# Determining Galois Groups of Polynomials with Factorization Under $\mathbb{Z}_p[x]$

Yaman Yağız Taşbağ
21601639

May 14, 2020

## 1 Introduction

In this report we will give examples of how to determine and guess the galois group of a degree 7 polynomial. There are 3 examples with galois groups of $S_7$, $A_7$ and neither $S_7$ nor $A_7$ (which is $D_{14}$ in our case). The polynomials are:

- $f_1 = x^7 + 11x^6 + 42x^5 + 45x^4 + 34x^3 + 31x^2 + 24x + 16$, $S_7$
- $f_2 = x^7 - 28x^2 - 35x - 10$, $A_7$
- $f_3 = x^7 + 2x^6 + x^5 + x^4 + x^3 + 5x^2 + 9x + 5$, $D_{14}$

## 2 Methodology

To predict the galois group I have divided the task into two parts: pre-processing of subgroups of $S_7$ and calculating the cycle distribution of polynomials. The pre-processing process was as follows:

- Calculate all subgroups of $S_7$.
- Remove non-transitive ones.
- Remove isomorphic ones.
- Go over each element of remaining subgroups and calculate cycle frequency.
- Plot the frequencies.

See Script 12. At this point there were 7 transitive subgroups of $S_7$ up to isomorphism.

Calculation of cycle distribution of polynomials was as follows:

- Generate 1000 primes.
- For each prime $p$:
  - if p divides discriminant of polynomial $f$ continue.
  - factor $f$ in $\mathbb{Z}_p[x]$ according to degrees of factors calculate frequency.
- Plot the frequency.

See Script 13.

# 3 Examples

As mentioned before there were 7 subgroups of $S_7$ to consider. They were of the following orders: 7, 14, 21, 42, 168, 2520, 5040. They had the following cycle distributions:

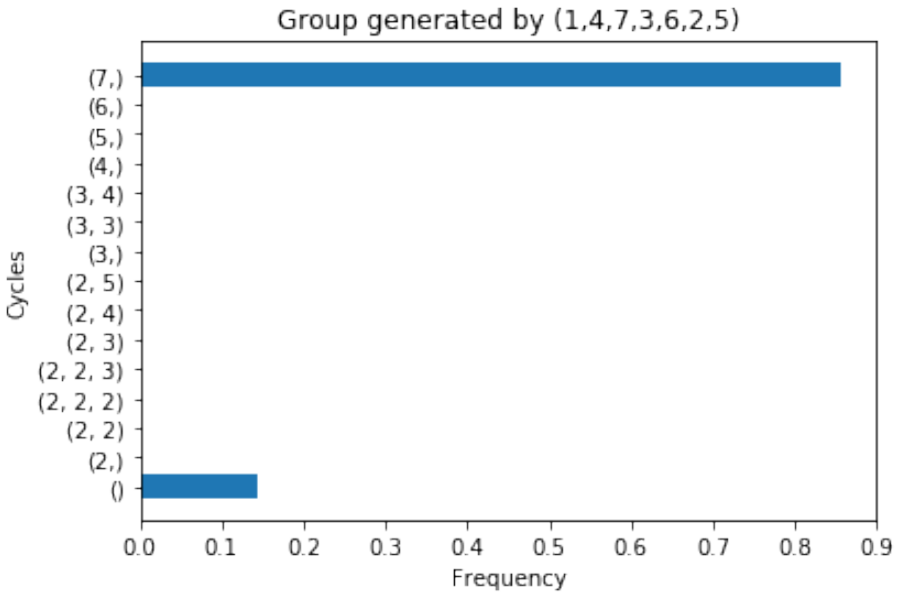


Figure 1: Cycle distribution of the subgroup of order 7

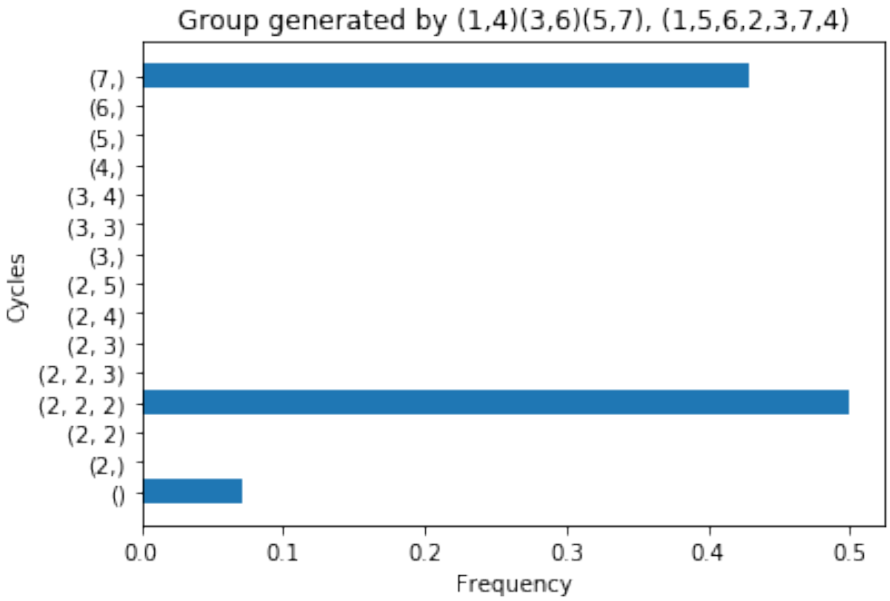


Figure 2: Cycle distribution of the subgroup of order 14

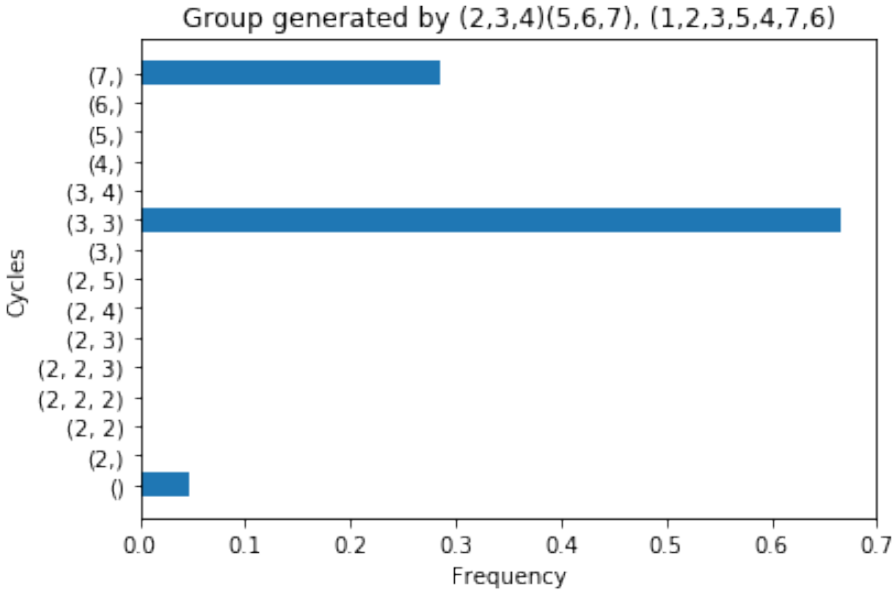


Figure 3: Cycle distribution of the subgroup of order 21

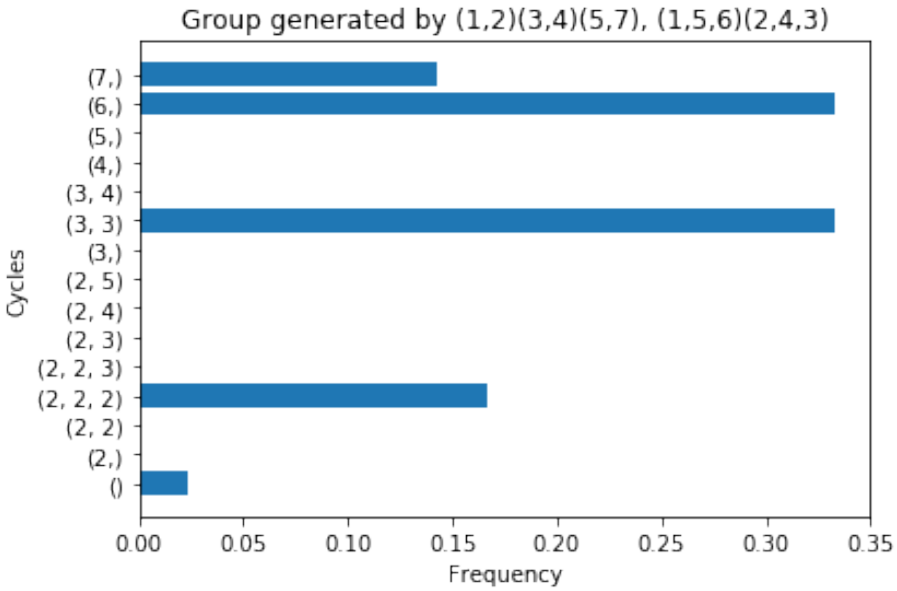


