```
> (* Mantej Sokhi *)
```

QUESTION 4A:

```
> restart:
  with(Groebner):
```

```
> m1 := z[1]^2-3:
  m2 := z[2]^2+z[2]+1:
  alias(alpha1=RootOf(m1)):
  alias(alpha2=RootOf(m2)):
```

```
> (* m2 is irreducible over the number field Q(alpha1) *)

  temp := irreduc(m2,alpha1):
  temp:
```

```
> MODG := proc(f)
  local normalF:

  normalF := NormalForm(f,[m1,m2],plex(z[2],z[1])):
  return normalF:
  end proc:
```

```
> MOD := proc(f)
  local res:

  res := expand(rem(rem(f,m2,z[2]),m1,z[1])):
  return res:
  end proc:
```

```
> gam := z[1]+z[2]:
  temp := seq(MODG(gam^i),i=0..4):
  temp;
```

$$1, z_1 + z_2, 2 z_1 z_2 - z_2 + 2, -3 z_1 z_2 + 9 z_2 + 1, 12 z_1 z_2 + 4 z_1 - 17 z_2 - 9 \tag{1}$$

```
> basisM := [1,z[1],z[2],z[1]*z[2]]:
  basisM;
```

$$\left[1, z_1, z_2, z_1 z_2\right] \tag{2}$$

```
> cordVec := proc(f)
  <coeff(coeff(f,z[1],0),z[2],0),
   coeff(coeff(f,z[1],1),z[2],0),
   coeff(coeff(f,z[1],0),z[2],1),
   coeff(coeff(f,z[1],1),z[2],1)>
  end proc:
```

```
> invCordVec := proc(v)
  local res,i:
```

```
  res := add(v[i]*basisM[i],i=1..nops(basisM)):
  return res:
  end proc:
> cordVecList := seq(cordVec(MODG(gam^i)),i=0..4):
  cordVecList;
```

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ -1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 9 \\ -3 \end{bmatrix}, \begin{bmatrix} -9 \\ 4 \\ -17 \\ 12 \end{bmatrix} \tag{3}$$

```
> matA := <cordVecList[1]|cordVecList[2]|cordVecList[3]|cordVecList
  [4]>:
  matA;
```

$$\begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & 9 \\ 0 & 0 & 2 & -3 \end{bmatrix} \tag{4}$$

```
> matAInv := (1/matA):
  matAInv;
```

$$\begin{bmatrix} 1 & \frac{8}{15} & -\frac{8}{15} & -\frac{19}{15} \\ 0 & 1 & 0 & 0 \\ 0 & -\frac{1}{5} & \frac{1}{5} & \frac{3}{5} \\ 0 & -\frac{2}{15} & \frac{2}{15} & \frac{1}{15} \end{bmatrix} \tag{5}$$

```
> bVec := -cordVecList[5]:
  bVec;
```

$$\begin{bmatrix} 9 \\ -4 \\ 17 \\ -12 \end{bmatrix} \tag{6}$$

```
> solVec := matAInv.bVec:
  solVec;
```

$$\begin{bmatrix} 13 \\ -4 \\ -3 \\ 2 \end{bmatrix} \tag{7}$$

```
> cordVec2Inv := proc(v)
  local i,res:

  res := add(v[i]*B2[i],i=1..4):
  return res:
  end proc:
```

```
> cordVec2 := proc(f)
  local i,res:

  res := <seq(coeff(f,z,i),i=0..3)>:
  return res:
  end proc:
```

```
> B2 := [1,z,z^2,z^3]:
  minP := z^4+cordVec2Inv(solVec):
  minP;
```

$$z^4 + 2\,z^3 - 3\,z^2 - 4\,z + 13 \tag{8}$$

QUESTION 4B:

```
> a := x^4+(2*x^3*z[1])+(-z[1]*z[2]+3*z[2]+1)*x^2+(2*z[1]-6*z[2])*
  x+(3*z[1]*z[2])+3*z[1]+3*z[2]:
  b := (x^4*z[1])-(2*x^3*z[2])+(z[1]-3*z[2]-3)*x^2+(-2*z[1]*z[2]-2*
  z[1]-2*z[2])*x+(3*z[1]*z[2])-3:
```

```
  c := MODG(a*b):
> phi := proc(f)
  local res:

  res := cordVec2Inv(matAInv.cordVec(f)):
  return res:
  end proc:
> phiInv := proc(f)
  local res:

  res := invCordVec(matA.cordVec2(f)):
  return res:
  end proc:
> checkOne := phiInv(phi(z[1])):
  checkTwo := phiInv(phi(z[2])):
  checkOne;
  checkTwo;
```

$$z_1$$

$$z_2 \tag{9}$$

```
> (* METHOD 1 *)

  aMap := subs(z[1]=alpha1,z[2]=alpha2,a):
  bMap := subs(z[1]=alpha1,z[2]=alpha2,b):
  alias(gamma=RootOf(minP,z)):
  aMap;
  bMap;
```

$$x^4 + 2\,x^3\,\alpha1 + \left(-\alpha2\,\alpha1 + 3\,\alpha2 + 1\right)x^2 + \left(2\,\alpha1 - 6\,\alpha2\right)x + 3\,\alpha2\,\alpha1 + 3\,\alpha1 + 3\,\alpha2$$

$$x^4\,\alpha1 - 2\,x^3\,\alpha2 + \left(\alpha1 - 3\,\alpha2 - 3\right)x^2 + \left(-2\,\alpha2\,\alpha1 - 2\,\alpha1 - 2\,\alpha2\right)x + 3\,\alpha2\,\alpha1 - 3 \tag{10}$$

```
> res1 := evala(Gcd(aMap,bMap)):
  res1 := subs(alpha1=z[1],alpha2=z[2],res1):
  res1;
```

$$x^2 - z_1\,z_2 + 1 \tag{11}$$

```
> (* METHOD 2 *)

  phiA := collect(a,x,phi):
  phiB := collect(b,x,phi):
  mapPhiA := subs(z=gamma,phiA):
  mapPhiB := subs(z=gamma,phiB):
  res2 := evala(Gcd(mapPhiA,mapPhiB)):
```

```
res2 := phiInv(subs(gamma=z,res2)):
res2;
```

$$x^2 - z_1 z_2 + 1 \tag{12}$$