MATH 324 - Algebra II Final Project
Calculating Galois Groups of Polynomials of Degree 7

Bilge Köksal

1 Introduction

The Galois group of a separable polynomial $f(x) \in \mathbf{F}[x]$ is defined to be the Galois group of the splitting field of $f(x)$ over $\mathbf{F}$. In our case we will take $\mathbf{F} = \mathbb{Q}$ and all the polynomials will be separable polynomials of degree 7.

Here are some general facts to narrow down the search and make the results easier to interpret. Given a polynomial $p(x) \in \mathbb{Q}[x]$ of degree seven.

- If $p(x)$ is irreducible in $\mathbb{Q}[x]$ than $Gal(p)$ is a transitive subgroup of S_7 since $Gal(p)$ will be permuting all roots of $p(x)$.[1] Transitive subgroups of S_7 are $S_7,\ F_7,\ F_{21},\ F_{42},\ GL_3(\mathbb{F}_2)$, D_{14} and A_7.
- $D(p)$, the discriminant of of $p(x)$ is a square if and only if $Gal(p) \subseteq A_7$.[2]
- The transitive subgroups of A_7 are, A_7, $GL_3(\mathbb{F}_2)$ and F_{21}.
- $D(p) = 0$ if and only if $p(x)$ is not separable.[3]
- We will also use the following table to interpret our results.

Brief Summary of the Algorithm: Let $f(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$ of degree 7.

- Compute the discriminant D of $f(x)$.
- Factor the polynomial in $\mathbb{Z}/p\mathbb{Z}$ where p is one of the first 1000 primes and p does not divide D.
- For each factorization we will have a different cycle type, we will record the frequencies of each cycle type.
- Compare the results with Table 1 and determine the Galois group.

[1] p. 611
[2] p. 611
[3] p. 610

Cycle Type	1	2	(2,2)	(2,2,2)	(2,2,3)	(2,3)	(2,4)	(2,5)	3	(3,3)	(3,4)	4	5	6	7
F_7	1	-	-	-	-	-	-	-	-	-	-	-	-	-	6
D_{14}	1	-	-	7	-	-	-	-	-	-	-	-	-	-	6
F_{21}	1	-	-	-	-	-	-	-	-	14	-	-	-	-	6
F_{42}	1	-	-	7	-	-	-	-	-	14	-	-	-	14	6
$GL_3(\mathbb{F}_2)$	1	-	21	-	-	-	42	-	-	56	-	-	-	-	48
A_7	1	-	105	-	210	-	630	-	70	280	-	-	504	-	720
S_7	1	21	105	105	210	420	630	504	70	280	420	210	504	840	720

Table 1: Cycle Type Frequencies for Transitive Subgroups of S_7

2 Examples

1 - $p(x) = x^7 + 3x^4 - 6 \in \mathbb{Q}[x]$

We have that $p(x)$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion, hence the Galois group of $Gal(p)$ is isomorphic to a transitive subgroup of S_7. Discriminant D of $p(x)$ is $D = -35158048704$. When we compute the cycle type frequencies of $Gal(p)$, we find Figure 1.

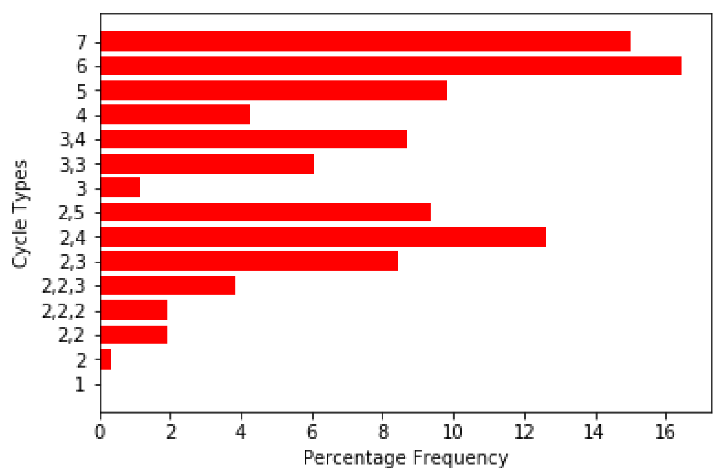

Figure 1: Cycle Type Frequencies for $Gal(p)$

We can verify from Table 1 that the only transitive subgroup of S_7 having all the cycle types is S_7 itself. Hence We have to have $Gal(p) = S_7$

2 - $f(x) = x^7 + 5 \in \mathbb{Q}[x]$

$f(x)$ is clearly irreducible in $\mathbb{Q}[x]$. The determinant of f is $D = -12867859375 = (-1) \cdot 5^6 \cdot 7^7$, not a square in $\mathbb{Q}$. Hence $Gal(f)$ is not a subgroup of A_7, this leaves us with the groups S_7, F_7, F_{42}, and D_{14}.

