Αλγεβρικές Δομές ΙΙ (2017-2018)
Φροντιστηριακές ασκήσεις #1

1. Έστω R μεταθετικός δακτύλιος με μονάδα και I γνήσιο ιδεώδες του R. Δείξτε (ή βρείτε σε κάποιο βιβλίο την απόδειξη) ότι υπάρχει maximal ιδεώδες P του R με $I \subseteq P$.

2. Έστω $R \neq 0$ μεταθετικός δακτύλιος με μονάδα και $a \in R$. Δείξτε ότι το a είναι αντιστρέψιμο αν και μόνο εάν δεν ανήκει σε κανένα maximal ιδεώδες του R.

3. Έστω D Ακέραια Περιοχή. Υποθέτουμε ότι το σύνολο των ιδεωδών της D είναι πεπερασμένο. Δείξτε ότι το D είναι σώμα. Επίσης δειξτε ότι για $m \geq 4$ σύνθετο ακέραιο ο δακτύλιος $\mathbb{Z}_m$ των ακεραίων modulo m έχει πεπερασμένο πλήθος ιδεωδών αλλά δεν είναι σώμα.

4. Έστω D Περιοχή Κυρίων Ιδεωδών και $0 \neq I$ πρώτο ιδεώδες του D. Δείξτε ότι το ιδεώδες I είναι maximal.

5. Έστω D Περιοχή Κυρίων Ιδεωδών και $(I_n)_{n\geq 1}$ ακολουθία ιδεωδών της D με την ιδιότητα ότι
$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$$
Δείξτε ότι το $I = \cup_{n\geq 1} I_n$ είναι ιδεώδες του D και ότι υπάρχει θετικός ακέραιος n_0 με την ιδιότητα $I_n = I_{n_0}$ για κάθε $n \geq n_0$.

6. Θεωρούμε τον δακτύλιο $D = \mathbb{Z}[x]$ των πολυωνύμων σε μια μεταβλητή με ακέραιους συντελεστές και τα υποσύνολα του
$$I = \{a_0 + a_1 x + \cdots + a_n x^n : \ n \geq 0, \ a_i \in \mathbb{Z}, \ a_0 = 0\}$$
και
$$J = \{a_0 + a_1 x + \cdots + a_n x^n : \ n \geq 0, \ a_i \in \mathbb{Z}, \ 2 \mid a_0\}.$$
   (α΄) Δείξτε ότι τα I και J είναι ιδεώδη του D.
   (β΄) Δείξτε ότι ο δακτύλιος πηλίκο D/I είναι ισόμορφος με τον δακτύλιο $\mathbb{Z}$ των ακεραίων. Επομένως το I είναι πρώτο αλλά όχι maximal ιδεώδες του D.
   (γ΄) Δείξτε ότι το J δεν είναι κύριο ιδεώδες του D. Επίσης δείξτε ότι ο δακτύλιος πηλίκο D/J είναι ισόμορφος με τον δακτύλιο $\mathbb{Z}_2$ των ακεραίων modulo 2, άρα είναι σώμα. Συνεπώς το J είναι maximal ιδεώδες του D.

7. Έστω $R \neq 0$ μεταθετικός δακτύλιος με μονάδα. Δείξτε ότι ο πολυωνυμικός δακτύλιος $R[x]$ είναι Περιοχή Κυρίων Ιδεωδών εάν και μόνο εάν ο R είναι σώμα.

-- Macaulay2 computer algebra online system
-- http://habanero.math.cornell.edu:3690/

– Polynomials taken from [Brzezinski, Galois Theory Through Exercises]

R = QQ [x]

factor (x^4 +4) -- answer: factor (x^4 +4)

factor (x^4 +64) -- answer: (x^2-4*x+8)*(x^2+4*x+8)

factor (x^3 -2) -- answer: (x^3 -2)

factor (x^4 +1) -- answer: (x^4 +1)

factor (x^6 + 27)
-- answer: (x^2+3)*(x^2-3*x+3)*(x^2+3*x+3)

isPrime ideal (x^2+1) -- answer true , hence x^2+1 is ireducible in QQ[x]

isPrime ideal (x^3+1) -- answer false, hence x^3+1 is not irreducible in Q[x]
factor (x^3 +1) -- answer: (x+1)*(x^2-x+1)

