TP16 : Théorie de Galois constructive

Elements de corrige

```
> restart:
> with(group);
```

[*DerivedS, LCS, NormalClosure, RandElement, SnConjugates, Sylow, areconjugate, center, centralizer, core, cosets, cosrep, derived, elements, groupmember, grouporder, inter, invperm, isabelian, isnormal, issubgroup, mulperms, normalizer, orbit, parity, permrep, pres, transgroup*
]

Question 1

On reprend la liste du TP2

```
> C4:=permgroup(4,{[[1,2,3,4]]}):
  S4:=permgroup(4,{[[1,2,3,4]],[[1,2]]}):
  D4:=permgroup(4,{[[1,2,3,4]],[[1,3]]}):
  V4:=permgroup(4,{[[1,2],[3,4]],[[1,3],[2,4]]}):
  A4:=permgroup(4,{[[1,2,3]],[[1,2],[3,4]]}):
  C5:=permgroup(5,{[[1,2,3,4,5]]}):
  S5:=permgroup(5,{[[1,2,3,4,5]],[[1,2]]}):
  D5:=permgroup(5,{[[1,2,3,4,5]],[[2,5],[3,4]]}):
  A5:=permgroup(5,{[[1,2,3,4,5]],[[1,2,3]]}):
  M20:=permgroup(5,{[[1,2,3,4,5]],[[2,3,5,4]]}):
```

Dans les résultats suivants, obtenus à partir de la commande Galois, le signe (+ ou -) indique si le groupe de Galois est un sous-groupe de An.
On vérifie que les différents groupes transitifs (au moins pour le degré 4 et 5) sont atteints, en se basant sur la liste (à conjugaison près) donnée au TP4.
Les générateurs que donne Maple coincident avec ceux ci-dessus, à numérotation près des racines donc à conjugaison près dans Sn.

a) degrés 1 à 3

```
> galois(x);
```
"1T1", {"Id"}, "+", 1, {""}

```
> galois(x^2+x+1);
```
"2T1", {"S(2)"}, "-", 2, {"(1 2)"}

```
> galois(x^3+x^2-2*x-1);
```
"3T1", {"A(3)"}, "+", 3, {"(1 2 3)"}

```
> galois(x^3+2);
```
"3T2", {"S(3)"}, "-", 6, {"(2 3)", "(1 3)"}

b) degré 4

```
> galois(x^4+x^3+x^2+x+1);
```
"4T1", {"C(4)"}, "-", 4, {"(1 2 3 4)"}

```
> galois(x^4+1);
```
"4T2", {"E(4)", "2[x]2"}, "+", 4, {"(1 2)(3 4)", "(1 4)(2 3)"}

```
> galois(x^4-2);
```
"4T3", {"D(4)"}, "-", 8, {"(1 2 3 4)", "(1 3)"}

```
> galois(x^4+8*x+12);
```
"4T4", {"A(4)"}, "+", 12, {"(2 3 4)", "(1 2 4)"}

```
> galois(x^4+x+1);
```
"4T5", {"S(4)"}, "-", 24, {"(3 4)", "(1 4)", "(2 4)"}

c) degré 5

```
> galois(x^5+x^4-4*x^3-3*x^2+3*x+1);
```
"5T1", {"C(5)"}, "+", 5, {"(1 2 3 4 5)"}

```
> galois(x^5-5*x+12);
```
"5T2", {"5:2", "D(5)"}, "+", 10, {"(1 2 3 4 5)", "(1 4)(2 3)"}

```
> galois(x^5+2);
```
"5T3", {"5:4", "F(5)"}, "-", 20, {"(1 2 4 3)", "(1 2 3 4 5)"}

```
> galois(x^5+20*x+16);
```
"5T4", {"A(5)"}, "+", 60, {"(1 2 5)", "(2 3 5)", "(3 4 5)"}

```
> galois(x^5-x+1);
```
"5T5", {"S(5)"}, "-", 120, {"(1 5)", "(2 5)", "(3 5)", "(4 5)"}

d) degré 6

```
> galois(x^6+x^5+x^4+x^3+x^2+x+1);
```
"6T1", {"C(6)", "3[x]2"}, "-", 6, {"(1 2 3 4 5 6)"}

```
> galois(x^6+108);
```
"6T2", {"D_6(6)", "[3]2"}, "-", 6, {"(5 6)(1 4)(2 3)", "(2 4 6)(1 3 5)"}

```
> galois(x^6+2);
```
"6T3", {"S(3)[x]2", "D(6)"}, "-", 12, {"(5 6)(1 4)(2 3)", "(1 2 3 4 5 6)"}

```
> galois(x^6-3*x^2-1);
```
"6T4", {"[2^2]3", "A_4(6)"}, "+", 12, {"(1 4)(2 5)", "(2 4 6)(1 3 5)"}

```
> galois(x^6+3*x^3+3);
```
"6T5", {"[3^2]2", "F_18(6)", "3 wr 2"}, "-", 18, {"(3 6)(1 4)(2 5)", "(2 4 6)"}

```
> galois(x^6-3*x^2+1);
```
"6T6", {"2A_4(6)", "2 wr 3", "[2^3]3"}, "-", 24, {"(2 4 6)(1 3 5)", "(3 6)"}

```
> galois(x^6-4*x^2-1);
```
"6T7", {"[2^2]S(3)", "S_4(6d)"}, "+", 24, {"(1 4)(2 5)", "(2 4 6)(1 3 5)", "(1 5)(2 4)"}

```
> galois(x^6-3*x^5+6*x^4-7*x^3+2*x^2+x-4);
```
"6T8", {"1/2[2^3]S(3)", "S_4(6c)"}, "-", 24,
{"(1 4)(2 5)", "(1 5)(2 4)(3 6)", "(2 4 6)(1 3 5)"}

```
> galois(x^6+2*x^3-2);
```
"6T9", {"F_18(6):2", "[1/2S(3)^2]2"}, "-", 36,
{"(3 6)(1 4)(2 5)", "(2 4 6)", "(1 5)(2 4)"}

```
> galois(x^6+6*x^4+2*x^3+9*x^2+6*x-4);
```
"6T10", {"1/2[S(3)^2]2", "F_36(6)"}, "+", 36,
{"(3 6)(1 4 5 2)", "(2 4 6)", "(1 5)(2 4)"}

```
> galois(x^6+2*x^2+2);
```
"6T11", {"[2^3]S(3)", "2 wr S(3)", "2S_4(6)"}, "-", 48,
{"(2 4 6)(1 3 5)", "(3 6)", "(1 5)(2 4)"}

```
> galois(x^6-2*x^5-5*x^2-2*x-1);
```
"6T12", {"PSL(2,5)", "A_5(6)", "L(6)"}, "+", 60, {"(1 2 3 4 6)", "(5 6)(1 4)"}

```
> galois(x^6+2*x^4+2*x^3+x^2+2*x+2);
```
"6T13", {"F_36(6):2", "[S(3)^2]2", "S(3) wr 2"}, "-", 72,
{"(3 6)(1 4)(2 5)", "(2 4 6)", "(2 4)"}

```
> galois(x^6-x^5-10*x^4+30*x^3-31*x^2+7*x+9);
```
"6T14", {"PGL(2,5)", "L(6):2", "S_5(6)"}, "-", 120, {"(1 2)(3 4)(5 6)", "(1 2 3 4 6)"}

```
> galois(x^6+24*x-20);
```
"6T15", {"A(6)"}, "+", 360, {"(3 4 6)", "(1 2 6)", "(2 3 6)", "(4 5 6)"}

```
> galois(x^6+x+1);
```
"6T16", {"S(6)"}, "-", 720, {"(1 6)", "(2 6)", "(4 6)", "(3 6)", "(5 6)"}

e) degré 7

```
> galois(x^7+x^6-12*x^5-7*x^4+28*x^3+14*x^2-9*x+1);
```
"7T1", {"C(7)"}, "+", 7, {"(1 2 3 4 5 6 7)"}

```
> galois(x^7+7*x^3+7*x^2+7*x-1);
```
"7T2", {"7:2", "D(7)"}, "-", 14, {"(1 6)(2 5)(3 4)", "(1 2 3 4 5 6 7)"}

```
> galois(x^7-14*x^5+56*x^3-56*x+22);
```
"7T3", {"7:3", "F_21(7)"}, "+", 21, {"(1 2 4)(3 6 5)", "(1 2 3 4 5 6 7)"}

```
> galois(x^7+2);
```
"7T4", {"7:6", "F_42(7)"}, "-", 42, {"(1 3 2 6 4 5)", "(1 2 3 4 5 6 7)"}

```
> galois(x^7-7*x^3+14*x^2-7*x+1);
```
"7T5", {"L(7)", "L(3,2)"}, "+", 168, {"(1 2)(3 6)", "(1 2 3 4 5 6 7)"}

```
> galois(x^7+7*x^4+14*x+3);
```
"7T6", {"A(7)"}, "+", 2520, {"(1 2 7)", "(2 3 7)", "(3 4 7)", "(4 5 7)", "(5 6 7)"}

```
> galois(x^7+x+1);
```
"7T7", {"S(7)"}, "-", 5040, {"(6 7)", "(4 7)", "(5 7)", "(1 7)", "(2 7)", "(3 7)"}

Question 2

An et Sn ne sont pas résolubles, mais Cn et Dn le sont. Cela permet de statuer sauf le cas de M20.

```
> P:=x^5-x+1: G:=permgroup(5,galois(P)[5]); DerivedS(G);
```
G := permgroup(5, {[[1, 5]], [[2, 5]], [[3, 5]], [[4, 5]]})

[permgroup(5, {[[1, 5]], [[2, 5]], [[3, 5]], [[4, 5]]}),
permgroup(5, {[[1, 4, 5]], [[2, 4, 5]], [ ], [[3, 4, 5]]})]

La chaine de groupes se termine par A5.

```
> solve(P);
```
RootOf($\_Z^5 - \_Z + 1$, *index* = 1), RootOf($\_Z^5 - \_Z + 1$, *index* = 2),
RootOf($\_Z^5 - \_Z + 1$, *index* = 3), RootOf($\_Z^5 - \_Z + 1$, *index* = 4),
RootOf($\_Z^5 - \_Z + 1$, *index* = 5)

Maple répond par des RootOf, puisqu'il ne peut écrire des formules pas radicaux.

```
> P:=x^5+2: G:=permgroup(5,galois(P)[5]); DerivedS(G);
```
G := permgroup(5, {[[1, 2, 4, 3]], [[1, 2, 3, 4, 5]]})

[permgroup(5, {[[1, 2, 4, 3]], [[1, 2, 3, 4, 5]]}), permgroup(5, {[[1, 2, 3, 4, 5]], [ ]}),
permgroup(5, {[ ]})]

La chaine de groupes termine par {id} : le groupe est bien résoluble. C5 est distingué dans M20.

```
> isnormal(permgroup(5,{[[1,2,3,4,5]]}),G);
```
true

```
> solve(P);
```
$$\cos\left(\frac{\pi}{5}\right)2^{(1/5)}+\sin\left(\frac{\pi}{5}\right)2^{(1/5)}I,\ \left(\left(\frac{\sqrt{5}}{4}-\frac{1}{4}\right)\cos\left(\frac{\pi}{5}\right)-\frac{1}{4}\sqrt{2}\sqrt{5+\sqrt{5}}\sin\left(\frac{\pi}{5}\right)\right)2^{(1/5)}$$
$$+\left(\frac{1}{4}\sqrt{2}\sqrt{5+\sqrt{5}}\cos\left(\frac{\pi}{5}\right)+\left(\frac{\sqrt{5}}{4}-\frac{1}{4}\right)\sin\left(\frac{\pi}{5}\right)\right)2^{(1/5)}I,$$
$$\left(\left(-\frac{\sqrt{5}}{4}-\frac{1}{4}\right)\cos\left(\frac{\pi}{5}\right)-\frac{1}{4}\sqrt{2}\sqrt{5-\sqrt{5}}\sin\left(\frac{\pi}{5}\right)\right)2^{(1/5)}$$
$$+\left(\frac{1}{4}\sqrt{2}\sqrt{5-\sqrt{5}}\cos\left(\frac{\pi}{5}\right)+\left(-\frac{\sqrt{5}}{4}-\frac{1}{4}\right)\sin\left(\frac{\pi}{5}\right)\right)2^{(1/5)}I,$$
$$\left(\left(-\frac{\sqrt{5}}{4}-\frac{1}{4}\right)\cos\left(\frac{\pi}{5}\right)+\frac{1}{4}\sqrt{2}\sqrt{5-\sqrt{5}}\sin\left(\frac{\pi}{5}\right)\right)2^{(1/5)}$$
$$+\left(-\frac{1}{4}\sqrt{2}\sqrt{5-\sqrt{5}}\cos\left(\frac{\pi}{5}\right)+\left(-\frac{\sqrt{5}}{4}-\frac{1}{4}\right)\sin\left(\frac{\pi}{5}\right)\right)2^{(1/5)}I,$$
$$\left(\left(\frac{\sqrt{5}}{4}-\frac{1}{4}\right)\cos\left(\frac{\pi}{5}\right)+\frac{1}{4}\sqrt{2}\sqrt{5+\sqrt{5}}\sin\left(\frac{\pi}{5}\right)\right)2^{(1/5)}$$
$$+\left(-\frac{1}{4}\sqrt{2}\sqrt{5+\sqrt{5}}\cos\left(\frac{\pi}{5}\right)+\left(\frac{\sqrt{5}}{4}-\frac{1}{4}\right)\sin\left(\frac{\pi}{5}\right)\right)2^{(1/5)}I$$

On a bien des formules par radicaux.