When we compute the cycle type frequencies of $Gal(f)$, we find Figure 2.

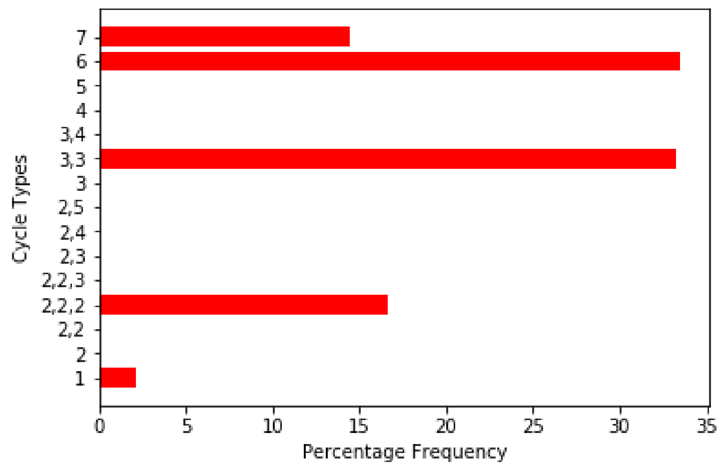

Figure 2: Cycle Type Frequencies for $Gal(f)$

Just by looking at the figure we can conclude that $Gal(f) \neq S_7$. Going back to Table 1, notice the only transitive subgroups of S_7 with $(2, 2, 2)$ cycles aside from S_7 itself are D_{14} and F_{42}. Since $Gal(f)$ contains $(2, 2, 2)$ cycle structures, we can automatically eliminate F_7 which has no $(2, 2, 2)$ cycles, so we are left with D_{14} and F_{42}.

Now notice that D_{14} contains no 6 cycles, while $Gal(f)$ does, hence $Gal(f) \neq D_{14}$. And we are left with only F_{42}, so $Gal(f) = F_{42}$. Figure 3 shows the Cycle Type Frequencies of F_{42}, which is evidently coinciding with Figure 2.

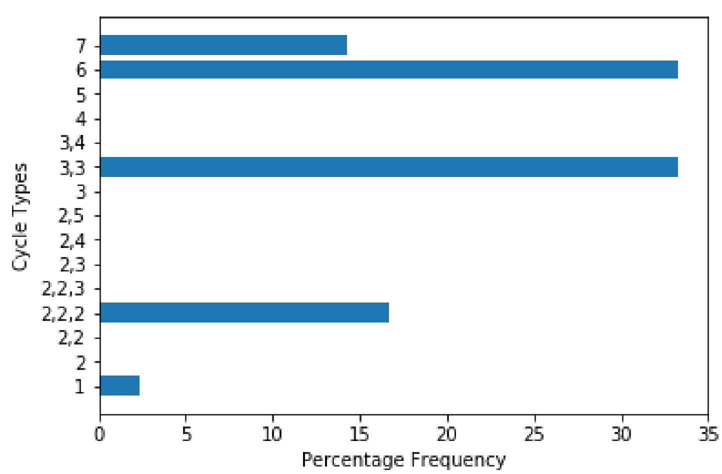

Figure 3: Cycle Type Frequencies for F_{42}

3 - $g(x) = x^7 - 56x + 48 \in \mathbb{Q}[x]$

We can easily verify that $g(x) = x^7 - 56x + 48$ is irreducible in $\mathbb{Q}[x]$. Computing the discriminant we obtain, $D = 70506920137457664 = 2^{24} \cdot 3^6 \cdot 7^8$. Hence, since D is a square in $\mathbb{Q}$, we can conclude that $Gal(g) \subseteq A_7$. So we have the candidates A_7, $GL_3(\mathbb{F}_2)$ and F_{21}. Computing the cycle type frequencies for $Gal(g)$, we have the following Figure.