R = ZZ/2 [x]
factor (x^7 + 1) -- answer: (x+1)*(x^3+x+1)*(x^3+x^2+1)

R = ZZ/3 [x]

factor (x^3 + 2) -- answer: (x-1)^3

factor (x^4 + x+ 2) -- answer: (x^4 + x -1)

R = ZZ/5 [x]

factor (x^4 + 2) -- answer: (x^4+2)

```
--- Find all irreducible polynomails in ZZ/2 [x] up to degree 5

R = ZZ/2[x]

list1 = {x,x+1}

-- degree 2: -- polynomials of the form x^2 + a1*x + a0
list2 = {}
for a1 from 0 to 1 do
  for a0 from 0 to 1 do
      if isPrime ideal (1_R*x^2 + a1*x + a0) then
list2 = list2 | {1_R*x^2 + a1*x + a0}
list2 -- answer: {x^2+x+1}

-- degree 3: -- polynomials of the form x^3 + a2*x^2 + a1*x + a0
list3 = {}
for a2 from 0 to 1 do
  for a1 from 0 to 1 do
    for a0 from 0 to 1 do
      if isPrime ideal (1_R*x^3 + a2*x^2 + a1*x + a0) then (
           list3 = list3 | {1_R*x^3 + a2*x^2 + a1*x + a0} )
list3 -- answer: {x^3+x+1, x^3+x^2+1}



-- degree 4: -- polynomials of the form x^4 + a3*x^3 + a2*x^2 + a1*x + a0
list4 = {}
for a3 from 0 to 1 do
 for a2 from 0 to 1 do
   for a1 from 0 to 1 do
      for a0 from 0 to 1 do
         if isPrime ideal (1_R*x^4 +a3*x^3+ a2*x^2 + a1*x + a0) then (
              list4 = list4 | {1_R*x^4 + a3*x^3 +a2*x^2 + a1*x + a0} )
list4 -- answer: {x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1}

-- degree 5: -- polynomials of the form x^5 +a4*x^4+ a3*x^3+a2*x^2+a1*x + a0
list5 = {}
for a4 from 0 to 1 do
 for a3 from 0 to 1 do
  for a2 from 0 to 1 do
    for a1 from 0 to 1 do
      for a0 from 0 to 1 do
       if isPrime ideal (1_R*x^5+ a4*x^4 +a3*x^3+ a2*x^2 + a1*x + a0) then (
            list5 = list5 | {1_R*x^5 + a4*x^4+ a3*x^3 +a2*x^2 + a1*x + a0} )
list5    -- answer: {x^5+x^2+1, x^5+x^3+1,
        --             x^5+x^3+x^2+x+1, x^5+x^4+x^2+x+1, x^5+x^4+x^3+x+1,
        --             x^5+x^4+x^3+x^2+1}
```

Αλγεβρικές Δομές II (2017-2018)

Φροντιστηριακές ασκήσεις #2

1. Δείξτε ότι αν $\mathbb{F}$ σώμα, τότε το σύνολο των αναγώγων στοιχείων του πολυωνυμικού δακτυλίου $\mathbb{F}[x]$ είναι άπειρο. Σαν συμπέρασμα, αν $\mathbb{F}$ πεπερασμένο σώμα, το σύνολο $A \subseteq \mathbb{Z}$ που έχει στοιχεία τους βαθμούς αναγώγων πολυωνύμων του $\mathbb{F}[x]$ είναι άπειρο. (Μπορεί να αποδειχθεί ότι το A είναι ίσο με το σύνολο των θετικών ακεραίων.)

2. Έστω $\mathbb{K}$ υπόσωμα του $\mathbb{F}$ και $g \in \mathbb{F}[x]$. Υποθέτουμε ότι υπάρχει μη μηδενικό $h \in \mathbb{K}[x]$ με $g \cdot h \in \mathbb{K}[x]$. Δείξτε ότι $g \in \mathbb{K}[x]$. Δείξτε με ένα παράδειγμα ότι το συμπέρασμα δεν ισχύει πάντα αν υποθέσουμε $\mathbb{K}, \mathbb{F}$ μόνο Ακέραιες Περιοχές.