Question 3

```
> restart; infolevel[galois]:=2:
> galois(x^4+x^3+x^2+x+1);
```
```
galois:   Computing the Galois group of    x^4+x^3+x^2+x+1
galois/absres:   125 = 125, (nonsquare)
galois/absres:   Possible groups:   {"4T1", "4T3", "4T5"}
galois/absres:   p = 2   gives shape   4
galois/absres:   p = 3   gives shape   4
galois/absres:   p = 7   gives shape   4
galois/absres:   p = 11   gives shape   1, 1, 1, 1
galois/absres:   p = 13   gives shape   4
galois/absres:   p = 17   gives shape   4
galois/absres:   p = 19   gives shape   2, 2
galois/absres:   p = 23   gives shape   4
galois/absres:   The Galois group is probably one of   {"4T1"}
galois/respol:   Using the orbit-length partition of 2-sequences.
galois/respol:   Calculating a resolvent polynomial...
galois/respol:   Factoring the resolvent polynomial...
galois/respol:   Orbit-length partition is   4, 4, 4
galois/respol:   Removing   {"4T3", "4T5"}
galois/respol:   Possible groups left:   {"4T1"}
```
"4T1", {"C(4)"}, "-", 4, {"(1 2 3 4)"}

C'est le groupe cyclique (théorie des extensions cyclotomiques). Ce n'est pas un sous-groupe de A4.

```
> galois(x^4+1);
```
```
galois:   Computing the Galois group of    x^4+1
galois/absres:   256 = ‘‘(16)^2
galois/absres:   Possible groups:   {"4T2", "4T4"}
galois/absres:   p = 3   gives shape   2, 2
galois/absres:   p = 5   gives shape   2, 2
galois/absres:   p = 7   gives shape   2, 2
```

```
galois/absres:   p = 11   gives shape   2, 2
galois/absres:   p = 13   gives shape   2, 2
galois/absres:   p = 17   gives shape   1, 1, 1, 1
galois/absres:   p = 19   gives shape   2, 2
galois/absres:   p = 23   gives shape   2, 2
galois/absres:   The Galois group is probably one of   {"4T2"}
galois/respol:   Using the orbit-length partition of 2-sets.
galois/respol:   Calculating a resolvent polynomial...
galois/respol:   Calculating a resolvent polynomial...
galois/respol:   Factoring the resolvent polynomial...
galois/respol:   Orbit-length partition is   2, 2, 2
galois/respol:   Removing   {"4T4"}
galois/respol:   Possible groups left:   {"4T2"}
```

"4T2", {"E(4)", "2[x]2"}, "+", 4, {"(1 2)(3 4)", "(1 4)(2 3)"}

C'est V4, qui est un sous-groupe de A4. On aurait pu le calculer à la main.

```
> solve(x^4+1);
```

$$\frac{\sqrt{2}}{2}+\frac{1}{2}I\sqrt{2},\ \frac{1}{2}I\sqrt{2}-\frac{\sqrt{2}}{2},\ -\frac{\sqrt{2}}{2}-\frac{1}{2}I\sqrt{2},\ -\frac{1}{2}I\sqrt{2}+\frac{\sqrt{2}}{2}$$

En effet, Q(sqrt(2),i) est corps de décomposition ; on raisonne comme pour x^4-2, ci-dessous.

```
> galois(x^4-2);
galois:   Computing the Galois group of    x^4-2
galois/absres:   -2048 = -2048, (nonsquare)
galois/absres:   Possible groups:   {"4T1", "4T3", "4T5"}
galois/absres:   p = 3   gives shape   2, 2
galois/absres:   p = 5   gives shape   4
galois/absres:   p = 7   gives shape   2, 1, 1
galois/absres:   Removing   {"4T1"}
galois/absres:   Possible groups left:   {"4T3", "4T5"}
galois/absres:   p = 11   gives shape   2, 2
galois/absres:   p = 13   gives shape   4
galois/absres:   p = 17   gives shape   2, 2
galois/absres:   p = 19   gives shape   2, 2
galois/absres:   p = 23   gives shape   2, 1, 1
galois/absres:   p = 29   gives shape   4
galois/absres:   p = 31   gives shape   2, 1, 1
galois/absres:   p = 37   gives shape   4
galois/absres:   The Galois group is probably one of   {"4T3"}
galois/respol:   Using the orbit-length partition of 2-sets.
galois/respol:   Calculating a resolvent polynomial...
galois/respol:   Calculating a resolvent polynomial...
galois/respol:   Factoring the resolvent polynomial...
galois/respol:   Orbit-length partition is   2, 4
galois/respol:   Removing   {"4T5"}
galois/respol:   Possible groups left:   {"4T3"}
```

"4T3", {"D(4)"}, "-", 8, {"(1 3)", "(1 2 3 4)"}

Ce groupe a déjà été calculé au papier-crayon (chapitre XIV) : c'est D4, qui n'est pas un sous-groupe de A4.

```
> galois(x^4+8*x+12);
galois:   Computing the Galois group of    x^4+8*x+12
galois/absres:   331776 = ``(576)^2
galois/absres:   Possible groups:   {"4T2", "4T4"}
galois/absres:   p = 5   gives shape   3, 1
galois/absres:   Removing   {"4T2"}
galois/absres:   Possible groups left:   {"4T4"}
```

"4T4", {"A(4)"}, "+", 12, {"(1 2 4)", "(2 3 4)"}

Maple peut conclure sans calculer de résolvante. C'est A4. Par contre à la main...

```
> solve(x^4+8*x+12);
```

$$\mathrm{RootOf}(\_Z^4+8\,\_Z+12,\ index=1),\ \mathrm{RootOf}(\_Z^4+8\,\_Z+12,\ index=2),$$
$$\mathrm{RootOf}(\_Z^4+8\,\_Z+12,\ index=3),\ \mathrm{RootOf}(\_Z^4+8\,\_Z+12,\ index=4)$$

```
> allvalues(RootOf(x^4+8*x+12,x));
```

$$\frac{\sqrt{2}\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}}{2}+\left(-\left(2\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}\,(4+4I\sqrt{3})^{(2/3)}+8\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}+8\sqrt{2}\,(4+4I\sqrt{3})^{(1/3)}\right)\Big/\left((4+4I\sqrt{3})^{(1/3)}\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}\right)\right)^{(1/2)}\Big/2,$$

$$\frac{\sqrt{2}\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}}{2}-\left(-\left(2\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}\,(4+4I\sqrt{3})^{(2/3)}+8\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}+8\sqrt{2}\,(4+4I\sqrt{3})^{(1/3)}\right)\Big/\left((4+4I\sqrt{3})^{(1/3)}\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}\right)\right)^{(1/2)}\Big/2,$$

$$-\frac{\sqrt{2}\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}}{2}+\left(-\left(2\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}\,(4+4I\sqrt{3})^{(2/3)}+8\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}-8\sqrt{2}\,(4+4I\sqrt{3})^{(1/3)}\right)\Big/\left((4+4I\sqrt{3})^{(1/3)}\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}\right)\right)^{(1/2)}\Big/2,$$

$$-\frac{\sqrt{2}\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}}{2}-\left(-\left(2\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}\,(4+4I\sqrt{3})^{(2/3)}+8\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}-8\sqrt{2}\,(4+4I\sqrt{3})^{(1/3)}\right)\Big/\left((4+4I\sqrt{3})^{(1/3)}\sqrt{\frac{(4+4I\sqrt{3})^{(2/3)}+4}{(4+4I\sqrt{3})^{(1/3)}}}\right)\right)^{(1/2)}\Big/2$$

L'expression des racines est beaucoup plus complexe...

```
> galois(x^4+x+1);
galois:   Computing the Galois group of    x^4+x+1
galois/absres:   229 = 229, (nonsquare)
galois/absres:   Possible groups:   {"4T1", "4T3", "4T5"}
```

```
galois/absres:   p = 2   gives shape   4
galois/absres:   p = 3   gives shape   3, 1
galois/absres:   Removing   {"4T1", "4T3"}
galois/absres:   Possible groups left:   {"4T5"}
```

"4T5", {"S(4)"}, "-", 24, {"(2 4)", "(3 4)", "(1 4)"}

Maple peut conclure sans calculer de résolvante. C'est S4.

```
> galois(x^5+2);
```

```
galois:   Computing the Galois group of    x^5+2
galois/absres:   50000 = 50000, (nonsquare)
galois/absres:   Possible groups:   {"5T3", "5T5"}
galois/absres:   p = 3   gives shape   4, 1
galois/absres:   p = 7   gives shape   4, 1
galois/absres:   p = 11   gives shape   5
galois/absres:   p = 13   gives shape   4, 1
galois/absres:   p = 17   gives shape   4, 1
galois/absres:   p = 19   gives shape   2, 2, 1
galois/absres:   p = 23   gives shape   4, 1
galois/absres:   p = 29   gives shape   2, 2, 1
galois/absres:   p = 31   gives shape   5
galois/absres:   p = 37   gives shape   4, 1
galois/absres:   The Galois group is probably one of   {"5T3"}
galois/special5:   Calculating a S5/F20 resolvent...
galois/special5:   Factoring this S5/F20 resolvent...
galois/special5:   Reducible, so the Galois group is   "5T3"
```

"5T3", {"5:4", "F(5)"}, "-", 20, {"(1 2 3 4 5)", "(1 2 4 3)"}

Maple calcule une résolvante pour trancher entre S5 et M20.

```
> galois(x^6+12);
```

```
galois:   Computing the Galois group of    x^6+12
galois/absres:   -11609505792 = -11609505792, (nonsquare)
galois/absres:   Possible groups:   {"6T5", "6T9", "6T1", "6T2", "6T3", "6T6
", "6T8", "6T11", "6T13", "6T14", "6T16"}
galois/absres:   p = 5   gives shape   2, 2, 2
galois/absres:   p = 7   gives shape   3, 3
galois/absres:   p = 11   gives shape   2, 2, 2
galois/absres:   p = 13   gives shape   1, 1, 1, 1, 1, 1
galois/absres:   p = 17   gives shape   2, 2, 2
galois/absres:   p = 19   gives shape   1, 1, 1, 1, 1, 1
galois/absres:   p = 23   gives shape   2, 2, 2
galois/absres:   p = 29   gives shape   2, 2, 2
galois/absres:   p = 31   gives shape   3, 3
galois/absres:   p = 37   gives shape   3, 3
galois/absres:   p = 41   gives shape   2, 2, 2
galois/absres:   p = 43   gives shape   3, 3
galois/absres:   The Galois group is probably one of   {"6T2"}
galois/respol:   Using the orbit-length partition of 2-sets.
galois/respol:   Calculating a resolvent polynomial...
galois/respol:   Calculating a resolvent polynomial...
galois/respol:   Factoring the resolvent polynomial...
galois/respol:   Orbit-length partition is   3, 3, 3, 6
galois/respol:   Removing   {"6T5", "6T9", "6T1", "6T3", "6T6", "6T8", "6T11
", "6T13", "6T14", "6T16"}
galois/respol:   Possible groups left:   {"6T2"}
```

"6T2", {"D_6(6)", "[3]2"}, "-", 6, {"(2 4 6)(1 3 5)", "(5 6)(1 4)(2 3)"}

Ce groupe a déjà été calculé, sachant que le polynome x^6+12 est normal (TP14) : c'est S3, isomorphe également à D6.

