quarterly, **12** (1974), 271&280

```
gap> r22:=RootsOfUPol(y^2-(22+2*r5))[1]; # root of expression starting with 22
-312563/1790898944*a^7+843909/895449472*a^6+64760293/1790898944*a^5-101635911/\
895449472*a^4-3089942017/1790898944*a^3+2366180495/895449472*a^2+18967544655/1\
790898944*a-3396381133/895449472
gap> A:=r5+r22;
-20639/111931184*a^7+113083/111931184*a^6+4290319/111931184*a^5-13886605/11193\
1184*a^4-206942825/111931184*a^3+340055609/111931184*a^2+1353055097/111931184*\
a-668606679/111931184
```

Now we do the same for B, building up root expressions

```
gap> r29:=RootsOfUPol(y^2-29)[1]; #root 29
20639/111931184*a^7-113083/111931184*a^6-4290319/111931184*a^5+13886605/111931\
184*a^4+206942825/111931184*a^3-340055609/111931184*a^2-1241123913/111931184*a\
+556675495/111931184
gap> r11:=RootsOfUPol(y^2-(11+2*r29))[1];
-318289/3581797888*a^7+1674531/3581797888*a^6+66219455/3581797888*a^5-20011801\
3/3581797888*a^4-3175703931/3581797888*a^3+4847083105/3581797888*a^2+197616604\
93/3581797888*a-15977491783/3581797888
gap> r55:=RootsOfUPol(y^2-(55-10*r29))[1];
-587121/3581797888*a^7+2690715/3581797888*a^6+125087039/3581797888*a^5-2819769\
97/3581797888*a^4-6353565723/3581797888*a^3+4276345801/3581797888*a^2+54570779\
021/3581797888*a-1796485759/3581797888
gap> r16:=RootsOfUPol(y^2-(16-2*r29+2*r55))[1];
-342159/3581797888*a^7+1944125/3581797888*a^6+71070753/3581797888*a^5-24425334\
7/3581797888*a^4-3446466469/3581797888*a^3+6034696383/3581797888*a^2+235361026\
11/3581797888*a-5417921945/3581797888
gap> B:=r11+r16;
-20639/111931184*a^7+113083/111931184*a^6+4290319/111931184*a^5-13886605/11193\
1184*a^4-206942825/111931184*a^3+340055609/111931184*a^2+1353055097/111931184*\
a-668606679/111931184
```

Comparison shows equality:

```
gap> A-B;
!0
gap> A=B;
true
```