3. Υποθέτουμε ότι τα $f \in \mathbb{Z}[x]$ και $g \in \mathbb{Q}[x]$ είναι μονικά πολυώνυμα. Αν το g διαιρεί το f στο $\mathbb{Q}[x]$ δείξτε ότι $g \in \mathbb{Z}[x]$.

4. Έστω R μεταθετικός δακτύλιος με μονάδα, $a, b \in R$ και $n \geq 1$ ακέραιος. Δείξτε ότι
$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

5. Έστω D Ακέραια Περιοχή χαρακτηριστικής p, όπου p πρώτος, και $n \geq 1$ ακέραιος. Θέτουμε $q = p^n$. Δείξτε ότι
$$(a+b)^q = a^q + b^q$$
για κάθε $a, b \in D$.

6. Έστω p πρώτος, και
$$f = x^{p-1} + x^{p-2} + \cdots + x + 1 \ \in \mathbb{Q}[x]$$
το p-τάξεως κυκλοτομικό πολυώνυμο. Χρησιμοποιώντας τον ισομορφισμό δακτυλίων
$$T_{x+1} : \mathbb{Q}[x] \to \mathbb{Q}[x], \qquad \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} a_i (x+1)^i$$
που διατηρεί βαθμούς, δείξτε με το κριτήριο Eisenstein ότι το $T_{x+1}(f)$ είναι ανάγωγο στο $\mathbb{Q}[x]$. Σαν συμπέρασμα έχουμε ότι το f είναι ανάγωγο στο $\mathbb{Q}[x]$.

7. Έστω $n \geq 3$ ακέραιος. Δείξτε ότι το πολυώνυμο
$$f = x^n + 11x^3 - 33x + 22$$
είναι ανάγωγο στο $\mathbb{Q}[x]$.

8. Έστω
$$f = x^4 - 6x^3 + kx^2 + 3x + 4$$
με $k \in \mathbb{Z}$. Για ποιες τιμές του k είναι το f ανάγωγο στο $\mathbb{Q}[x]$;

Pari/GP: Computer Algebra program for Number Theory

Homepage: https://pari.math.u-bordeaux.fr/

Online platform: http://pari.math.u-bordeaux.fr/gp.html

Online Documentation: https://pari.math.u-bordeaux.fr/dochtml/html-stable/

\\ INDEX

\\ Task 4: keycode: 12145 Find minimal polynomial with Macaulay2 and Pari/GP

\\ Task 3: keycode: 98211 Factoring with Pari/GP over a field extension

\\ Task 2: keycode: 2536 Factoring with Pari/GP over the finite field ZZ/(p)