Question 4

```
> with(group);
```

[DerivedS, LCS, NormalClosure, RandElement, SnConjugates, Sylow, areconjugate, center, centralizer, core, cosets, cosrep, derived, elements, groupmember, grouporder, inter, invperm, isabelian, isnormal, issubgroup, mulperms, normalizer, orbit, parity, permrep, pres, transgroup]

```
> ordre:=proc(a,b) local i;
   for i from 1 to min(nops(a),nops(b)) do if a[i]<>b[i] then
  return(evalb(a[i]<b[i])); fi; od;
    if nops(a)<=nops(b) then return(true) else return(false);
  fi;
  end:
> ordre([1,3],[1,1,1,1]);
```

false

```
> sort({[1,3],[1,1,1,1],[1,1,2]},ordre);
```

{[1, 1, 2], [1, 1, 1, 1], [1, 3]}

Ce n'est pas correct !

```
> sort([[1,4],[1,1,1,1],[1,1,2]],ordre);
```

[[1, 1, 1, 1], [1, 1, 2], [1, 4]]

Il faut trier des listes (qui tient compte de l'ordre) et non des ensembles.

```
> listetypes:=proc(n)
   local S,i,j,b;
   S:={[n]} ;
   for i from 1 to n-1 do j:=n-i ;
     for b in listetypes(j) do
       S:=S union {sort([i,op(b)])};
     od;
   od;
   return(sort([op(S)],ordre));
  end:
> listetypes(4);
```

[[1, 1, 1, 1], [1, 1, 2], [1, 3], [2, 2], [4]]

```
> listetypes(5);
```

[[1, 1, 1, 1, 1], [1, 1, 1, 2], [1, 1, 3], [1, 2, 2], [1, 4], [2, 3], [5]]

cf TP2 :

```
> typ:=proc(n,g) local N,res,i,N1;
   N:=nops(g);
   if N=0 then return([1$n])
     else res:=[seq(nops(op(i,g)),i=1..N)];
     N1:=sum(res[i],i=1..nops(res));
     return([1$(n-N1),op(sort(res))]);
   fi;
  end:
> typesG:=proc(G)
    local S,GG,N,t,g,L,m,n;
    n:=op(1,G); S:=listetypes(n);
    GG:=elements(G); N:=nops(GG);
    for t in S do m[t]:=0; od;
    for g in GG do
      t:=typ(n,g); m[t]:=m[t]+1;
    od;
    L:=[];
    for t in S do
      L:=[op(L),[t,m[t]/N]] ;
    od;
    return(L);
  end:
> C4:=permgroup(4,{[[1,2,3,4]]}):
  S4:=permgroup(4,{[[1,2,3,4]],[[1,2]]}):
  D4:=permgroup(4,{[[1,2,3,4]],[[1,3]]}):
```

```
V4:=permgroup(4,{[[1,2],[3,4]],[[1,3],[2,4]]}):
A4:=permgroup(4,{[[1,2,3]],[[1,2],[3,4]]}):
C5:=permgroup(5,{[[1,2,3,4,5]]}):
S5:=permgroup(5,{[[1,2,3,4,5]],[[1,2]]}):
D5:=permgroup(5,{[[1,2,3,4,5]],[[2,5],[3,4]]}):
A5:=permgroup(5,{[[1,2,3,4,5]],[[1,2,3]]}):
M20:=permgroup(5,{[[1,2,3,4,5]],[[2,3,5,4]]}):
> listeG:=[C4,S4,D4,V4,A4,C5,S5,D5,A5,M20]:
> listetypesG:=[]: for G in listeG do
  listetypesG:=[op(listetypesG),typesG(G)]; od:
> for i from 1 to 10 do print(listetypesG[i]); od;
```

$$[[[1,1,1,1],\frac{1}{4}],[[1,1,2],0],[[1,3],0],[[2,2],\frac{1}{4}],[[4],\frac{1}{2}]]$$

$$[[[1,1,1,1],\frac{1}{24}],[[1,1,2],\frac{1}{4}],[[1,3],\frac{1}{3}],[[2,2],\frac{1}{8}],[[4],\frac{1}{4}]]$$

$$[[[1,1,1,1],\frac{1}{8}],[[1,1,2],\frac{1}{4}],[[1,3],0],[[2,2],\frac{3}{8}],[[4],\frac{1}{4}]]$$

$$[[[1,1,1,1],\frac{1}{4}],[[1,1,2],0],[[1,3],0],[[2,2],\frac{3}{4}],[[4],0]]$$

$$[[[1,1,1,1],\frac{1}{12}],[[1,1,2],0],[[1,3],\frac{2}{3}],[[2,2],\frac{1}{4}],[[4],0]]$$

$$[[[1,1,1,1,1],\frac{1}{5}],[[1,1,1,2],0],[[1,1,3],0],[[1,2,2],0],[[1,4],0],[[2,3],0],[[5],\frac{4}{5}]]$$

$$[[[1,1,1,1,1],\frac{1}{120}],[[1,1,1,2],\frac{1}{12}],[[1,1,3],\frac{1}{6}],[[1,2,2],\frac{1}{8}],[[1,4],\frac{1}{4}],[[2,3],\frac{1}{6}],[[5],\frac{1}{5}]]$$

$$[[[1,1,1,1,1],\frac{1}{10}],[[1,1,1,2],0],[[1,1,3],0],[[1,2,2],\frac{1}{2}],[[1,4],0],[[2,3],0],[[5],\frac{2}{5}]]$$

$$[[[1,1,1,1,1],\frac{1}{60}],[[1,1,1,2],0],[[1,1,3],\frac{1}{3}],[[1,2,2],\frac{1}{4}],[[1,4],0],[[2,3],0],[[5],\frac{2}{5}]]$$

$$[[[1,1,1,1,1],\frac{1}{20}],[[1,1,1,2],0],[[1,1,3],0],[[1,2,2],\frac{1}{4}],[[1,4],\frac{1}{2}],[[2,3],0],[[5],\frac{1}{5}]]$$

Question 5

```
> infolevel[galois]:=0:
> testAn:=proc(P);
  if type(sqrt(discrim(P,x)),integer) then return('+') else
  return('-'); fi;
  end:
> typeMod:=proc(P,r) local p,F,S,d;
   if not(irreduc(P)) then error("P doit etre irreductible")
     else
     S:={}; d:=discrim(P,x);
     for p to r do
       if isprime(p) and d mod p<>0 then
         F := op(2, Factors(P) mod p);
         S:=S union {sort([seq(degree(op(1,a),x),a=F)])};
       fi;
     od;
   return(S);
   fi;
  end:
> P:=x^4+x^3+x^2+x+1: testAn(P); typeMod(P,31);
```

$$-$$

$$\{[2,2],[1,1,1,1],[4]\}$$

Ce peut etre C4, D4 ou S4 : on ne peut pas conclure. Le test modulaire n'apporte rien.

```
> typeMod(P,200);
```

$$\{[2,2],[1,1,1,1],[4]\}$$

Calculer avec davantage de nombres premiers ne sert pas.

```
> P:=x^4+1: testAn(P); typeMod(P,31);
```

$$+$$

$$\{[2,2],[1,1,1,1]\}$$

```
> typeMod(P,200);
```

$$\{[2,2],[1,1,1,1]\}$$

On en peut pas décider entre A4 et V4. Le test modulaire n'apporte rien.

```
> P:=x^4-2: testAn(P); typeMod(P,31);
```

$$-$$

$$\{[2,2],[1,1,2],[4]\}$$

```
> typeMod(P,200);
```

$$\{[2,2],[1,1,2],[1,1,1,1],[4]\}$$

(le nouveau type obtenu ne donne pas de nouvelle information : dommage)

Ce peut etre D4 ou S4. Le test modulaire a permis d'éliminer C4.

```
> P:=x^4+8*x+12: testAn(P); typeMod(P,31);
```

$$+$$

$$\{[2,2],[1,3]\}$$

C'est A4.

```
> P:=x^4+x+1: testAn(P); typeMod(P,31);
```

-

{[1, 1, 2], [1, 3], [4]}

C'est S4.

Les deux derniers cas correspondent aux deux cas où Maple a pu conclure sans calculer de résolvante.

```
> P:=x^5+x^4-4*x^3-3*x^2+3*x+1: testAn(P); typeMod(P,31);
```

+

{[1, 1, 1, 1, 1], [5]}

C5, D5 ou A5

```
> P:=x^5-5*x+12: testAn(P); typeMod(P,31);
```

+

{[1, 2, 2], [5]}

D5 ou A5

```
> P:=x^5+2: testAn(P); typeMod(P,31);
```

-

{[1, 2, 2], [1, 4], [5]}

M20 ou S5

```
> P:=x^5+20*x+16: testAn(P); typeMod(P,31);
```

+

{[1, 2, 2], [1, 1, 3], [5]}

A5

```
> P:=x^5-x+1: testAn(P); typeMod(P,31);
```

-

{[1, 4], [2, 3], [1, 1, 3], [5]}

S5

Question 6

Ecrivons le programme demandé :

```
> typeMod2:=proc(P,r) local p,F,S,L,d,pi,t,m,n; global x;
   if not(irreduc(P)) then error("P doit etre irreductible")
     else
     d:=discrim(P,x); pi:=0; n:=degree(P,x);
     S:=listetypes(n);
     for t in S do m[t]:=0; od;
     for p to r do
       if isprime(p) and d mod p<>0 then
         F := op(2, Factors(P) mod p);
         t:=sort([seq(degree(op(1,a),x),a=F)]);
         m[t]:=m[t]+1; pi:=pi+1;
       fi;
     od;
     L:=[]; for t in S do
       L:=[op(L),[t,m[t]/pi]] ;
     od;
   return(L);
   fi;
  end:
```

```
> P:=x^4+x^3+x^2+x+1: typeMod2(P,31);
```

$$\left[\left[[1, 1, 1, 1], \frac{1}{5}\right], [[1, 1, 2], 0], [[1, 3], 0], \left[[2, 2], \frac{1}{5}\right], \left[[4], \frac{3}{5}\right]\right]$$

C4, D4 ou S4 ?

```
> for G in [C4,D4,S4] do typesG(G); od;
```

$$\left[\left[[1, 1, 1, 1], \frac{1}{4}\right], [[1, 1, 2], 0], [[1, 3], 0], \left[[2, 2], \frac{1}{4}\right], \left[[4], \frac{1}{2}\right]\right]$$

$$\left[\left[[1, 1, 1, 1], \frac{1}{8}\right], \left[[1, 1, 2], \frac{1}{4}\right], [[1, 3], 0], \left[[2, 2], \frac{3}{8}\right], \left[[4], \frac{1}{4}\right]\right]$$

$$\left[\left[[1, 1, 1, 1], \frac{1}{24}\right], \left[[1, 1, 2], \frac{1}{4}\right], \left[[1, 3], \frac{1}{3}\right], \left[[2, 2], \frac{1}{8}\right], \left[[4], \frac{1}{4}\right]\right]$$

On penche plutot pour C4, à cause du type [4].

```
> P:=x^4+1: typeMod2(P,31);
```

$$\left[\left[[1, 1, 1, 1], \frac{1}{10}\right], [[1, 1, 2], 0], [[1, 3], 0], \left[[2, 2], \frac{9}{10}\right], [[4], 0]\right]$$

A4 ou V4 ?

```
> for G in [A4,V4] do typesG(G); od;
```

$$\left[\left[[1, 1, 1, 1], \frac{1}{12}\right], [[1, 1, 2], 0], \left[[1, 3], \frac{2}{3}\right], \left[[2, 2], \frac{1}{4}\right], [[4], 0]\right]$$

$$\left[\left[[1, 1, 1, 1], \frac{1}{4}\right], [[1, 1, 2], 0], [[1, 3], 0], \left[[2, 2], \frac{3}{4}\right], [[4], 0]\right]$$

On penche plutot pour V4, à cause du type [2,2]

```
> P:=x^4-2: typeMod2(P,31);
```

$$\left[[[1, 1, 1, 1], 0], \left[[1, 1, 2], \frac{3}{10}\right], [[1, 3], 0], \left[[2, 2], \frac{2}{5}\right], \left[[4], \frac{3}{10}\right]\right]$$

D4 ou S4 ?

```
> for G in [D4,S4] do typesG(G); od;
```

$$\left[\left[[1, 1, 1, 1], \frac{1}{8}\right], \left[[1, 1, 2], \frac{1}{4}\right], [[1, 3], 0], \left[[2, 2], \frac{3}{8}\right], \left[[4], \frac{1}{4}\right]\right]$$

$$\left[\left[[1, 1, 1, 1], \frac{1}{24}\right], \left[[1, 1, 2], \frac{1}{4}\right], \left[[1, 3], \frac{1}{3}\right], \left[[2, 2], \frac{1}{8}\right], \left[[4], \frac{1}{4}\right]\right]$$

On penche plutot pour D4 à cause du type [1,3]

```
> P:=x^5+x^4-4*x^3-3*x^2+3*x+1: typeMod2(P,31);
```

$$\left[\left[[1, 1, 1, 1, 1], \frac{1}{10}\right], [[1, 1, 1, 2], 0], [[1, 1, 3], 0], [[1, 2, 2], 0], [[1, 4], 0], [[2, 3], 0], \left[[5], \frac{9}{10}\right]\right]$$

C5, D5 ou A5

```
> for G in [C5,D5,A5] do typesG(G); od;
```

$$\left[\left[[1, 1, 1, 1, 1], \frac{1}{5}\right], [[1, 1, 1, 2], 0], [[1, 1, 3], 0], [[1, 2, 2], 0], [[1, 4], 0], [[2, 3], 0], \left[[5], \frac{4}{5}\right]\right.$$

$$]$$

$$\left[\left[[1,1,1,1,1],\frac{1}{10}\right],[[1,1,1,2],0],[[1,1,3],0],\left[[1,2,2],\frac{1}{2}\right],[[1,4],0],[[2,3],0],\left[[5],\frac{2}{5}\right]\right]$$

$$\left[\left[[1,1,1,1,1],\frac{1}{60}\right],[[1,1,1,2],0],\left[[1,1,3],\frac{1}{3}\right],\left[[1,2,2],\frac{1}{4}\right],[[1,4],0],[[2,3],0],\left[[5],\frac{2}{5}\right]\right]$$

On penche plutot pour C5 à cause du type [5]

```
> P:=x^5-5*x+12: typeMod2(P,31);
```

$$\left[[[1,1,1,1,1],0],[[1,1,1,2],0],[[1,1,3],0],\left[[1,2,2],\frac{4}{9}\right],[[1,4],0],[[2,3],0],\left[[5],\frac{5}{9}\right]\right]$$

D5 ou A5

```
> for G in [D5,A5] do typesG(G); od;
```

$$\left[\left[[1,1,1,1,1],\frac{1}{10}\right],[[1,1,1,2],0],[[1,1,3],0],\left[[1,2,2],\frac{1}{2}\right],[[1,4],0],[[2,3],0],\left[[5],\frac{2}{5}\right]\right]$$

$$\left[\left[[1,1,1,1,1],\frac{1}{60}\right],[[1,1,1,2],0],\left[[1,1,3],\frac{1}{3}\right],\left[[1,2,2],\frac{1}{4}\right],[[1,4],0],[[2,3],0],\left[[5],\frac{2}{5}\right]\right]$$

