Computing in algebraic number fields using a primitive element.

Michael Monagan, Fall 2023.

Setting up the isomorphism between $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ and $\mathbb{Q}\left(\gamma = \sqrt{2} + \sqrt{3}\right)$.

```
> m1 := z1^2-2;
```

$$m1 := z1^2 - 2 \qquad (1)$$

```
> m2 := z2^2-3;
```

$$m2 := z2^2 - 3 \qquad (2)$$

Here are two ways to normalize in R = $\mathbb{Q}$ [z1,z2]/<m1,m2>

```
> MODG := proc(f)
     Groebner[NormalForm](f,[m1,m2],plex(z2,z1))
  end:
> MOD := proc(f) expand( rem(rem(f,m2,z2),m1,z1) ) end:
> gam := z1+z2;
```

$$gam := z1 + z2 \qquad (3)$$

```
> seq( MOD( gam^i ), i=0..4 );
```

$$1, z1 + z2, 2\, z1\, z2 + 5, 11\, z1 + 9\, z2, 20\, z1\, z2 + 49 \qquad (4)$$

```
> seq( MODG( gam^i ), i=0..4 );
```

$$1, z1 + z2, 2\, z1\, z2 + 5, 11\, z1 + 9\, z2, 20\, z1\, z2 + 49 \qquad (5)$$

```
> B := [1,z1,z2,z1*z2]; # Basis for Q[z1,z2]/<m1,m2>
```

$$B := [1, z1, z2, z1\, z2] \qquad (6)$$

The co-ordinate vector operation for R and it's inverse

```
> CV := proc(f) <coeff(coeff(f,z1,0),z2,0),
                 coeff(coeff(f,z1,1),z2,0),
                 coeff(coeff(f,z1,0),z2,1),
                 coeff(coeff(f,z1,1),z2,1)> end:
> CVinv := proc(v) local i; add(v[i]*B[i],i=1..4) end:
> seq( CV(MOD(gam^i)), i=0..4 );
```

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 5 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 11 \\ 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 49 \\ 0 \\ 0 \\ 20 \end{bmatrix} \qquad (7)$$

```
> A := <CV(1)|CV(gam)|CV(MOD(gam^2))|CV(MOD(gam^3))>;
```

$$A := \begin{bmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 11 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 2 & 0 \end{bmatrix} \qquad (8)$$

```
> AI := 1/A;
```

$$AI := \begin{bmatrix} 1 & 0 & 0 & -\frac{5}{2} \\ 0 & -\frac{9}{2} & \frac{11}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 \end{bmatrix} \quad (9)$$

To get the minimal polynomial for γ we have m(z) = z^4+az^3+bz^2+cz+d so m(γ)=0 implies
$a \cdot \gamma^3 + b \cdot \gamma^2 + c \cdot \gamma + c = -\gamma^4$ so

```
> b := -CV(MOD(gam^4));
```

$$b := \begin{bmatrix} -49 \\ 0 \\ 0 \\ -20 \end{bmatrix} \quad (10)$$

```
> AI.b;
```

$$\begin{bmatrix} 1 \\ 0 \\ -10 \\ 0 \end{bmatrix} \quad (11)$$

```
> Bz := [1,z,z^2,z^3];
```

$$Bz := [1, z, z^2, z^3] \quad (12)$$

```
> CVzinv := proc(v) local i; add(v[i]*Bz[i],i=1..4) end:
  CVz := proc(f) local i; <seq(coeff(f,z,i),i=0..3)> end:
> m := z^4+CVzinv(AI.b); # minpoly for gamma over Q
```

$$m := z^4 - 10\,z^2 + 1 \quad (13)$$

```
> a := 2+3*z1+4*z2-z1*z2;
```

$$a := -z1\,z2 + 3\,z1 + 4\,z2 + 2 \quad (14)$$

```
> b := 3-z1+z2+5*z1*z2;
```

$$b := 5\,z1\,z2 - z1 + z2 + 3 \quad (15)$$

```
> c := MOD(a*b);
```

$$c := 6\,z1\,z2 + 64\,z1 + 46\,z2 - 18 \quad (16)$$

Now mulitply a b using the isomorphism $\mathbb{Q}[z1, z2]\,/\,\langle m1, m2\rangle$ and $\mathbb{Q}[z]/\langle m\rangle$.

```
> phi := proc(f) CVzinv(AI.CV(f)) end;
```

ϕ := **proc**(*f*) *CVzinv*(\`.\`(*AI*, *CV*(*f*))) **end proc** (17)

```
> phiinv := proc(f) CVinv(A.CVz(f)) end;
```

phiinv := **proc**(*f*) *CVinv*(\`.\`(*A*, *CVz*(*f*))) **end proc** (18)

```
> phi(a);
```

```
phi(b);
```

$$\frac{9}{2}+\frac{17}{2}z-\frac{1}{2}z^2-\frac{1}{2}z^3$$

$$-\frac{19}{2}+10z+\frac{5}{2}z^2-z^3 \quad (19)$$

Now, we want to multiply these in $\mathbb{Q}(\gamma)$. We can use rem like this

```
> phic := rem(phi(a)*phi(b),m,z);
```

$$phic := 9z^3+3z^2-35z-33 \quad (20)$$

```
> phiinv(phic);
```

$$6\,z1\,z2+64\,z1+46\,z2-18 \quad (21)$$

On the assignment I'm asking you to use Maple's RootOf representation.

```
> alias(alpha1=RootOf(m1,z1));
  alias(alpha2=RootOf(m2,z2));
  alias(gamma=RootOf(m,z));
```

$$\alpha1$$

$$\alpha1,\ \alpha2$$

$$\alpha1,\ \alpha2,\ \gamma \quad (22)$$

```
> amap := subs(z1=alpha1,z2=alpha2,a);
  bmap := subs(z1=alpha1,z2=alpha2,b);
```

$$amap := -\alpha1\,\alpha2+3\,\alpha1+4\,\alpha2+2$$

$$bmap := 5\,\alpha1\,\alpha2-\alpha1+\alpha2+3 \quad (23)$$

```
> cmap := evala(amap*bmap);
```

$$cmap := 6\,\alpha1\,\alpha2+64\,\alpha1+46\,\alpha2-18 \quad (24)$$

```
> subs(alpha1=z1,alpha2=z2,cmap);
```

$$6\,z1\,z2+64\,z1+46\,z2-18 \quad (25)$$

```
> aphimap := subs(z=gamma,phi(a));
  bphimap := subs(z=gamma,phi(b));
```

$$aphimap := \frac{9}{2}+\frac{17}{2}\gamma-\frac{1}{2}\gamma^2-\frac{1}{2}\gamma^3$$

$$bphimap := -\frac{19}{2}+10\gamma+\frac{5}{2}\gamma^2-\gamma^3 \quad (26)$$

```
> cphimap := evala(aphimap*bphimap);
```

$$cphimap := 9\gamma^3+3\gamma^2-35\gamma-33 \quad (27)$$

```
> cphi := subs(gamma=z,cphimap);
```

$$cphi := 9z^3+3z^2-35z-33 \quad (28)$$

```
> phiinv(cphi);
```

$$6\,z1\,z2+64\,z1+46\,z2-18 \quad (29)$$