\\ Task 1: keycode: 8372 Factoring with Pari/GP over the rational numbers

\\ Task 4: keycode: 12145 Find minimal polynomial with Macaulay2 and Pari/GP

-- Example 1, 15apr18, keycode: 156641

```
-- M2 code related to the discussion at
--
-- https://math.stackexchange.com/questions/
-- 1779204/prove-or-disprove-that-sqrt32-sqrt1-sqrt2-is-aroot-of-a-polynomial
--
```

```
-- PROBLEM: Find a nonzero polynomial with integer coefficients that vanishes on
--
-- u = A + B
--
-- where
--
-- A = 3rd root of 2
--
-- B = square Root of ( 1+ C )
--
-- and C = square root of 2



-- Macaulay2 code:

clearAll

R = QQ [A,B,C,u]

I = ideal ( A^3-2, C^2-2 , B^2 - (1+C), u - (A+ B) )

eliminate (I, { A,B,C} )
-- answer: ideal(u^12-6*u^10-8*u^9+9*u^8+28*u^6-144*u^5+
-- 63*u^4+96*u^3-78*u^2-168*u-41)




\\ Pari/gp computation for the minimal polynomial of algebraic integer:

a=sqrtn(1+sqrt(7),3)
algdep(a,6)
\\ answer: x^6 - 2*x^3 - 6 [M2, p. 42]
```

```
\\ Task 3: keycode: 98211 Factoring with Pari/GP over a field extension


\\ Example 1 : Aim: Define t to be a root of pol1 defined below. Find the
\\ decomposition of pol1 over the field QQ(t)

pol1 = X^4-4*X^3-20*X^2-8*X+4

polisirreducible(pol1) \\answer 1, hence true, so pol1 is irreducible in QQ[t]

print ( lift( factornf(pol1, t^4-4*t^3-20*t^2-8*t+4) ) )
\\answer [X - t, 1; X + (1/2*t^3 - 2*t^2 - 10*t - 4), 1;
\\ X^2 + (-1/2*t^3 + 2*t^2 + 11*t)*X + 2, 1]



\\ Example 2:
\\
\\ Aim: Factor x^4 +1 over QQ[t]/(t^2+1)
pol1 = X^4 +1
polisirreducible(x^4+1) \\answer 1, hence true, so pol1 is irreducible in QQ[t]

print ( lift( factornf( X^4+1 , t^2+1) ) )
\\ answer: [X^2 - t, 1; X^2 + t, 1]




\\ Task 2: keycode: 2536 Factoring with Pari/GP over the finite field ZZ/(p)

g = Mod ( x^7+1, 2)

polisirreducible (g) \\ answer 0, so g is not irreducible in ZZ/2

fa = factor (g)

print (fa)

\\ answer:
\\ [ Mod(1, 2)*x + Mod(1, 2), 1;
\\ Mod(1, 2)*x^3 + Mod(1, 2)*x + Mod(1, 2), 1;
\\ Mod(1,2)*x^3 + Mod(1, 2)*x^2 + Mod(1, 2), 1 ]
```

```
\\ Task 1: keycode: 8372 Factoring with Pari/GP over the rational numbers

\\ Example 1, Polynomial is x^4 + 4 \in QQ[x] keycode: 2831124

polisirreducible(x^4+4)
\\ answer 0, it means false, so x^4+4 is not irreducible in QQ[x]

fa = factor (x^4+ 4) \\ fa has the structure of a 2 \times 2 matrix
print (fa)
\\ answer: [x^2 - 2*x + 2, 1; x^2 + 2*x + 2, 1]
\\ It means fa = (x^2-2*x+2) * (x^2+2*x+2) is the decomposition
\\ of x^4+4 in QQ[x] as product of irreducible polynomials.



\\ Example 2, Polynomial is x^2 - 3 \in QQ[x] keycode: 155252

polisirreducible(x^2-3)
\\ answer 1, it means true, so x^2-3 is irreducible in QQ[x]
```

Αλγεβρικές Δομές ΙΙ (2017-2018)

Φροντιστηριακές ασκήσεις #3

1. Έστω $v \in \mathbb{C}$ με ελάχιστο πολυώνυμο $x^2 + x + 1$ επί του $\mathbb{Q}$. Δείξτε ότι $v^2 - 1 \neq 0$, και εκφράστε το στοιχείο $(v^2+1)/(v^2-1)$ του $\mathbb{Q}(v)$ στην μορφή $a_0 + a_1 v$ με συντελεστές $a_0, a_1 \in \mathbb{Q}$.

2. Δείξτε ότι το πολυώνυμο $p = x^3 + x + 1$ είναι ανάγωγο επί του $\mathbb{Q}$. Έστω $v \in \mathbb{C}$ μια ρίζα του p. Εκφράστε τα στοιχεία $1/v$ και $1/(v+2)$ του $\mathbb{Q}(v)$ στην μορφή $a_0 + a_1 v + a_2 v^2$ με συντελεστές $a_0, a_1, a_2 \in \mathbb{Q}$.

3. (1) Δείξτε ότι $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ και ότι $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.

   (2) Έστω $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Δείξτε ότι $\mathbb{K} = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

   (3) Δείξτε ότι το σύνολο
   $$1,\ \sqrt{2},\ \sqrt{3},\ \sqrt{6}$$
   είναι μια βάση του $\mathbb{K}$ σαν διανυσματικός χώρος επί του $\mathbb{Q}$. Συνεπώς $[\mathbb{K} : \mathbb{Q}] = 4$.