On penche plutot pour D5 à cause du type [1,2,2]

```
> P:=x^5+2: typeMod2(P,31);
```

$$\left[[[1,1,1,1,1],0],[[1,1,1,2],0],[[1,1,3],0],\left[[1,2,2],\frac{2}{9}\right],\left[[1,4],\frac{5}{9}\right],[[2,3],0],\left[[5],\frac{2}{9}\right]\right]$$

M20 ou S5

```
> for G in [M20,S5] do typesG(G); od;
```

$$\left[\left[[1,1,1,1,1],\frac{1}{20}\right],[[1,1,1,2],0],[[1,1,3],0],\left[[1,2,2],\frac{1}{4}\right],\left[[1,4],\frac{1}{2}\right],[[2,3],0],\left[[5],\frac{1}{5}\right]\right]$$

$$\left[\left[[1,1,1,1,1],\frac{1}{120}\right],\left[[1,1,1,2],\frac{1}{12}\right],\left[[1,1,3],\frac{1}{6}\right],\left[[1,2,2],\frac{1}{8}\right],\left[[1,4],\frac{1}{4}\right],\left[[2,3],\frac{1}{6}\right],\left[[5],\frac{1}{5}\right]\right]$$

On penche plutot pour M20 à cause du type [1,4]

Question 7

```
> typeMod3:=proc(P,r) local p,F,S,L,d,pi,t,m,n; global x;
  if not(irreduc(P)) then error("P doit etre irreductible")
    else
    d:=discrim(P,x); pi:=0; n:=degree(P,x);
    S:=listetypes(n);
    for t in S do m[t]:=0; od;
    for p to r do
      if isprime(p) and d mod p<>0 then
        F := op(2, Factors(P) mod p);
        t:=sort([seq(degree(op(1,a),x),a=F)]);
        m[t]:=m[t]+1; pi:=pi+1;
      fi;
    od;
      d:=galois(P)[4];
      L:=[]; for t in S do
      L:=[op(L),[t,round(evalf(d*m[t]/pi))/d]] ;
    od;
  return(L);
  fi;
end:
```

```
> P:=x^4+x^3+x^2+x+1: typeMod3(P,100); typeMod3(P,1000);
```

$$\left[\left[[1,1,1,1],\frac{1}{4}\right],[[1,1,2],0],[[1,3],0],\left[[2,2],\frac{1}{4}\right],\left[[4],\frac{1}{2}\right]\right]$$

$$\left[\left[[1,1,1,1],\frac{1}{4}\right],[[1,1,2],0],[[1,3],0],\left[[2,2],\frac{1}{4}\right],\left[[4],\frac{1}{2}\right]\right]$$

```
> typesG(C4);
```

$$\left[\left[[1,1,1,1],\frac{1}{4}\right],[[1,1,2],0],[[1,3],0],\left[[2,2],\frac{1}{4}\right],\left[[4],\frac{1}{2}\right]\right]$$

```
> P:=x^5+2: typeMod3(P,100); typeMod3(P,1000);
```

$$\left[[[1,1,1,1,1],0],[[1,1,1,2],0],[[1,1,3],0],\left[[1,2,2],\frac{1}{5}\right],\left[[1,4],\frac{11}{20}\right],[[2,3],0],\left[[5],\frac{1}{5}\right]\right]$$

$$\left[\left[[1,1,1,1,1],\frac{1}{20}\right],[[1,1,1,2],0],[[1,1,3],0],\left[[1,2,2],\frac{1}{4}\right],\left[[1,4],\frac{11}{20}\right],[[2,3],0],\right.$$

$$\left[\left[[5], \frac{1}{5}\right]\right]$$

```
> typesG(M20);
```

$$\left[\left[[1, 1, 1, 1, 1], \frac{1}{20}\right], [[1, 1, 1, 2], 0], [[1, 1, 3], 0], \left[[1, 2, 2], \frac{1}{4}\right], \left[[1, 4], \frac{1}{2}\right], [[2, 3], 0], \left[[5], \frac{1}{5}\right]\right]$$

Question 8

```
> P:=x[2]*x[3]^2+x[3]*x[1]+x[3]^2*x[1]+x[1]*x[4]:
  sort(P,[seq(x[i],i=1..4)],tdeg);
```

$$x_1 x_3^2 + x_2 x_3^2 + x_1 x_3 + x_1 x_4$$

On reprend la procédure image du TP4B :

```
> image:=proc(g,n,i) local c,l,j;
      for c in g do
      l:=nops(c);
      for j from 1 to l do
        if op(j,c)=i then if j=l then return(op(1,c)) else
  return(op(j+1,c)); fi; fi;
      od;
    od;
    return(i);
  end:
> action_poly:=proc(P,n,g)  local S,i:
   S:={} ;
   for i from 1 to n do
     S:=S union {x[i]=x[image(g,n,i)]}
   od;
   return(sort(subs(S,P),[seq(x[i],i=1..n)],tdeg));
  end:
> g:=[[1,2,3],[4,5]]: action_poly(P,5,g);
```

$$x_1^2 x_2 + x_1^2 x_3 + x_1 x_2 + x_2 x_5$$

```
> sym:=proc(G,P) local n,GG,L,F,g;
    n:=op(1,G); GG:=elements(G);
    F:=0; for g in GG do F:=F+action_poly(P,n,g); od;
    return(sort(F,[seq(x[i],i=1..n)],tdeg));
  end:
> F:=sym(D4,x[1]*x[2]);
```

$$F := 2\,x_1 x_2 + 2\,x_1 x_4 + 2\,x_2 x_3 + 2\,x_3 x_4$$

```
> evalb(x[1]*(x[2]+x[3])=x[1]*x[2]+x[1]*x[3]);
```

false

Il est nécessaire de mettre au préalable sous une forme permettant la comparaison :

```
> evalb(sort(expand(x[1]*(x[2]+x[3])),[seq(x[i],i=1..3)],tdeg)=
  x[1]*x[2]+x[1]*x[3]);
```

true

```
> invariant?:=proc(P,n,g);
    if
  sort(expand(action_poly(P,n,g)),[seq(x[i],i=1..n)],tdeg)=sort
  (expand(P),[seq(x[i],i=1..n)],tdeg)
      then return(true) else return(false);
    fi;
  end:
> invariant?(P,5,g); invariant?(sym(permgroup(5,{g}),P),5,g);
```

false

true

```
> invariantG?:=proc(G,P) local n,S,g;
    n:=op(1,G); S:=op(2,G);
    for g in S do
      if not(invariant?(P,n,g)) then return(false); fi;
    od;
    return(true);
  end:
> invariantG?(C4,F); invariantG?(D4,F); invariantG?(S4,F);
```

true

true

false

La procédure (naive) de calcul du stabilisateur (ce n'est pas important d'optimiser car nous l'appliquerons sur des groupes de permutations de petits degrés) :

```
> S:=proc(n);
    if n=2 then return(permgroup(2,{[[1,2]]})) else
  return(permgroup(n,{[[1,2]],[[$1..n]]})); fi;
  end:
> stab:=proc(P,n)
    local g,G,H;
    G:=elements(S(n)); H:={};
    for g in G do
      if invariant?(P,n,g) then H:=H union {g}; fi;
    od;
    return(H);
  end:
> stab(P,5); G:=stab(F,4);
```

{[ ]}

$G :=$ {
[[1, 4, 3, 2]], [ ], [[1, 2], [3, 4]], [[1, 4], [2, 3]], [[1, 3]], [[1, 2, 3, 4]], [[2, 4]], [[1, 3], [2, 4]]
}

```
> nops(G);
```

8

```
> evalb(elements(G)=elements(D4));
```

true

Question 9

```
> sym_elem:=proc(n)  local P,S,i;
    if n=1 then return({s[1]=x[1]});
      else P:=collect(expand(mul(x+x[i],i=1..n)),x);
      return({seq(s[i]=coeff(P,x,n-i),i=1..n)});
    fi;
```

```
end:
> sym_elem(1); sym_elem(4);
```

$$\{s_1 = x_1\}$$

$$\{s_1 = x_2 + x_1 + x_4 + x_3,\ s_2 = x_1 x_2 + x_2 x_4 + x_2 x_3 + x_1 x_4 + x_1 x_3 + x_3 x_4,$$
$$s_3 = x_1 x_2 x_4 + x_1 x_2 x_3 + x_2 x_3 x_4 + x_1 x_3 x_4,\ s_4 = x_1 x_2 x_3 x_4\}$$

```
> subs(sym_elem(4),s[1]^2*s[2]);
```

$$(x_2 + x_1 + x_4 + x_3)^2 (x_1 x_2 + x_2 x_4 + x_2 x_3 + x_1 x_4 + x_1 x_3 + x_3 x_4)$$

```
> normal((x[1]^2*x[2]+x[2]^2*x[1])/(x[1]*x[2]));
```

$$x_1 + x_2$$

```
> P; degree(P,{seq(x[i],i=1..4)});
```

$$x_1 x_3^2 + x_2 x_3^2 + x_1 x_3 + x_1 x_4$$

$$3$$

```
> convert_sym:=proc(P,n)
    local g1,P1,P2;
    if degree(P,{seq(x[i],i=1..n)})<=0
      then return(P)
      else g1:=convert_sym(subs(x[n]=0,P),n-1);
      P1:=subs(sym_elem(n),P-g1);
      P2:=convert_sym(normal(P1/mul(x[i],i=1..n)),n);
      return(g1+s[n]*P2);
    fi;
  end:
> convert_sym((x[1]+x[2]+x[3]+x[4])^2,4);
```

$$s_1^2$$

```
> convert_sym(sym(S4,x[1]^2*x[2]),4);
```

$$2\, s_2\, s_1 - 6\, s_3$$

Question 10

```
> F:=sym(D4,mul(x[i]^(4-i),i=1..3)): G:=stab(F,4):
  evalb(nops(G)=grouporder(D4));
```

true

Cela montre que le corps des invariants de Q(x1,...,x4) sous D4 est engendré sur Q(s1,...,s4) par F

```
> F:=sym(C4,mul(x[i]^(4-i),i=1..3)): G:=stab(F,4):
  evalb(nops(G)=grouporder(C4));
```

true

Cela montre que le corps des invariants de Q(x1,...,x4) sous C4 est engendré sur Q(s1,...,s4) par F

Au papier-crayon, on démontre que le stablisateur de F=sym(H,x_1^(n-1)...x_{n-1}) est H, donc que le corps des invariants de Q(x1,...xn) sous H est Q(s1,...sn)(F), pour tout sous-groupe H de Sn.

```
> d:=n->mul(mul(x[i]-x[j],i=1..j-1),j=1..n):
> d(4);
```

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)(x_1 - x_4)(x_2 - x_4)(x_3 - x_4)$$

```
> action_poly(d(4),4,[[1,2,3]]); invariant?(d(4),4,[[1,2,3]]);
```

$$(x_2 - x_3)(-x_1 + x_2)(-x_1 + x_3)(x_2 - x_4)(x_3 - x_4)(x_1 - x_4)$$

true

```
> evalb(nops(stab(d(4),4))=grouporder(A4));
```

true

```
> for n from 5 to 6 do evalb(nops(stab(d(n),n))=n!/2); od;
```

true

true

Question 11

```
> resolvante:=proc(F,G) #F est supposé symétrique
    local n,H,L,h,l;
    n:=op(1,G);
    if not(nops(stab(F,n))=grouporder(G)) then error("cet
  élément n'est pas primitif")
      else H:=cosets(S(n),G);
      L:=[seq(action_poly(F,n,h),h=H)];
      return(mul(x-l,l=L));
    fi;
  end:
> F:=sym(D4,x[1]); resolvante(F,D4);
```

$$F := 2\, x_1 + 2\, x_2 + 2\, x_3 + 2\, x_4$$

```
Error, (in resolvante) cet élément n'est pas primitif
```

```
> F:=sym(D4,mul(x[i]^(4-i),i=1..3)): R:=resolvante(F,D4);
```

$$R := (x - x_1^3 x_2 x_3^2 - x_1^3 x_2 x_4^2 - x_1^2 x_3^3 x_4 - x_1^2 x_3 x_4^3 - x_1 x_2^3 x_3^2 - x_1 x_2^3 x_4^2 - x_2^2 x_3^3 x_4$$
$$- x_2^2 x_3 x_4^3)(x - x_1^3 x_2^2 x_3 - x_1^3 x_3 x_4^2 - x_1^2 x_2^3 x_4 - x_1^2 x_2 x_4^3 - x_1 x_2^2 x_3^3 - x_1 x_3^3 x_4^2$$
$$- x_2^3 x_3^2 x_4 - x_2 x_3^2 x_4^3)(x - x_1^3 x_2^2 x_4 - x_1^3 x_3^2 x_4 - x_1^2 x_2^3 x_3 - x_1^2 x_2 x_3^3 - x_1 x_2^2 x_4^3$$
$$- x_1 x_3^2 x_4^3 - x_2^3 x_3 x_4^2 - x_2 x_3^3 x_4^2)$$

```
> collect(expand(%),x);
```