Figure 4: Cycle distribution of the subgroup of order 42

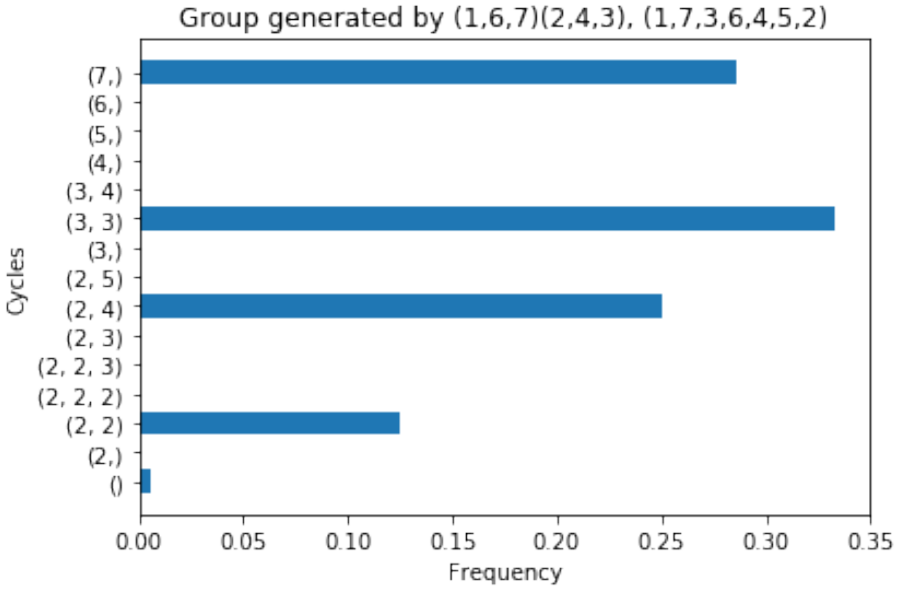


Figure 5: Cycle distribution of the subgroup of order 168

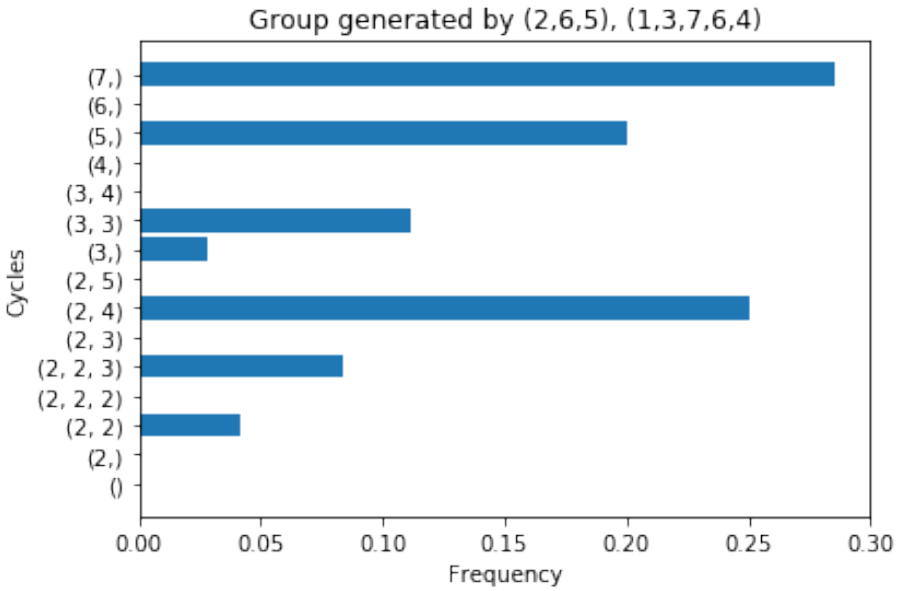


Figure 6: Cycle distribution of the subgroup of order 2520

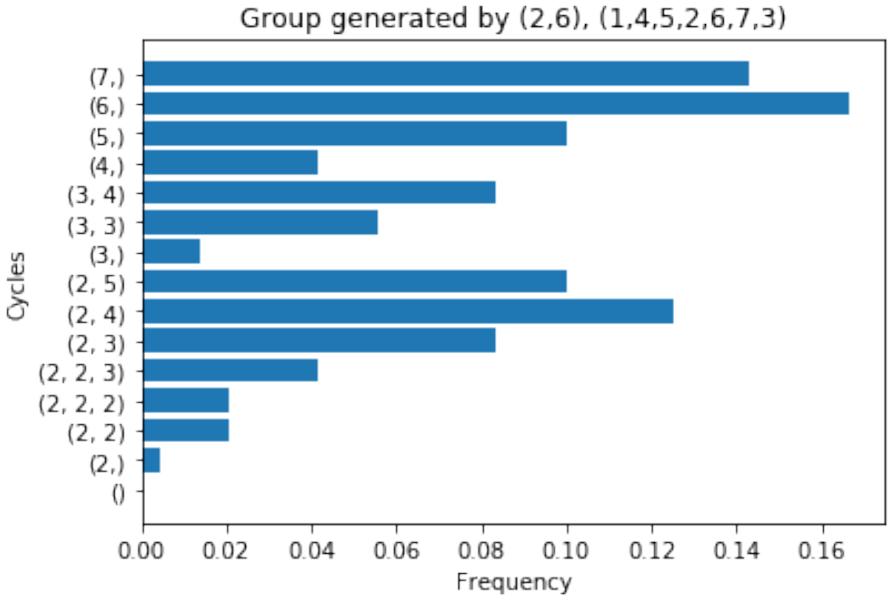


Figure 7: Cycle distribution of the subgroup of order 5040