   (4) Γράψτε τον αντίστροφο ως προς τον πολλαπλασιασμό του στοιχείου
   $$1 + \sqrt{2} + \sqrt{3} + \sqrt{6}$$
   του $\mathbb{K}$ ως προς την παραπάνω βάση.

   (5) Βρείτε το ελάχιστο πολυώνυμο του $\sqrt{2} + \sqrt{3}$ επί των $\mathbb{Q}$ και $\mathbb{Q}[\sqrt{3}]$.

4. Βρείτε το ελάχιστο πολυώνυμο επί του $\mathbb{Q}$ για καθένα από τα στοιχεία
   $$1 + \sqrt{3}, \qquad \frac{\sqrt{3}}{\sqrt{5}}, \qquad \sqrt{3} + \sqrt{5}, \qquad (1+i)\sqrt{3}, \qquad \sqrt{1 + \sqrt{2}}.$$

5. Δείξτε ότι το πολυώνυμο $p = x^2 + x + 1$ είναι ανάγωγο επί του $\mathbb{Z}_2$. Θέτουμε $\mathbb{K} = \mathbb{Z}_2[x]/(p)$. Δείξτε ότι το σώμα $\mathbb{K}$ έχει 4 στοιχεία, τα εξής:
   $$0 + (p), \qquad 1 + (p), \qquad x + (p), \qquad 1 + x + (p).$$
   Γράψτε τους πίνακες πρόσθεσης και πολλαπλασιασμού στο $\mathbb{K}$.

6. Δείξτε ότι το πολυώνυμο $p = x^3 + x + 1$ είναι ανάγωγο επί του $\mathbb{Z}_2$. Θέτουμε $\mathbb{K} = \mathbb{Z}_2[x]/(p)$. Γράψτε τα 8 στοιχεία του σώματος $\mathbb{K}$ και τους πίνακες πρόσθεσης και πολλαπλασιασμού στο $\mathbb{K}$. Έστω $v = x + (p) \in \mathbb{K}$. Υπολογίστε τις δυνάμεις v^m, για $m \in \mathbb{Z}$. Σαν πόρισμα, έχουμε ότι η ομάδα $\mathbb{K} \setminus \{0\}$ είναι κυκλική ομάδα τάξης 7 με γεννήτορα το v.