$$-x_1^3 x_2^9 x_3^5 x_4 - 2\, x_1^3 x_2^7 x_3^7 x_4 - 4\, x_1^8 x_2^4 x_3^2 x_4^4 - 4\, x_1^8 x_2^2 x_3^4 x_4^4 - 8\, x_1^7 x_2^5 x_3^3 x_4^3$$
$$- 8\, x_1^7 x_2^3 x_3^5 x_4^3 - 8\, x_1^6 x_2^4 x_3^2 x_4^6 - 8\, x_1^6 x_2^2 x_3^4 x_4^6 - 14\, x_1^5 x_2^5 x_3^3 x_4^5$$
$$- 14\, x_1^5 x_2^3 x_3^5 x_4^5 - 8\, x_1^5 x_2^7 x_3^3 x_4^3 - 14\, x_1^5 x_2^5 x_3^5 x_4^3 - 4\, x_1^4 x_2^8 x_3^4 x_4^2$$
$$- 8\, x_1^4 x_2^6 x_3^6 x_4^2 - 8\, x_1^3 x_2^7 x_3^3 x_4^5 - 14\, x_1^3 x_2^5 x_3^5 x_4^5 - 4\, x_1^2 x_2^8 x_3^4 x_4^4 - 8\, x_1^2 x_2^6 x_3^6 x_4^4$$
$$- 2\, x_1^6 x_2^8 x_3^2 x_4^2 - 8\, x_1^6 x_2^6 x_3^4 x_4^2 - x_1^5 x_2^9 x_3^3 x_4 - 4\, x_1^5 x_2^7 x_3^5 x_4 - 4\, x_1^4 x_2^8 x_3^2 x_4^4$$
$$- 14\, x_1^4 x_2^6 x_3^4 x_4^4 - 2\, x_1^3 x_2^9 x_3^3 x_4^3 - 8\, x_1^3 x_2^7 x_3^5 x_4^3 - 8\, x_1^6 x_3^6 x_4^2 x_2^4 - 2\, x_1^6 x_3^8 x_4^2 x_2^2$$
$$- 4\, x_1^5 x_3^7 x_4 x_2^5 - x_1^5 x_3^9 x_4 x_2^3 - 4\, x_1 x_2^7 x_4^5 x_3^5 - 4\, x_2^4 x_3^8 x_4^2 x_1^4 - x_2^5 x_3^9 x_4 x_1^3$$
$$- 4\, x_2^4 x_3^8 x_4^4 x_1^2 - x_2^5 x_3^9 x_4^3 x_1 - 14\, x_2^4 x_3^6 x_4^4 x_1^4 - 4\, x_2^2 x_3^8 x_4^4 x_1^4 - 8\, x_2^5 x_3^7 x_4^3 x_1^3$$
$$- 2\, x_2^3 x_3^9 x_4^3 x_1^3 - 8\, x_2^4 x_3^6 x_4^6 x_1^2 - 2\, x_2^2 x_3^8 x_4^6 x_1^2 - 4\, x_2^5 x_3^7 x_4^5 x_1 - x_2^3 x_3^9 x_4^5 x_1$$

$$-4 x_2^5 x_3 x_4^7 x_1^5 - 8 x_2^3 x_3^3 x_4^7 x_1^5 - 8 x_2^6 x_3^2 x_4^6 x_1^4 - 14 x_2^4 x_3^4 x_4^6 x_1^4 - x_2^5 x_3 x_4^9 x_1^3$$
$$-2 x_2^3 x_3^3 x_4^9 x_1^3 - 2 x_2^6 x_3^2 x_4^8 x_1^2 - 4 x_2^4 x_3^4 x_4^8 x_1^2 - 8 x_2^2 x_3^6 x_4^6 x_1^4 - 8 x_2^3 x_3^7 x_4^5 x_1^3$$
$$-2 x_2^2 x_3^6 x_4^8 x_1^2 - 4 x_2^5 x_3^5 x_4^7 x_1 - 2 x_2^3 x_3^7 x_4^7 x_1 - 4 x_1^5 x_3^7 x_4^5 x_2 - 8 x_1^3 x_3^5 x_4^7 x_2^3$$
$$-2 x_1^3 x_3^7 x_4^7 x_2 - 2 x_1^7 x_3 x_4^7 x_2^3 - 2 x_1^7 x_3^3 x_4^7 x_2 - x_1^5 x_3 x_4^9 x_2^3 - x_1^5 x_3^3 x_4^9 x_2$$
$$-4 x_1^4 x_3^2 x_4^8 x_2^4 - 4 x_1^4 x_3^4 x_4^8 x_2^2 - 4 x_1^5 x_3^5 x_4^7 x_2 - x_1^3 x_3^5 x_4^9 x_2 - x_1^9 x_2^5 x_4^3 x_3$$
$$-2 x_1^9 x_2^3 x_4^3 x_3^3 - 2 x_1^8 x_2^6 x_4^2 x_3^2 - 4 x_1^8 x_2^4 x_4^2 x_3^4 - x_1 x_2^9 x_3^5 x_4^3 - 2 x_1 x_2^7 x_3^7 x_4^3$$
$$-2 x_1^2 x_2^8 x_4^6 x_3^2 - 8 x_1^2 x_2^6 x_4^6 x_3^4 - x_1 x_2^9 x_4^5 x_3^3 - x_2^6 x_3^4 x_4^8 - x_1^8 x_2^4 x_3^6 - x_1^8 x_2^6 x_3^4$$
$$-x_1^6 x_2^4 x_3^8 - 2 x_1^6 x_2^6 x_3^6 - 2 x_1^6 x_2^6 x_4^6 - x_1^8 x_2^6 x_4^4 - x_1^6 x_2^4 x_4^8 - x_1^8 x_2^4 x_4^6$$
$$-x_1^8 x_3^6 x_4^4 - x_1^4 x_3^8 x_4^6 - x_1^6 x_3^8 x_4^4 - x_1^6 x_3^4 x_4^8 - x_1^8 x_3^4 x_4^6 - x_1^4 x_3^6 x_4^8 - 2 x_1^6 x_3^6 x_4^6$$
$$-x_2^4 x_3^8 x_4^6 - 2 x_2^6 x_3^6 x_4^6 - x_2^8 x_3^4 x_4^6 - x_2^4 x_3^6 x_4^8 - x_2^8 x_3^6 x_4^4 - 4 x_1^7 x_2^5 x_4^5 x_3$$
$$-8 x_1^7 x_2^3 x_4^5 x_3^3 - 8 x_1^6 x_2^6 x_4^4 x_3^2 - 14 x_1^6 x_2^4 x_4^4 x_3^4 - x_1^9 x_2^3 x_4^5 x_3 - x_1^9 x_2 x_4^5 x_3^3$$
$$-2 x_1 x_2^7 x_3^3 x_4^7 - 4 x_1^5 x_2^7 x_3 x_4^5 - 2 x_1^3 x_2^7 x_3 x_4^7 - 8 x_1^3 x_2^5 x_3^3 x_4^7 - 8 x_1^6 x_2^2 x_3^6 x_4^4$$
$$-8 x_1^5 x_2^3 x_3^7 x_4^3 - x_1^9 x_2 x_3^5 x_4^3 - 2 x_1^8 x_2^2 x_3^6 x_4^2 - 4 x_1^7 x_2 x_3^5 x_4^5 - x_2^6 x_3^8 x_4^4$$
$$-2 x_1^7 x_2^7 x_3^3 x_4 - 4 x_1^7 x_2^5 x_3^5 x_4 - 2 x_1^8 x_3^2 x_4^6 x_2^2 - 2 x_1^6 x_3^2 x_4^8 x_2^2 - x_1^6 x_2^8 x_3^4$$
$$-x_1^4 x_2^6 x_3^8 - x_1^4 x_2^8 x_3^6 - x_1^4 x_2^8 x_4^6 - x_1^6 x_2^8 x_4^4 - x_1^4 x_2^6 x_4^8 + x^3 + (2 x_1^5 x_2^2 x_3^3 x_4^2$$
$$+2 x_1^5 x_2^2 x_3^2 x_4^3 + 2 x_1^2 x_2^5 x_3^3 x_4^2 + 2 x_1^3 x_2^4 x_3 x_4^4 + 2 x_1^4 x_2^4 x_3 x_4^3 + 3 x_1^3 x_2^3 x_3^4 x_4^2$$
$$+x_1^3 x_2^6 x_3^2 x_4 + x_1 x_2^6 x_3^4 x_4 + x_1 x_2^6 x_4^3 x_3^2 + x_2^4 x_3^6 x_4 x_1 + x_2^2 x_3^6 x_4^3 x_1 + x_2^3 x_3 x_4^6 x_1^2$$
$$+x_2^2 x_3^4 x_4^5 x_1 + x_1^3 x_3^6 x_4 x_2^2 + x_1^2 x_3^5 x_4^4 x_2 + x_1^4 x_3 x_4^6 x_2 + x_1^2 x_3^3 x_4^6 x_2 + x_1^6 x_2^3 x_4^2 x_3$$
$$+x_1^6 x_2 x_4^4 x_3 + 2 x_1 x_2^4 x_3^4 x_4^3 + 3 x_1^4 x_2^2 x_3^3 x_4^3 + x_1^2 x_2^4 x_3 x_4^5 + x_1 x_2^4 x_3^2 x_4^5$$
$$+x_1^2 x_2^5 x_3 x_4^4 + x_1 x_2^5 x_3^2 x_4^4 + 2 x_1^4 x_2^3 x_3 x_4^4 + 3 x_1^3 x_2^2 x_3^4 x_4^3 + x_1^6 x_2 x_3^3 x_4^2$$
$$+3 x_1^2 x_2^3 x_3^3 x_4^4 + x_1^5 x_2^4 x_3^2 x_4 + 2 x_1^4 x_2^3 x_3^4 x_4 + 3 x_1^2 x_2^3 x_3^4 x_4^3 + 2 x_1^3 x_2^2 x_3^2 x_4^5$$
$$+2 x_1^3 x_2^5 x_3^2 x_4^2 + x_1^5 x_2^4 x_3 x_4^2 + x_1^3 x_3^4 x_4^5 + x_1^5 x_3^2 x_4^5 + x_1^3 x_3^6 x_4^3 + x_1^5 x_3^4 x_4^3$$
$$+x_1^5 x_2^2 x_4^5 + x_1^5 x_2^4 x_4^3 + x_1^4 x_2^3 x_3^5 + x_1^6 x_2^3 x_3^3 + x_2^3 x_3^3 x_4^6 + x_2^5 x_3^3 x_4^4 + x_2^3 x_3^5 x_4^4$$
$$+x_2^5 x_3^5 x_4^2 + x_1^3 x_2^4 x_4^5 + x_1^3 x_2^6 x_4^3 + x_1^2 x_2^5 x_3^5 + x_1^4 x_2^5 x_3^3 + x_1^5 x_2^2 x_3^4 x_4$$
$$+x_1^4 x_2^2 x_3^5 x_4 + x_1^2 x_3^6 x_4^3 x_2 + x_1^5 x_3 x_4^4 x_2^2 + x_1^3 x_3 x_4^6 x_2^2 + 2 x_1^2 x_3^2 x_4^5 x_2^3$$
$$+x_1^2 x_3^4 x_4^5 x_2 + x_1 x_2^6 x_3^3 x_4^2 + x_1 x_2^4 x_3^5 x_4^2 + x_1^3 x_2^6 x_4^2 x_3 + x_1 x_2^6 x_4^4 x_3 + 2 x_1 x_2^4 x_4^4 x_3^3$$
$$+x_2^5 x_3^4 x_4 x_1^2 + x_2^3 x_3^6 x_4 x_1^2 + x_2^2 x_3^5 x_4^4 x_1 + x_2^4 x_3 x_4^6 x_1 + x_2^2 x_3^3 x_4^6 x_1 + x_1^3 x_2^5 x_4^4$$
$$+x_1^5 x_2^5 x_4^2 + x_1^4 x_3^3 x_4^5 + x_1^6 x_3^3 x_4^3 + x_1^5 x_2^3 x_3^4 + x_1^5 x_2^5 x_3^2 + x_1^3 x_2^3 x_4^6 + x_1^5 x_2^3 x_4^4$$
$$+x_1^3 x_2^3 x_3^6 + x_1^3 x_2^5 x_3^4 + x_2^6 x_3^3 x_4^3 + x_1^2 x_3^5 x_4^5 + x_1^4 x_3^5 x_4^3 + x_2^4 x_3^5 x_4^3 + x_1^3 x_3^3 x_4^6$$
$$+x_2^3 x_3^4 x_4^5 + x_2^5 x_3^2 x_4^5 + x_2^3 x_3^6 x_4^3 + x_2^5 x_3^4 x_4^3 + x_1^2 x_2^5 x_4^5 + x_1^4 x_2^5 x_4^3 + x_1^3 x_2^4 x_3^5$$
$$+x_1^3 x_2^6 x_3^3 + x_1^5 x_3^3 x_4^4 + x_1^3 x_3^5 x_4^4 + x_1^5 x_3^5 x_4^2 + x_1^4 x_2^3 x_4^5 + x_1^6 x_2^3 x_4^3 + x_1^5 x_2^2 x_3^5$$
$$+x_1^5 x_2^4 x_3^3 + x_2^2 x_3^5 x_4^5 + x_2^4 x_3^3 x_4^5 + 2 x_1^2 x_2^2 x_3^5 x_4^3 + 2 x_1^5 x_2^3 x_3^2 x_4^2$$
$$+2 x_1^2 x_2^2 x_3^3 x_4^5 + 2 x_1 x_2^3 x_3^4 x_4^4 + 3 x_1^4 x_2^3 x_3^3 x_4^2 + x_1 x_3^6 x_4^4 x_2 + x_2^6 x_3^3 x_4 x_1^2$$
$$+x_2^4 x_3^5 x_4 x_1^2 + x_2^3 x_3^2 x_4^6 x_1 + x_2 x_3^4 x_4^6 x_1 + x_1^6 x_2^3 x_3^2 x_4 + x_1^6 x_2 x_3^4 x_4 + 3 x_1^4 x_2^3 x_3^2 x_4^3$$
$$+2 x_1^4 x_2 x_3^4 x_4^3 + 3 x_1^3 x_2^4 x_3^3 x_4^2 + 2 x_1^3 x_2^2 x_3^5 x_4^2 + x_1^6 x_2 x_4^3 x_3^2 + x_1^4 x_2 x_4^5 x_3^2$$
$$+x_1^4 x_3^6 x_4 x_2 + 2 x_1^3 x_2 x_3^4 x_4^4 + 2 x_1^4 x_2^4 x_3^3 x_4 + 2 x_1^4 x_2 x_3^3 x_4^4 + 3 x_1^3 x_2^4 x_3^2 x_4^3$$
$$+3 x_1^2 x_2^4 x_3^3 x_4^3 + 2 x_1^2 x_2^3 x_3^5 x_4^2 + x_1^5 x_2 x_3^4 x_4^2 + x_1^4 x_2 x_3^5 x_4^2 + 3 x_1^3 x_2^3 x_3^2 x_4^4$$
$$+3 x_1^3 x_2^2 x_3^3 x_4^4 + x_1^4 x_2^5 x_3 x_4^2 + 2 x_1^3 x_2^4 x_3^4 x_4 + 2 x_1^2 x_2^5 x_3^2 x_4^3 + x_1^4 x_2^5 x_3^2 x_4$$
$$+x_1^6 x_2^4 x_3 x_4 + x_1^6 x_2^2 x_3^3 x_4 + x_1^6 x_3 x_4^3 x_2^2 + x_1^4 x_3 x_4^5 x_2^2 + x_1^4 x_2^6 x_4 x_3 + x_1^2 x_2^6 x_4^3 x_3$$
$$+x_1^5 x_2 x_4^4 x_3^2 + x_1^3 x_2 x_4^6 x_3^2 + x_1 x_2^5 x_3^4 x_4^2 + x_1 x_2^3 x_3^6 x_4^2 + x_1^3 x_3^6 x_4^2 x_2) x + (-x_1^3 x_2 x_4^2$$
$$-x_1^3 x_2^2 x_3 - x_1^2 x_2 x_3^3 - x_1^2 x_3^3 x_4 - x_1^2 x_3 x_4^3 - x_1^2 x_2 x_4^3 - x_1 x_2^3 x_4^2 - x_1^3 x_2^2 x_4$$
$$-x_1 x_2^2 x_3^3 - x_2^2 x_3 x_4^3 - x_2^2 x_3^3 x_4 - x_1 x_3^3 x_4^2 - x_1^3 x_3 x_4^2 - x_1 x_2^3 x_3^2 - x_2^3 x_3^2 x_4$$
$$-x_1^2 x_2^3 x_4 - x_1^3 x_2 x_3^2 - x_2 x_3^2 x_4^3 - x_1^3 x_3^2 x_4 - x_1^2 x_2^3 x_3 - x_2 x_3^3 x_4^2 - x_1 x_2^2 x_4^3$$
$$-x_1 x_3^2 x_4^3 - x_2^3 x_3 x_4^2) x^2 - x_1^5 x_3^9 x_4^3 x_2 - x_1^3 x_3^9 x_4^5 x_2 - 2 x_1^7 x_3^7 x_4^3 x_2 - 2 x_1^7 x_2^7 x_4^3 x_3$$
$$-2 x_1^7 x_2^3 x_3^7 x_4 - x_1^9 x_2^5 x_3^3 x_4 - x_1^9 x_2^3 x_3^5 x_4 - x_2^5 x_3^3 x_4^9 x_1 - x_2^3 x_3^5 x_4^9 x_1$$
$$-2 x_2^8 x_3^6 x_4^2 x_1^2 - 2 x_2^6 x_3^8 x_4^2 x_1^2 - x_1^5 x_2^9 x_4^3 x_3 - x_1^3 x_2^9 x_4^5 x_3$$