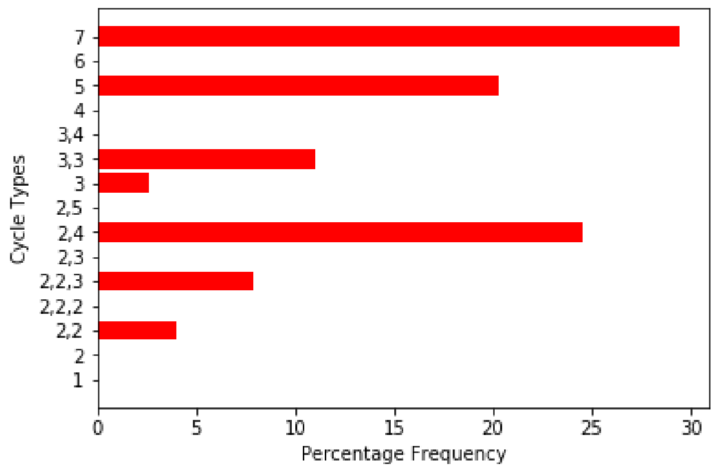

Figure 4: Cycle Type Frequencies for $Gal(g)$

Again, looking back at Table 1 observe that no proper subgroup of A_7, has cycle type $(2, 2, 3)$. So we have to have $Gal(g) = A_7$. Figure 5 shows the cycle type frequencies of the group A_7 which is coinciding with that of $Gal(g)$.

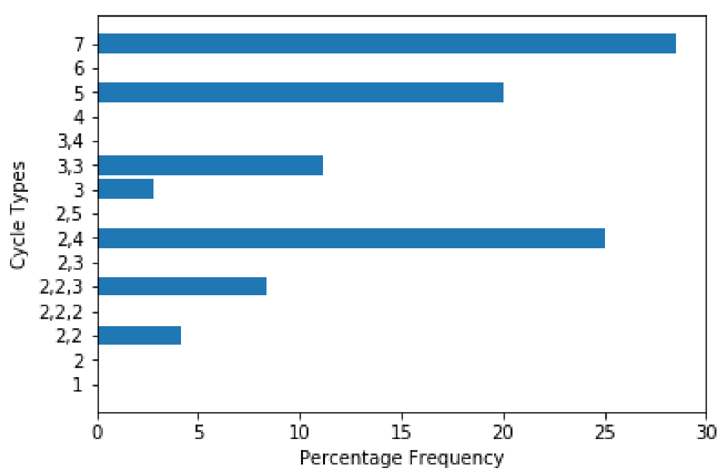

Figure 5: Cycle Type Frequencies for A_7

3 Sage Code

```
import numpy
import matplotlib.pyplot as plt

def percentage(cyc):
    c = 0
    for s in range(len(cyc)):
        c = c + cyc[s]
    g = []
    for i in range(len(cyc)):
        g.append(100*cyc[i]/c)
    return g

R.<x> =QQ[]
f = x^7-56*x+48;
disc = f.discriminant();
primes = []

for p in range(0,10000):
    primes.append(Primes()[p])
factors = list(disc.factor())

for i in range(len(factors)):
    if factors[i][0] in primes:
        primes.remove(factors[i][0])

cycletypes = [[1], [2], [2,2], [2,2,2], [2,2,3], [2,3],
[2,4], [2,5], [3], [3,3], [3,4],[4], [5], [6], [7]]
frequency = numpy.zeros(len(cycletypes))
Poly=[]

for p in primes:
    F.<x> = GF(p)[]
    evaluate = F(f)
    Poly.append(list(factor(evaluate)))
ct_f=[]

for i in range(len(Poly)):
    k = []
    for j in range(len(Poly[i])):
```

```
            if Poly[i][j][0].degree() != 1:
                k.append(Poly[i][j][0].degree())
    if k == []:
        k=[1]
    ct_f.append(k)

for i in range(len(ct_f)-1):
    frequency[cycletypes.index(ct_f[i])] += 1
frequency=100*frequency/len(ct_f)
finfreq=[]
for t in frequency:
    finfreq.append(t)
c_chart = ['1','2','(2,2)','(2,2,2)','(2,2,3)','(2,3)','(2,4)',
'(2,5)','3','(3,3)','(3,4)','4','5','6','7']

galois_g = plt.barh(c_chart, finfreq, color="red")
# actual_g = plt.barh(c_chart, convert_to_percentage([1,0,105,0,210,
# 0,630,0,70,280,0,0,504,0,720]))
plt.xlabel('Percentage Frequency')
plt.ylabel("Cycle Types")
plt.figure(figsize=(10, 10));
```