7. Δείξτε ότι το πολυώνυμο $p = x^4 - 2$ είναι ανάγωγο επί του $\mathbb{Q}$. Υπολογίστε (σαν υπόσωμα του $\mathbb{C}$) το σώμα ριζών $\mathbb{K}$ του p επί του $\mathbb{Q}$ και βρείτε τον βαθμό $[\mathbb{K} : \mathbb{Q}]$.

```
\\    Pari/GP   code for computing Galois groups of field extensions

\\ INDEX

\\ Task 5: keycode: 53134  Computing Galois groups etc. with Pari/GP



\\ 01apr18, 3 Important examples of computation of Galois groups with Pari/GP

nf=nfinit(a^4+1)
polgalois (x^4+1)
\\ answer: [4, 1, 1, "E(4) = 2[x]2"] , this means Z_2 \oplus Z_2
print ( lift(nffactor(nf,x^4+1)) )
\\ answer [x - a, 1; x + a, 1; x - a^3, 1; x + a^3, 1]




nf=nfinit(a^4+2) ;
polgalois (x^4+2)
\\answer: [8, -1, 1, "D(4)"] , this means the Dihedral group of order 8
print (lift(nffactor(nf,x^4+2)))
\\ answer : [x - a, 1; x + a, 1; x^2 + a^2, 1]


nf=nfinit(a^4+2*a+3)
polgalois (x^4+2*x+3)
\\answer: [24, -1, 1, "S4"]
print ( lift(nffactor(nf,x^4+2*x+3)) )
\\answer: [x - a, 1; x^3 + a*x^2 + a^2*x + (a^3 + 2), 1]




for(i = 5, 9, print (polgalois (x^4+2*x+i) ))
\\ answer: [24, -1, 1, "S4"]
\\ [24, -1, 1, "S4"]
\\ [24, -1, 1, "S4"]
\\ [24, -1, 1, "S4"]
\\ [24, -1, 1, "S4"]
```

```
for(i = 5, 30, print
 (i, polgalois (x^4+i) ))
\\ answer: interesting pattern depending on whether i is a sqaure or not

\\ 5[8, -1, 1, "D(4)"]
\\ 6[8, -1, 1, "D(4)"]
\\ 7[8, -1, 1, "D(4)"]
\\ 8[8, -1, 1, "D(4)"]
\\ 9[4, 1, 1, "E(4) = 2[x]2"]
\\ 10[8, -1, 1, "D(4)"]
\\ 11[8, -1, 1, "D(4)"]
\\ 12[8, -1, 1, "D(4)"]
\\ 13[8, -1, 1, "D(4)"]
\\ 14[8, -1, 1, "D(4)"]
\\ 15[8, -1, 1, "D(4)"]
\\ 16[4, 1, 1, "E(4) = 2[x]2"]
\\ 17[8, -1, 1, "D(4)"]
```

```
\\ Example 2, 11apr18, keycode: 2989131
\\
\\ Example of working with Galois groups with K the
\\ splitting field of x^4 + 2 \in QQ[t]

P = x^4 + 2;
print ( lift(factornf ( x^4 + 2, a^4+2 )) ) \\ keycode: 282784
\\ answer: [x - a, 1; x + a, 1; x^2 + a^2, 1]

polisirreducible(P)
\\ answer 1, hence P is irreducible in QQ[t]

G = galoisinit(P)
\\ answer 0 , problem due perhaps (??) to the fact that P does not factor
\\ completely in QQ[a]/( a^4+2)

K = nfsplitting (P)
\\ answer x^8 - 28*x^4 + 2500
\\ Hence the splitting field of K is isomorphic to QQ[x]/ ( x^8 - 28*x^4 + 2500 )

polgalois ( K)
\\ answer: [8, 1, 4, "D_8(8)=[4]2"]
\\
\\ The Dihedral group of order 8
```

```
G = galoisinit(K);
\\
\\ G is the Dihedral group of order 8



galoisexport(G)
\\ answer: "Group((1, 5, 8, 4)(2, 3, 7, 6), (1, 2)(3, 4)(5, 6)(7, 8))"
\\
\\ Two elements of S_8 that generate G as a subgroup of S_8.



Galoisexport(G,1)
\\ answer: "PermutationGroup<8|[5, 3, 7, 1, 8, 2, 6, 4], [2, 1, 4, 3, 6, 5, 8, 7]>"
\\
\\ The order of the group G and two elements of S_8 that generate G as a group.

galoisidentify(G) \\ answer: [8, 3] Related GAP: First coordinate 8 is the order of the group,
\\ 3 is the identifier of the group among all groups of order 8

\\ Compare: https://groupprops.subwiki.org/wiki/Groups_of_order_8 and
\\ maths/papadakis_partial_screenshot_groups_of_order_8.png