Que c'est long !

```
> collect(convert_sym(expand(R),4),x);
```

$$x^3 + (s_3 (-s_2 s_1 + 3 s_3) + s_4 (3 s_1^2 - 4 s_2)) x^2 + (s_3^2 (s_2^3 + s_3 (s_1^3 - 5 s_2 s_1 + 3 s_3))$$
$$+ s_4 (s_3 (s_2 (-5 s_1^3 + 16 s_2 s_1) + s_3 (2 s_1^2 - 8 s_2)) + s_4 (-8 s_2 s_1^2 + 3 s_1^4) + s_2^3 (s_1^2 - 4 s_2))) x +$$
$$s_4 (s_4 (s_4 (s_1^6 - 4 s_2 s_1^4) + s_2^3 (2 s_1^4 + s_2 (-12 s_1^2 + 16 s_2))$$
$$+ s_3 (s_2 (-4 s_1^5 + s_2 (24 s_1^3 - 32 s_2 s_1)) + s_3 (-s_1^4 + 8 s_2 s_1^2)))$$
$$+ s_3^2 (s_2^2 (-s_1^4 + s_2 (8 s_1^2 - 12 s_2)) + s_3 (2 s_1^5 + s_2 (-16 s_1^3 + 24 s_2 s_1) + s_3 (-s_1^2 - 4 s_2))))$$

$$+ s_3^{4} (s_2^{2} (-s_1^{2} + 2 s_2) + s_3 (2 s_1^{3} - 4 s_2 s_1 + s_3))$$

C'est bien un polynome de Q(s1,...s4)[x]

```
> resolvante_f:=proc(f,G) #f est quelconque

  return(convert_sym(expand(resolvante(sym(G,f),G)),op(1,G)));
  end:
> resolvante_f(x[1]*x[2],D4);
```

$$x^{3} + s_2 (-4 x^{2} + 4 s_2 x) + s_3 (4 s_1 x - 8 s_2 s_1 + 8 s_3) + s_4 (-16 x + 8 s_1^{2})$$

```
> collect(%,x);
```

$$x^{3} - 4 s_2 x^{2} + (4 s_3 s_1 - 16 s_4 + 4 s_2^{2}) x + 8 s_4 s_1^{2} + s_3 (-8 s_2 s_1 + 8 s_3)$$

C'est un élément qui donne une résolvante bien plus simple !

```
> resolvante_f(x[1]*x[2],C4);
Error, (in resolvante) cet élément n'est pas primitif
> resolvante_f(x[1]^2*x[2],C4);
```

$$x^{6} + s_2 (-2 s_1 x^{5} + s_2 (s_1^{2} x^{4} + s_2 (2 x^{4} + s_2 (-2 s_1 x^{3} + s_2^{2} x^{2})))) + s_3 (6 x^{5} + 2 s_1^{3} x^{4} + s_2 ($$
$$s_1 (-17 x^{4} - 2 s_1^{3} x^{3}) + s_2 (10 s_1^{2} x^{3} + s_2 (8 x^{3} + 3 s_1^{3} x^{2} + s_2 (-13 s_1 x^{2} + s_2 (-s_1^{2} x + 2 s_2 x))))$$
$$) + s_3 (24 x^{4} + s_1^{3} (8 x^{3} + s_1^{3} x^{2}) +$$
$$s_2 (s_1 (-54 x^{3} - 13 s_1^{3} x^{2}) + s_2 (s_1^{2} (33 x^{2} - s_1^{3} x) + s_2 (22 x^{2} + 10 s_1^{3} x + s_2 (-19 s_1 x + s_2^{2}))))$$
$$+ s_3 (56 x^{3} + s_1^{3} (22 x^{2} + 2 s_1^{3} x)$$
$$+ s_2 (s_1 (-116 x^{2} - 19 s_1^{3} x) + s_2 (34 s_1^{2} x + s_2 (28 x + 2 s_1^{3} - 12 s_2 s_1))) + s_3 (96 x^{2}$$
$$+ s_1^{3} (28 x + s_1^{3}) + s_2 (s_1 (-128 x - 12 s_1^{3}) + s_2 (36 s_1^{2} + 16 s_2))$$
$$+ s_3 (96 x + 16 s_1^{3} - 96 s_2 s_1 + 64 s_3))))) + s_4 (s_1^{2} (x^{4} - 2 s_1^{3} x^{3}) + s_2 (-8 x^{4}$$
$$+ s_1^{3} (10 x^{3} + 2 s_1^{3} x^{2})$$
$$+ s_2 (-11 s_1^{4} x^{2} + s_2 (s_1^{2} (10 x^{2} - 2 s_1^{3} x) + s_2 (-12 x^{2} + 9 s_1^{3} x + s_2 (s_1^{4} - 4 s_2 s_1^{2}))))) + s_3 ($$
$$s_1^{2} (-12 x^{3} + s_1^{3} (-5 x^{2} - 2 s_1^{3} x)) + s_2 (-32 x^{3} + s_1^{3} (30 x^{2} + 22 s_1^{3} x)$$
$$+ s_2 (s_1 (48 x^{2} + s_1^{3} (-60 x + s_1^{3})) + s_2 (s_1^{2} (-4 x - 12 s_1^{3}) + s_2 (-24 x + 29 s_1^{3} + 16 s_2 s_1)))) +$$
$$s_3 (s_1^{2} (-36 x^{2} + s_1^{3} (-29 x - 2 s_1^{3}))$$
$$+ s_2 (-120 x^{2} + s_1^{3} (134 x + 17 s_1^{3}) + s_2 (s_1 (120 x - 6 s_1^{3}) + s_2 (-134 s_1^{2} - 28 s_2)))$$
$$+ s_3 (s_1^{2} (-104 x - 22 s_1^{3}) + s_2 (-176 x + 48 s_1^{3} + 296 s_2 s_1) + s_3 (-48 s_1^{2} - 224 s_2)))) + s_4 ($$
$$s_1 (32 x^{3} + s_1^{3} (7 x^{2} + s_1^{3} (-x + s_1^{3})))$$
$$+ s_2 (s_1^{2} (-72 x^{2} - 11 s_1^{6}) + s_2 (48 x^{2} + s_1^{3} (24 x + 45 s_1^{3}) + s_2 (-76 s_1^{4} + 32 s_2 s_1^{2}))) + s_3 ($$
$$s_1 (144 x^{2} + s_1^{3} (38 x + 15 s_1^{3})) + s_2 (s_1^{2} (-288 x - 133 s_1^{3}) + s_2 (96 x + 344 s_1^{3} - 128 s_2 s_1))$$
$$+ s_3 (s_1 (336 x + 128 s_1^{3}) + s_2 (-648 s_1^{2} + 176 s_2) + 416 s_3 s_1)) + s_4$$
$$(-64 x^{2} + s_1^{3} (16 x - 5 s_1^{3}) + s_2 (32 s_1^{4} - 64 s_2 s_1^{2}) + s_3 (-128 x - 48 s_1^{3} + 256 s_2 s_1 - 320 s_3))$$
$$))$$

```
> resolvante_f(x[1]*x[2],V4);
Error, (in resolvante) cet élément n'est pas primitif
> resolvante_f(x[1]^2*x[2],V4);
Error, (in resolvante) cet élément n'est pas primitif
> resolvante_f(x[1]^3*x[2]^2*x[3],V4);
```