### 3.1 Example with $S_7$

When we run the polynomial $f_1$ through script 13 we see the following distribution:

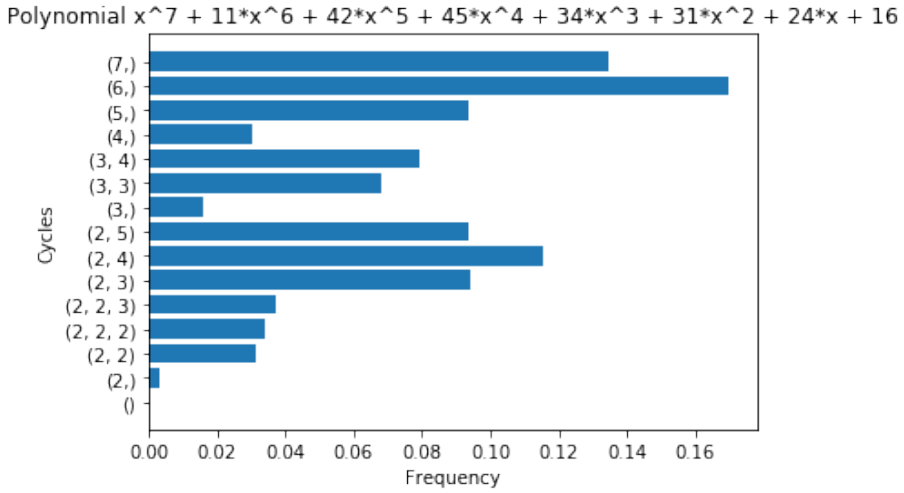


Figure 8: Cycle distribution of the polynomial $f_1$

As we can see the galois group of $f_1$ contains a 2 cycle which is only present in $S_7$. Therefore the galois group of $f_1$ is $S_7$