G.group

u = galoissubgroups(G)

matsize (u)
\\ answer [1, 10] This means G has 10 subgroups



vector(#u, i, galoisisabelian(u[i],1))
\\ answer: [0, 1, 1, 1, 1, 1, 1, 1, 1, 1]
\\
\\



vector(#u, i, galoisidentify(u[i]))
\\ answer: [ [8, 3], [4, 1], [4, 2], [4, 2], [2, 1], [2, 1], [2, 1],
\\ [2, 1], [2, 1], [1, 1]]
\\
\\ [4,1] corresponds to the cyclic order 4 subgroup of G, while
\\ the two [4,2] correspond to the two subgroups of G
\\ which are isomorphic to Z_2 \oplus \Z_2
```

```
\\

\\ Example 1, 11apr18, keycode: 113421
\\
\\ Example of working with Galois groups with K the
\\ splitting field of x^6 + 108 \in QQ[t]

P = x^6 + 108;
polisirreducible(P)
\\ answer 1, hence P is irreducible in QQ[t]
\\ Notice: 108 = 2^2 * 3^3 , using factor (108)

K = nfsplitting (P)
\\ K is the splitting field of P
\\ answer: x^6 + 108
\\ Hence P splits completely over QQ[a]/(a^6+108)
\\ and K = QQ[a]/(a^6+108)

print ( lift(factornf ( x^6 + 108, a^6+108 )) ) \\ keycode: 282784
\\ answer: [ x - a, 1; x + a, 1;
\\ x + (-1/12*a^4 - 1/2*a), 1; x + (-1/12*a^4 + 1/2*a), 1;
\\ x + (1/12*a^4 - 1/2*a), 1; x + (1/12*a^4 + 1/2*a), 1 ]
\\
\\ This means, that X^6+ 108 has 6 roots in QQ[a]/(a^6+108)
\\ and the roors are
\\
\\ a, -a , root_{e1,e2} = (-1/12* e_1 * a^4 - 1/2*e_2 *a)
\\
\\ for all possible e_1, e_2 \in {1, -1}

G = galoisinit(K);

polgalois ( G.pol)
[6, -1, 2, "D_6(6) = [3]2"] -- it is a group isomorphic to S_3 considered as
-- subgroup of S_6

galoisexport(G)
\\ answer: "Group((1, 2, 3)(4, 5, 6), (1, 4)(2, 6)(3, 5))"
\\
\\ Two elements of S_6 that generate G as a subgroup of S_6.

galoisexport(G,1)
\\ answer: "PermutationGroup<6|[2, 3, 1, 5, 6, 4], [4, 6, 5, 1, 3, 2]>"
\\
\\ The order of the group G and two elements of S_6 that generate G as a group.
```

```
galoisidentify(G) \\ answer: [6, 1] Related GAP: First coordinate 6 is the order of the group,
\\ 6 is the identifier of the group among all groups of order 1

\\ Compare: https://groupprops.subwiki.org/wiki/Groups_of_order_6 and
\\ maths/papadakis_partial_screenshot_groups_of_order_6.png
```

```
G.group
\\ answer: [Vecsmall([1, 2, 3, 4, 5, 6]), Vecsmall([2, 3, 1, 5, 6, 4]),
\\ Vecsmall([3,1, 2, 6, 4, 5]), Vecsmall([4, 6, 5, 1, 3, 2]),
\\ Vecsmall([5, 4, 6, 2, 1, 3]), Vecsmall([6, 5, 4, 3, 2, 1])]
\\
\\ Very likely, it means that G is the subgroup of S_4 with 6 elements,
\\ namely s_1 = identity = i \mapsto i for all 1 \leq i \leq 6
\\ s_2 : 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1,
\\ 4 \mapsto 5, 5 \mapsto 6 , 6 \mapsto 4
\\ that is s_2 = (1,2,3) (4,5,6)
\\
\\ s_3 : 1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2,
\\ 4 \mapsto 6, 5 \mapsto 4 , 6 \mapsto 5
\\ that is s_3 = (1,3,2) (4,6,5) = s_2 \circ s_2
\\
\\ s_4 : 1 \mapsto 4, 2 \mapsto 6, 3 \mapsto 5,
\\ 4 \mapsto 1, 5 \mapsto 3 , 6 \mapsto 2
\\ that is s_4 = (1,4) (2,6)(3,5)
\\
\\ s_5 : 1 \mapsto 5, 2 \mapsto 4, 3 \mapsto 6,
\\ 4 \mapsto 2, 5 \mapsto 1 , 6 \mapsto 3
\\ that is s_5 = (1,5) (2,4) (3,6)
\\
\\ s_6 : 1 \mapsto 6, 2 \mapsto 5, 3 \mapsto 4,