$$x^{6} + s_3 (-s_2 s_1 x^{5} + s_3 (3 x^{5} + s_2^{3} x^{4} + s_3 (s_1^{3} x^{4} - 5 s_2 s_1 x^{4} + s_3 (6 x^{4} + s_2^{2} (-s_1^{2} x^{3} + 2 s_2 x^{3}) +$$
$$s_3 (2 s_1^{3} x^{3} - 6 s_2 s_1 x^{3}$$
$$+ s_3 (7 x^{3} + s_2^{3} x^{2} + s_3 (s_1^{3} x^{2} - 5 s_2 s_1 x^{2} + s_3 (6 x^{2} + s_3 (-s_2 s_1 x + s_3 (3 x + s_3^{2}))))))))) + s_4 ($$
$$3 s_1^{2} x^{5} + s_2 (-4 x^{5} + s_2^{2} (s_1^{2} x^{4} - 4 s_2 x^{4})) + s_3 (s_2 (-5 s_1^{3} x^{4} + 16 s_2 s_1 x^{4}) + s_3 (4 s_1^{2} x^{4}$$
$$+ s_2 (-24 x^{4} + s_2 (-s_1^{4} x^{3} + s_2 (8 s_1^{2} x^{3} - 12 s_2 x^{3}))) + s_3 (2 s_1^{5} x^{3}$$
$$+ s_2 (-18 s_1^{3} x^{3} + 38 s_2 s_1 x^{3}) + s_3 (7 s_1^{2} x^{3} + s_2 (-50 x^{3} + s_2^{2} (s_1^{2} x^{2} - 8 s_2 x^{2})) + s_3 (2 s_1^{5} x^{2}$$
$$+ s_2 (-19 s_1^{3} x^{2} + 48 s_2 s_1 x^{2}) + s_3$$
$$(12 s_1^{2} x^{2} - 62 s_2 x^{2} + s_3 (s_2 (-2 s_1^{3} x + 14 s_2 s_1 x) + s_3 (5 s_1^{2} x - 42 s_2 x + s_3^{2} (2 s_1^{2} - 16 s_2))))$$
$$))))) + s_4 (6 s_1^{4} x^{4} + s_2 (-24 s_1^{2} x^{4} + s_2 (20 x^{4} + s_2 (2 s_1^{4} x^{3} + s_2 (-12 s_1^{2} x^{3} + 16 s_2 x^{3})))) + s_3 ($$
$$24 s_1 x^{4} + s_2 (-6 s_1^{5} x^{3} + s_2 (38 s_1^{3} x^{3} - 60 s_2 s_1 x^{3})) + s_3 (7 s_1^{4} x^{3}$$
$$+ s_2 (-64 s_1^{2} x^{3} + s_2 (108 x^{3} + s_2 (s_1^{4} x^{2} + s_2 (-8 s_1^{2} x^{2} + 20 s_2 x^{2})))) + s_3 (s_1 (44 x^{3} + s_1^{6} x^{2})$$
$$+ s_2 (-19 s_1^{5} x^{2} + s_2 (96 s_1^{3} x^{2} - 140 s_2 s_1 x^{2})) + s_3 (16 s_1^{4} x^{2} + s_2 (-138 s_1^{2} x^{2} + 216 s_2 x^{2}) +$$
$$s_3 (60 s_1 x^{2} + s_2 (-2 s_1^{5} x + s_2 (22 s_1^{3} x - 68 s_2 s_1 x)) + s_3$$
$$(8 s_1^{4} x + s_2 (-84 s_1^{2} x + 220 s_2 x) + s_3 (48 s_1 x + s_3 (3 s_1^{4} + s_2 (-32 s_1^{2} + 104 s_2) + 16 s_3 s_1)))))$$
$$))) + s_4 (-32 x^{4} + 7 s_1^{6} x^{3} +$$
$$s_2 (-50 s_1^{4} x^{3} + s_2 (108 s_1^{2} x^{3} + s_2 (-64 x^{3} + s_1^{6} x^{2} + s_2 (-8 s_1^{4} x^{2} + s_2 (20 s_1^{2} x^{2} - 16 s_2 x^{2})))))$$
$$+ s_3 (44 s_1^{3} x^{3} + s_2 (s_1 (-96 x^{3} - 5 s_1^{6} x^{2}) + s_2 (48 s_1^{5} x^{2} + s_2 (-140 s_1^{3} x^{2} + 112 s_2 s_1 x^{2}))) +$$
$$s_3 (-64 x^{3} + 12 s_1^{6} x^{2} + s_2 (-138 s_1^{4} x^{2} + s_2 (424 s_1^{2} x^{2} - 288 s_2 x^{2})) + s_3 (72 s_1^{3} x^{2}$$
$$+ s_2 (s_1 (-272 x^{2} - 2 s_1^{6} x) + s_2 (22 s_1^{5} x + s_2 (-88 s_1^{3} x + 136 s_2 s_1 x))) + s_3 (-88 x^{2} + 8 s_1^{6} x$$
$$+ s_2 (-116 s_1^{4} x + s_2 (484 s_1^{2} x - 536 s_2 x)) + s_3 (64 s_1^{3} x - 424 s_2 s_1 x$$
$$+ s_3 (-56 x + 4 s_1^{6} + s_2 (-48 s_1^{4} + s_2 (208 s_1^{2} - 352 s_2)) + s_3 (32 s_1^{3} - 192 s_2 s_1 - 16 s_3)))))))$$

$$+s_4 (s_1^2 (-64 x^3+6 s_1^6 x^2)$$
$$+s_2 (128 x^3-62 s_1^6 x^2+s_2 (216 s_1^4 x^2+s_2 (-288 s_1^2 x^2+128 s_2 x^2)))+s_3 (60 s_1^5 x^2+s_2$$
$$(s_1^3 (-272 x^2-s_1^6 x)+s_2 (s_1 (192 x^2+14 s_1^6 x)+s_2 (-68 s_1^5 x+s_2 (136 s_1^3 x-96 s_2 s_1 x))))$$
$$+s_3 (s_1^2 (32 x^2+5 s_1^6 x)+s_2 (416 x^2-84 s_1^6 x+s_2 (484 s_1^4 x+s_2 (-1072 s_1^2 x+608 s_2 x)))$$
$$+s_3 (64 s_1^5 x+s_2 (-528 s_1^3 x+1104 s_2 s_1 x)+s_3 (s_1^2 (120 x+3 s_1^6)$$
$$+s_2 (496 x-48 s_1^6+s_2 (272 s_1^4+s_2 (-672 s_1^2+656 s_2)))$$
$$+s_3 (32 s_1^5+s_2 (-320 s_1^3+832 s_2 s_1)+s_3 (32 s_1^2+192 s_2))))))+s_4 (s_1^4 (-88 x^2+3 s_1^6 x)+$$
$$s_2$$
$$(s_1^2 (416 x^2-42 s_1^6 x)+s_2 (-384 x^2+220 s_1^6 x+s_2 (-536 s_1^4 x+s_2 (608 s_1^2 x-256 s_2 x))))$$
$$+s_3 (s_1 (-384 x^2+48 s_1^6 x)+s_2 (-424 s_1^5 x+s_2 (1104 s_1^3 x-704 s_2 s_1 x))+s_3 ($$
$$s_1^4 (120 x+2 s_1^6)$$
$$+s_2 (s_1^2 (-160 x-32 s_1^6)+s_2 (-1344 x+208 s_1^6+s_2 (-672 s_1^4+s_2 (1056 s_1^2-640 s_2))))$$
$$+s_3 (s_1 (-448 x+32 s_1^6)+s_2 (-320 s_1^5+s_2 (1152 s_1^3-1536 s_2 s_1))$$
$$+s_3 (96 s_1^4+s_2 (-192 s_1^2-832 s_2)-128 s_3 s_1))))+s_4 (256 x^2+s_1^6 (-56 x+s_1^6)+s_2 ($$
$$s_1^4 (496 x-16 s_1^6)$$
$$+s_2 (s_1^2 (-1344 x+104 s_1^6)+s_2 (1024 x-352 s_1^6+s_2 (656 s_1^4+s_2 (-640 s_1^2+256 s_2)))))$$
$$+s_3 (s_1^3 (-448 x+16 s_1^6)$$
$$+s_2 (s_1 (1792 x-192 s_1^6)+s_2 (832 s_1^5+s_2 (-1536 s_1^3+1024 s_2 s_1)))+s_3$$
$$(256 x+32 s_1^6+s_2 (-192 s_1^4+s_2 (-128 s_1^2+1536 s_2))+s_3 (-256 s_1^3+1024 s_2 s_1+64 s_3)))$$
$$+s_4 (s_1^2 (256 x-16 s_1^6)+s_2 (-1024 x+192 s_1^6+s_2 (-832 s_1^4+s_2 (1536 s_1^2-1024 s_2)))$$
$$+s_3 (-128 s_1^5+s_2 (1024 s_1^3-2048 s_2 s_1)+s_3 (128 s_1^2-512 s_2))$$
$$+s_4 (64 s_1^4+s_2 (-512 s_1^2+1024 s_2))))))))$$

Question 12

```
> roots(x^2-1); roots(x^2+1);
```

[[1, 1], [-1, 1]]

[ ]

```
> resolvanteP:=proc(P,f,G)
    local n;
    n:=op(1,G);
  return(subs({seq(s[i]=(-1)^i*coeff(P,x,i),i=1..n)},resolvante
  _f(f,G)));
  end:
> resolvanteP(x^4+1,x[1]*x[2],D4);
```

$$x^3-16\, x$$

```
> test_resolvante:=proc(P,f,G)
    local R;
    R:=resolvanteP(P,f,G);
    if gcd(R,diff(R,x))<>1 then error("facteur carré")
      elif nops(roots(R))<>0 then return(true)
      else return(false);
    fi;
  end:
> testD4:=P->test_resolvante(P,x[1]*x[2],D4):
> testC4:=P->test_resolvante(P,x[1]^2*x[2],C4):
> testV4:=P->test_resolvante(P,x[1]^3*x[2]^2*x[3],V4):
> P:=x^4+x^3+x^2+x+1: testD4(P); testC4(P);
```

true

true

Donc c'est C4.

```
> P:=x^4+1: testD4(P); testV4(P);
```

true

```
Error, (in test_resolvante) facteur carré
```

On ne peut pas conclure.

```
> P:=x^4-2: testD4(P);
```

true

Donc c'est D4.

Pour le degré 5, on prend comme élément primitif l'élément qui marche à tous les coups, mais bien sur, on peut faire mieux au cas par cas (comme on l'a vu pour d=4).

On ne refait pas le test de vérification qu'il s'agit bien d'un élément primitif.

```
> resolvante2:=proc(G)
    local n,f,H,L,h,l,F,R;
    n:=op(1,G);
    f:=mul(x[i]^(n-i),i=1..n-1);
    F:=sym(G,f);
    H:=cosets(S(n),G);
    L:=[seq(action_poly(F,n,h),h=H)];
    R:=mul(x-l,l=L);
  end:
> resolvante2P:=proc(P,G)
    local n;
    n:=op(1,G);

  return(sort(subs({seq(s[i]=(-1)^i*coeff(P,x,n-i),i=1..n)},con
  vert_sym(expand(resolvante2(G)),n)),x));
  end:
> test_resolvante2:=proc(P,G)
    local R;
    R:=resolvante2P(P,G);
    if gcd(R,diff(R,x))<>1 then error("facteur carré")
```

```
    elif nops(roots(R))<>0 then return(true)
    else return(false);
  fi;
end:
> P:=x^4+x^3+x^2+x+1: test_resolvante2(P,D4);
test_resolvante2(P,C4);
```

true

```
Error, (in test_resolvante2) facteur carré
```

Remarquer que l'on ne peut plus conclure avec cette résolvante.

```
> #P:=x^5+x^4-4*x^3-3*x^2+3*x+1: t:=time():
test_resolvante2(P,D5); t-time();
```

Maple met trop de temps : il nous faut un autre moyen de calculer les résolvantes.

```
> resolvante3P:=proc(P,G,N)
  local R,rac,n,R1;
  Digits:=N; n:=degree(P);
  R:=resolvante2(G);
  rac:=[evalf(allvalues(RootOf(P)))];
  R1:=expand(subs({seq(x[i]=rac[i],i=1..n)},R));

return(sort(convert([seq(x^i*round(coeff(R1,x,i)),i=0..degree
(R1))],'+'),x));
end:
> resolvante3P(x^4+1,V4,10); resolvante3P(x^4+1,V4,100);
```

$$x^6-32x^4+256x^2$$

$$x^6-32x^4+256x^2$$

```
> resolvante2P(x^4+1,V4);
```

$$x^6-32x^4+256x^2$$

```
> test_resolvante3:=proc(P,G,N)
  local R;
  R:=resolvante3P(P,G,N);
  if gcd(R,diff(R,x))<>1 then error("facteur carré")
    elif nops(roots(R))<>0 then return(true)
    else return(false);
  fi;
end:
> P:=x^5+x^4-4*x^3-3*x^2+3*x+1: t:=time():
test_resolvante3(P,D5,100); time()-t;
```

true

0.280

```
> test_resolvante3(P,C5,100);
```

true

C'est C5

```
> P:=x^5-5*x+12: test_resolvante3(P,D5,100);
```

true

C'est D5

```
> P:=x^5+2: test_resolvante3(P,M20,100);
Error, (in test_resolvante3) facteur carré
```

On ne peut pas conclure

```
> roots(resolvante3P(P,D5,100));
```

[[40, 2]]