### 3.2 Example with $A_7$

When we run the polynomial $f_2$ through script 13 we see the following distribution:

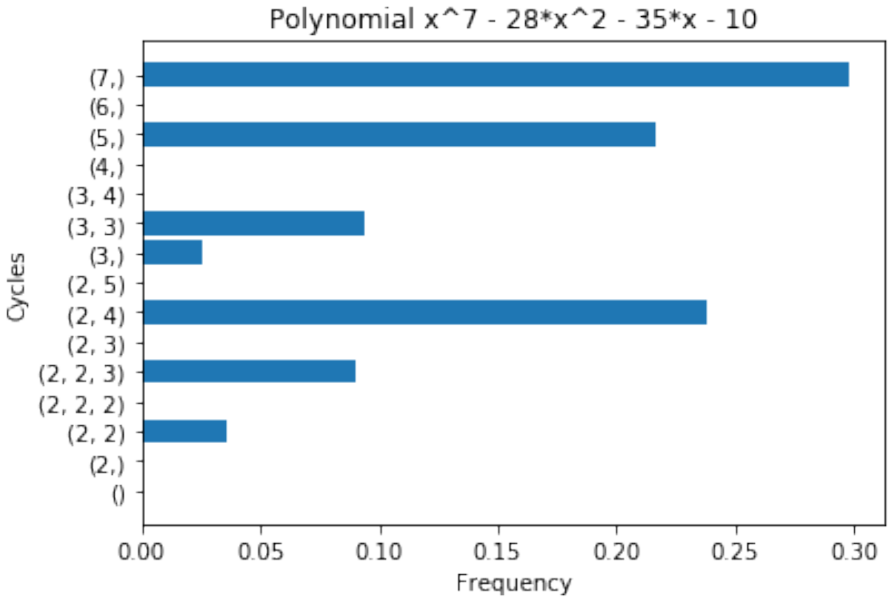


Figure 9: Cycle distribution of the polynomial $f_2$

The discriminant of $f_2$ is $207532836000000 = 14406000^2$. Therefore the galois group of $f_2$ is a subgroup of $A_7$. But no transitive subgroup of $A_7$ have a 2-2-3 cycle. Therefore the galois group of $f_2$ is $A_7$.

### 3.3 Example with $D_{14}$

When we run the polynomial $f_3$ through script 13 we see the following distribution:

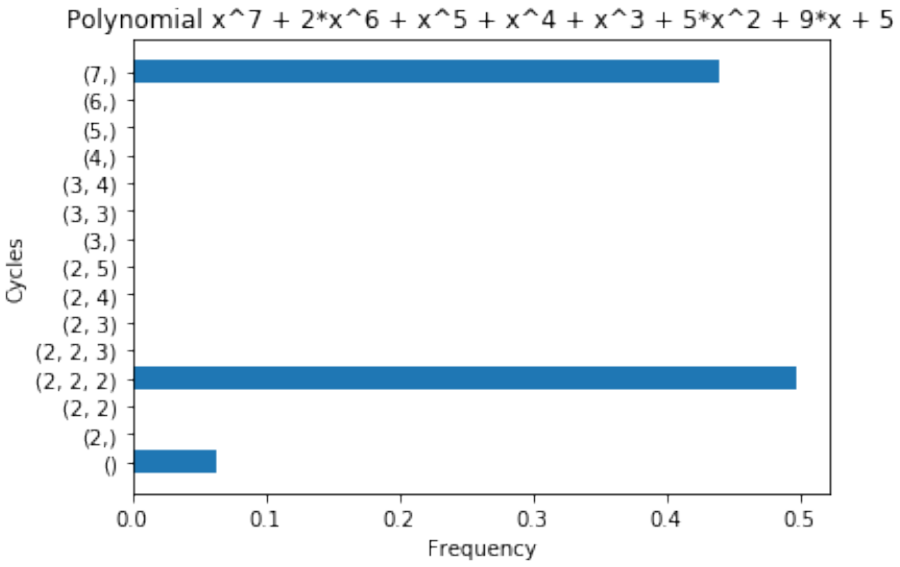


Figure 10: Cycle distribution of the polynomial $f_2$

The discriminant of $f_3$ is $-62114843752$ which is not a square in $\mathbb{Q}$. Therefore the galois group of $f_3$ is not a subgroup of $A_7$. From the distribution we can see the one it is most similar to is the subgroup of order 14 which is $D_{14}$. But it can also be the subgroup of order 42. But it would be a safe guess that the galois group is actually $D_{14}$. Sage also confirms our guess:

```
R = QQ["x"]
f = x^7 + 2*x^6 + x^5 + x^4 + x^3 + 5*x^2 + 9*x + 5
G = NumberField(f, 'theta').galois_group(type="pari")
print(G) # Galois group PARI group [14, -1, 2, "D(7) = 7:2"] of
    degree 7 of the Number Field in theta with defining polynomial
    x^7 + 2*x^6 + x^5 + x^4 + x^3 + 5*x^2 + 9*x + 5
```

Figure 11: Galois group of $f_3$

# Appendices

## A Scripts

```
import matplotlib.pyplot as plt

S = SymmetricGroup(7)
tsg = filter(lambda s: s.is_transitive(), S.subgroups())
final_tsg = []

for tg in tsg:
    should_add = True
    for g2 in final_tsg:
        if tg.is_isomorphic(g2):
            should_add = False
            break
    if should_add:
        final_tsg.append(tg)

transitive_groups = final_tsg

cycles = [dict() for _ in range(7)]
for i in range(7):
    G = transitive_groups[i].list()
    for a in G:
        b = a.cycle_tuples()
        b = map(len, b)
        b.sort()
        b = tuple(b)
        if b not in cycles[i]:
            cycles[i][b] = 0
        cycles[i][b] += 1

for i in range(7):
    G = transitive_groups[i].list()
    l = len(G)
    for e in cycles[i]:
        cycles[i][e] = cycles[i][e] / l

cs = set()
for i in range(7):
    cs = cs.union(set(cycles[i].keys()))

for i in range(7):
    for c in cs:
        if c not in cycles[i]:
            cycles[i][c] = 0

for i in range(7):
    plt.figure(i)
    l = cycles[i].items()
    l.sort()
    keys = map(lambda s: str(s[0]), l)
    values = map(lambda s: s[1], l)
    plt.ylabel("Cycles")
    plt.xlabel("Frequency")
    gs = map(str, transitive_groups[i].gens())

    plt.title("Group generated by " + ", ". join(gs))
    plt.barh(keys, values)
    plt.show()
```

Figure 12: Script for plotting subgroup cycle frequencies

```
import matplotlib.pyplot as plt
R = QQ["x"]
f = <POLYNOMIAL>
f = R(f)
ps = []
p = 2
l = 1000
for _ in range(l):
    ps.append(p)
    p = next_prime(p)


d = l
cs = set([(2, 3), (2, 2, 3), (2, 5), (2, 2, 2), (3, 3), (2,), (3,),
     (4,), (5,), (), (6,), (2, 2), (7,), (3, 4), (2, 4)])
cycles = dict()

for c in cs:
    cycles[c] = 0

for p in ps:
    if f.discriminant() % p == 0:
        d -= 1
        continue
    S = GF(p)["y"]
    f2 = S(f)
    fs = list(factor(f2))
    fs = filter(lambda s: s != 1, map(lambda s: s[0].degree(), fs))
    fs.sort()
    fs = tuple(fs)
    # print(fs)
    cycles[fs] += 1

for c in cs:
    cycles[c] = cycles[c] / d

calc = cycles.items()
calc.sort()

keys = map(lambda s: str(s[0]), calc)
values = map(lambda s: s[1], calc)
plt.ylabel("Cycles")
plt.xlabel("Frequency")
plt.title("Polynomial " + str(f))
plt.barh(keys, values)
```

Figure 13: Script for plotting polynomial cycle frequencies