\\ 4 \mapsto 3, 5 \mapsto 2, 6 \mapsto 1
\\ that is s_6 = (1,6) (2,5) (3,4)
```

```
G.gen \\answer: [Vecsmall([2, 3, 1, 5, 6, 4]), Vecsmall([4, 6, 5, 1, 3, 2])]
\\
\\ Hence G is generated (as a group) by the set { s_2, s_4 }
```

```
G.orders \\ answer: Vecsmall([3, 2]) , this means
\\ order (s_2) = 3 , order (s_4) = 2
```

```
\\ (where order means order of an element of a group )

galoisisabelian (G) \\answer 0, which means false. Expected since S_3 is not abelian

u = galoissubgroups(G)

matsize(u) \\ answer [1, 6]

u[1]
\\ answer: [[Vecsmall([2, 3, 1, 5, 6, 4]), Vecsmall([4, 6, 5, 1, 3, 2])], Vecsmall([, 2])]
\\ Hence we get S_3 as subgroup of S_3

u[2]
\\ answer: [[Vecsmall([2, 3, 1, 5, 6, 4])], Vecsmall([3])]
\\ Hence we get the cyclic group of order 3 generated by s_2

u[3]
\\ answer: [[Vecsmall([4, 6, 5, 1, 3, 2])], Vecsmall([2])]
\\ Hence we get the cyclic group of order 2 generated by s_4

u[4]
\\ answer: [[Vecsmall([6, 5, 4, 3, 2, 1])], Vecsmall([2])]
\\ Hence we get the cyclic group of order 2 generated by s_6

u[5]
\\ answer: [[Vecsmall([5, 4, 6, 2, 1, 3])], Vecsmall([2])]
\\ Hence we get the cyclic group of order 2 generated by s_6

u[6]
\\ answer: [[], Vecsmall([])]
\\ Hence we get the trivial subgroup of S_3

F1= galoisfixedfield( G, u[1] , 2)
\\ answer: [x, Mod(0, x^6 + 108), [x^6 + 108]]
\\
\\ u[1] is the whole Galois group S_3, hence F1 =QQ
\\ so the meaning is that F_1 = QQ [x] / (x) = QQ \subset K
\\
\\ The last component is how x^6 + 108 splits over F1
```

```
F2 = galoisfixedfield( G, u[2] , 2 )
\\ answer: [x^2 + 972, Mod(3*x^3, x^6 + 108), [x^3 - 1/3*y, x^3 + 1/3*y]]
\\
\\ Apparently, we have F_2 \iso QQ [x] / (x^2+971)
\\
\\ The last component is how x^6 + 108 splits over F2, where
\\ by the second component F2 = Q ( 3*x^3) \subset K
\\
\\ where K computed above is the splitting field of P


galoisfixedfield( G, u[3] , 2 )
\\ answer: [x^3 + 54, Mod(1/12*x^4 + 3/2*x, x^6 + 108),
\\ [x^2 - y*x + 1/3*y^2, x^2 + 1/3*y^2, x^2 + y*x + 1/3*y^2]]


galoisfixedfield( G, u[4] ,2 )
\\ answer: [x^3 + 864, Mod(2*x^2, x^6 + 108),
\\ [x^2 - 1/2*y, x^2 - 1/24*y^2*x - 1/2*y, x^2 + 1/24*y^2*x - 1/2*y]]


galoisfixedfield( G, u[5] ,2 )
\\ answer: [x^3 - 54, Mod(-1/12*x^4 + 3/2*x, x^6 + 108),
\\ [x^2 - y*x + 1/3*y^2, x^2 + y*x + 1/3*y^2, x^2 + 1/3*y^2]]


galoisfixedfield( G, u[6] , 2 )
\\ answer: [x^6 + 108, Mod(x, x^6 + 108),
\\ [x - y, x + (-1/12*y^4 + 1/2*y),
\\ x + (1/12*y^4 + 1/2*y), x + (-1/12*y^4 - 1/2*y),
\\ x + (1/12*y^4 - 1/2*y), x + y]]
\\
\\ Hence the subgroup is trivial.


vector(#u, i, galoisisabelian(u[i],1))
\\answer: [0, 1, 1, 1, 1, 1]
\\ Meaning: The first subgroup is not abelian, all the other are


vector(#u, i, galoisidentify(u[i]))
\\ answer: [[6, 1], [3, 1], [2, 1], [2, 1], [2, 1], [1, 1]]
\\
\\ REMARK: galoisidentify (u[i]) returns a pair [a,b] where a is the order of
\\ the group u[i] and b is the group index in the GAP4 Small Group
\\ library, by Hans Ulrich Besche, Bettina Eick and Eamonn O'Brien.
```