Question 13

La transformée de Tschirnhausen

```
> randpoly(x,degree=5);
```

$$50-85x^5-55x^4-37x^3-35x^2+97x$$

```
> tschirn:=proc(P)
  local R,y,d,Q;
  do
    d:=rand(0..degree(P)-1)(); Q:=randpoly(x,degree=d);
    R:=resultant(subs(x=y,P),x-subs(x=y,Q),y);
    if degree(gcd(R,diff(R,x)),x)=0 then return(sort(R)); fi;
  od;
end:
> resolvante2P(x^4+1,V4);
```

$$x^6-32x^4+256x^2$$

```
> test_resolvante2(x^4+1,V4);
Error, (in test_resolvante2) facteur carré
```

```
> P1:=tschirn(x^4+1);
```

$$P1:=x^4-196x^3+14406x^2-470596x+15599297$$

```
> test_resolvante2(P1,V4);
```

true

On peut maitenant conclure : c'est V4.

```
> galois(x^4+1);
```

"4T2", {"E(4)", "2[x]2"}, "+", 4, {"(1 2)(3 4)", "(1 4)(2 3)"}

```
> tschirnR:=proc(P,G,N)
  local R,P1;
  R:=resolvante3P(P,G,N);
  while not degree(gcd(R,diff(R,x)),x)=0 do
    P1:=tschirn(P); R:=resolvante3P(P1,G,100);
  od;
  return(R);
end:
> tschirnR(x^4+1,V4,100);
```

$$x^6-130442259840x^5-6753261961697406374455568x^4$$
$$-10806534972859233922402450286809395 2x^3$$
$$+17316096411800081100071176373602239257075712000x^2$$
$$-5029690428162998635351110196583116590648038008912084992 00x$$
$$+692750731773444994266911132722009490422930945452789841568727040000$$

```
> test_resolvante4:=proc(P,G,N)
  local R;
  R:=tschirnR(P,G,N);
  if gcd(R,diff(R,x))<>1 then error("facteur carré")
    elif nops(roots(R))<>0 then return(true)
    else return(false);
  fi;
end:
> test_resolvante4(x^4+1,V4,100);
```

true

```
> P:=x^5+2: test_resolvante4(P,M20,100);
```

false

```
> galois(P);
```

"5T3", {"5:4", "F(5)"}, "-", 20, {"(1 2 4 3)", "(1 2 3 4 5)"}

oups !!!

```
> test_resolvante4:=proc(P,G,N)
    local R;
    R:=tschirnR(P,G,N); print(R);
    if gcd(R,diff(R,x))<>1 then error("facteur carré")
      elif nops(roots(R))<>0 then return(true)
      else return(false);
    fi;
  end:
> test_resolvante4(P,M20,100);
```

$$x^6 - 10852584305736677380120\,x^5 + 49074410880353438426740407694308999909881000\,x^4 - 118352040295760195848520152514958892650406236352101620607488910000\,x^3 + 160553186882090577333281383201435856146489142458917356563499651176824046211481027400000\,x^2 - (1161611330784254879698344345424405541732430610930666074146040584851750160257908122517548046147389828000000000 - 2942429\,I)\,x + 35018013604690487920034326957680238947224850885207374562505392197990575169516946855993395488436348340000000000000000000000000000 - 1064556680849033681832995217\,I$$

false

On a l'explication : on n'a pas travaillé avec assez de précision : R est un polynome complexe !!!

```
> test_resolvante4(P,M20,1000);
```

$$x^6 + 1693256741806681416180\,x^5 + 11430429469129151908906240945986957248760000\,x^4 + 378152352366129281691566191098842990052162525567890845585040000\,x^3 + 54953716958803568479746192666067556770313317479785871428960064888242486275898400000\,x^2 + (64781025933810467560822268216104047210280893649883810936936390973676793278759963649903972225302082590 0 - 26300\,I)\,x - 21258781263444388193416681909182816964628668184626883390309746823351580655831433822273026504416790170000000000000000000000000 - 1390828786097271655572671\,I$$

false

```
> #test_resolvante4(P,M20,10000);
```

On atteint les limites de Maple : calculer avant autant de chiffres significatifs fait planter le noyau.

Pour s'en sortir, on travaille avec une résultante plus simple :

```
> F:=sym(M20,x[1]^2*(x[2]*x[5]+x[3]*x[4]));
```

$$F := 4\,(x_2 x_5 + x_3 x_4)\,x_1^2 + 4\,(x_1 x_3 + x_4 x_5)\,x_2^2 + 4\,(x_1 x_5 + x_2 x_4)\,x_3^2 + 4\,(x_1 x_2 + x_3 x_5)\,x_4^2 + 4\,(x_1 x_4 + x_2 x_3)\,x_5^2$$

```
> stab(F,5);
```

{[[1, 4, 3, 5]], [[1, 2], [3, 5]], [[2, 4, 5, 3]], [[1, 2, 5, 4]], [[1, 5, 2, 3]], [[1, 4, 5, 2]], [[1, 3, 5, 2, 4]], [[2, 5], [3, 4]], [ ], [[1, 3, 2, 5]], [[2, 3, 5, 4]], [[1, 5], [2, 4]], [[1, 3], [4, 5]], [[1, 4, 2, 5, 3]], [[1, 4], [2, 3]], [[1, 3, 4, 2]], [[1, 2, 4, 3]], [[1, 5, 3, 4]], [[1, 2, 3, 4, 5]], [[1, 5, 4, 3, 2]]}

```
> nops(%);
```

20

Il s'agit donc d'un élément primitif.

```
> R:=resolvante(F,M20);
```

$$R := (x - 4\,(x_2 x_4 + x_3 x_5)\,x_1^2 - 4\,(x_1 x_5 + x_3 x_4)\,x_2^2 - 4\,(x_1 x_2 + x_4 x_5)\,x_3^2 - 4\,(x_1 x_3 + x_2 x_5)\,x_4^2 - 4\,(x_1 x_4 + x_2 x_3)\,x_5^2)\,(x - 4\,(x_2 x_5 + x_3 x_4)\,x_1^2 - 4\,(x_1 x_3 + x_4 x_5)\,x_2^2 - 4\,(x_1 x_5 + x_2 x_4)\,x_3^2 - 4\,(x_1 x_2 + x_3 x_5)\,x_4^2 - 4\,(x_1 x_4 + x_2 x_3)\,x_5^2)\,(x - 4\,(x_2 x_3 + x_4 x_5)\,x_1^2 - 4\,(x_1 x_4 + x_3 x_5)\,x_2^2 - 4\,(x_1 x_5 + x_2 x_4)\,x_3^2 - 4\,(x_1 x_3 + x_2 x_5)\,x_4^2 - 4\,(x_1 x_2 + x_3 x_4)\,x_5^2)\,(x - 4\,(x_2 x_3 + x_4 x_5)\,x_1^2 - 4\,(x_1 x_5 + x_3 x_4)\,x_2^2 - 4\,(x_1 x_4 + x_2 x_5)\,x_3^2 - 4\,(x_1 x_2 + x_3 x_5)\,x_4^2 - 4\,(x_1 x_3 + x_2 x_4)\,x_5^2)\,(x - 4\,(x_2 x_4 + x_3 x_5)\,x_1^2 - 4\,(x_1 x_3 + x_4 x_5)\,x_2^2 - 4\,(x_1 x_4 + x_2 x_5)\,x_3^2 - 4\,(x_1 x_5 + x_2 x_3)\,x_4^2 - 4\,(x_1 x_2 + x_3 x_4)\,x_5^2)\,(x - 4\,(x_2 x_5 + x_3 x_4)\,x_1^2 - 4\,(x_1 x_4 + x_3 x_5)\,x_2^2 - 4\,(x_1 x_2 + x_4 x_5)\,x_3^2 - 4\,(x_1 x_5 + x_2 x_3)\,x_4^2 - 4\,(x_1 x_3 + x_2 x_4)\,x_5^2)$$

```
> resolvante5P:=proc(P,G,R,N)
    local rac,n,R1;
    Digits:=N; n:=degree(P);
    rac:=[evalf(allvalues(RootOf(P)))];
    R1:=expand(subs({seq(x[i]=rac[i],i=1..n)},R));

  return(sort(convert([seq(x^i*round(coeff(R1,x,i)),i=0..degree
  (R1))],'+'),x));
  end:
> P1:=tschirn(P);
```

$$P1 := x^5 + 455\,x^4 + 82810\,x^3 + 7535240\,x^2 + 341751035\,x + 5683260433$$

```
> resolvante5P(P1,M20,R,100);
```

$$x^6 - 16492240480\,x^5 + 113330889176709680000\,x^4 - 4153515953642563994492019200000\,x^3 + 85626110893424186098609583473465600000 0\,x^2 - 941446341155868722883260882650420582688000000000\,x + 43129474863419492498627101661194898651317098101760000000 0$$

```
> resolvante5P(P1,M20,R,1000);
```

$$x^6 - 16492240480\,x^5 + 113330889176709680000\,x^4$$

$$- 4153515953642563994492019200000\, x^3$$
$$+ 856261108934241860986095834734656000000\, x^2$$
$$- 94144634115586872288326088265042058268800000000\, x$$
$$+ 4312947486341949249862710166119489865131709810176000000000$$

```
> roots(%);
```

$$[[2755628280, 1]]$$

Si le controle numérique est bon, alors cela démontre que le groupe de Galois est bien M20.

Question 14

Utilisation des résolvantes linéaires

```
> RP2a:=proc(P) local R,Q,S;
   R:=resultant(subs(x=y,P),subs(x=x-y,P),y);
   Q:=2^(degree(P,x))*subs(x=x/2,P);
   S:=factors(quo(R,Q,x));
   S:=mul(op([2,i,1],S)^(op([2,i,2],S)/2),i=1..nops(op(2,S)));
   return(sort(S,x));
  end:
> test2a:=proc(P) local R,L;
    R:=RP2a(P);
    if gcd(R,diff(R,x))<>1 then
      error("facteur carré");
    else
      L:=factors(R);

  return(sort([seq(degree(op([2,i,1],L),x),i=1..nops(op(2,L)))]
  ));
    fi;
  end:
> RP2b:=proc(P)  local R,Q,S;

  R:=resultant(subs(x=y,P),2^(degree(P,x))*subs(x=(x-y)/2,P),y)
  ;
    Q:=3^(degree(P,x))*subs(x=x/3,P);
    S:=quo(R,Q,x);
    return(sort(S,x));
  end:
> test2b:=proc(P) local R,L;
    R:=RP2b(P);
    if gcd(R,diff(R,x))<>1 then
      error("facteur carré");
    else
      L:=factors(R);

  return(sort([seq(degree(op([2,i,1],L),x),i=1..nops(op(2,L)))]
  ));
    fi;
  end:
```

De l'autre coté, on établit, pour les dégrés 4 et 5, la liste des cardinaux des orbites pour l'action des groupes de permutations transitifs sur les parties à 2 éléments et les listes ordonnées à 2 éléments.

On reprend des procédures du TP4B (orbite, Orbite2G)

```
> orbite_i:=proc(G,i,action) local S, O, N;
    S:=op(2,G); O:={i};
    N:={seq(action(g,i),g=S)} minus O;
    while nops(N)>0 do O:=O union N;
  N:={seq(seq(action(g,a),g=S),a=N)} minus O; od;
    return(O);
  end:
> orbite:=proc(G,X,action) local L,GG,X1,S,a,g;
   L:={};
   X1:=X;
    while nops(X1)>0 do
     a:=op(1,X1);
     S:=orbite_i(G,a,action);
     L:=[op(L),nops(S)];
     X1:=X1 minus S;
    od;
  return(sort(L));
  end:
> X2b:=n->{seq(seq([i,j],i=1..j-1),j=1..n)}:
> X2a:=n->map(x->convert(x,set),X2b(n)):
> X2a(3);
```

$$\{\{2, 3\}, \{1, 3\}, \{1, 2\}\}$$

```
> X2b(3);
```

$$\{[1, 2], [2, 3], [1, 3]\}$$

```
> orbite2a:=G->orbite(G,X2a(op(1,G)),(g,x)->{image(g,op(1,G),x[
  1]),image(g,op(1,G),x[2])}):
> orbite2b:=G->orbite(G,X2b(op(1,G)),(g,x)->[image(g,op(1,G),x[
  1]),image(g,op(1,G),x[2])]):
> listeG:=[C4,S4,D4,V4,A4,C5,S5,D5,A5,M20]:
> liste2a:=[]: for G in listeG do
  liste2a:=[op(liste2a),orbite2a(G)]; od:
> liste2b:=[]: for G in listeG do
  liste2b:=[op(liste2b),orbite2b(G)]; od:
> for i from 1 to 10 do print(liste2a[i],liste2b[i]); od;
```

$$[2, 4], [4, 4, 4]$$
$$[6], [12]$$
$$[2, 4], [4, 8]$$
$$[2, 2, 2], [4, 4, 4]$$
$$[6], [12]$$
$$[5, 5], [5, 5, 5, 5]$$
$$[10], [20]$$
$$[5, 5], [10, 10]$$
$$[10], [20]$$
$$[10], [20]$$

On ne peut pas différencier S4 et A4, mais ce n'est pas grave car on a déjà appliqué le critère du discriminant

On se sait pas par contre distinguer S5 et M20.

```
> P:=x^4+x^3+x^2+x+1: test2a(P); test2b(P);
```

[2, 4]

[4, 4, 4]

Donc c'est C4. Maple conclut.

```
> P:=x^4+1: test2a(P); test2b(P);
Error, (in test2a) facteur carré
```

[4, 4, 4]

Maple arrive à calculer test2a(P) et conclut. C'est à nouveau une transformée de Tschirnhausen qui a été appliquée :

```
> P1:=tschirn(P): test2a(P1); test2b(P1);
```

[2, 2, 2]

[4, 4, 4]

(répéter la ligne précédente si un message d'erreur "facteur carré" apparait)

```
> P:=x^4-2: test2a(P); test2b(P);
Error, (in test2a) facteur carré
```

[4, 8]

Donc c'est D4. Noter que Maple conclut à partir de test2a(P)

```
> P1:=tschirn(P): test2a(P1); test2b(P1);
Error, (in test2a) facteur carré
```

[4, 8]

```
> P:=x^5+x^4-4*x^3-3*x^2+3*x+1: test2a(P); test2b(P);
```

[5, 5]

[5, 5, 5, 5]

C'est C5

```
> P:=x^5-5*x+12: test2a(P); test2b(P);
```

[5, 5]

[10, 10]

C'est D5

```
> P:=x^5+2: test2a(P); test2b(P);
```

[10]

[20]

On ne peut pas conclure. Noter que Maple n'applique pas ces tests dans ce cas.