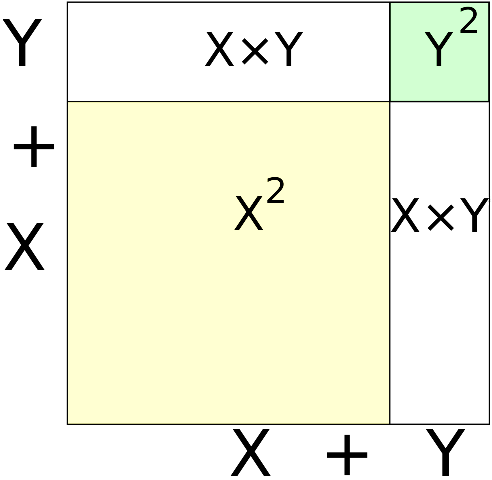
What are...the Galois groups of finite fields?

Or: Finite fields are easy

Freshman's dream



- A freshman dreams: $(X+Y)^q = X^q + Y^q$
- Common sense This is nonsense, you are missing the white bits
- Frobenius Well, maybe not

The Frobenius endomorphism

- The bait Freshman's dream works in prime characteristic p, *e.g.*

$$(X+Y)^3 = X^3 + 3 \cdot X^2Y + 3 \cdot XY^2 + Y^3 \xrightarrow[\text{a.k.a. mod 3}]{\text{characteristic 3}} X^3 + Y^3$$

- The catch Ok, not quite – the powers q need to be $q = p^k$, *e.g.*

$$(X+Y)^3 = X^6 + 6 \cdot X^5Y + 15 \cdot X^4Y^2 + 20 \cdot X^3Y^3 + 15 \cdot X^2Y^4 + 6 \cdot XY^5 + Y^6 \xrightarrow[\text{a.k.a. mod 3}]{\text{characteristic 3}} X^6 + 2 \cdot X^3Y^3 + Y^6$$

Frobenius: This gives an automorphism $\sigma_q\colon \mathbb{F}_q \to \mathbb{F}_q, a \mapsto a^q$

~~Fermat's~~ Frobenius's little theorem

For any $q' \geq q$, $\sigma_q \colon \mathbb{F}_{q'} \to \mathbb{F}_{q'}, a \mapsto a^q$ is an isomorphism

Example For $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{F}_{3^2} = \mathbb{F}_3[X]/(X^2 + X + 2 = 0)$, $\sigma_3 \colon \mathbb{F}_{3^2} \to \mathbb{F}_{3^2}$ is

	0,0	0,1	0,2	1,0	1,1	1,2	2,0	2,1	2,2
0,0	1								
0,1		1							
0,2			1						
1,0									1
1,1							1		
1,2								1	
2,0					1				
2,1						1			
2,2				1					

This "matrix" has order 3

For completeness: The formal statement

If $\mathbb{L}$ is an algebraic field extension over $\mathbb{K} = \mathbb{F}_q$ with $q = p^k$, then:

(a) $\mathbb{L}$ is Galois over $\mathbb{K}$ Always!

(b) The Galois group $G(\mathbb{L}/\mathbb{K}) = \mathrm{Aut}(\mathbb{L}/\mathbb{K})$ is cyclic $G(\mathbb{L}/\mathbb{K}) \cong \mathbb{Z}/[\mathbb{L} : \mathbb{K}]\mathbb{Z}$

(c) We have $G(\mathbb{L}/\mathbb{K}) = \langle \sigma_q \rangle$ Generated by the Frobenius automorphism

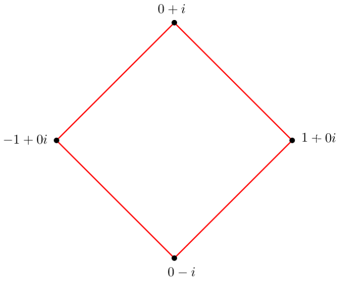
For comparison, $\mathbb{Q}$ is more complicated:

- Not every algebraic $\mathbb{L}$ over $\mathbb{Q}$ is Galois
- The Galois group $G(\mathbb{L}/\mathbb{Q})$ is rarely cyclic:

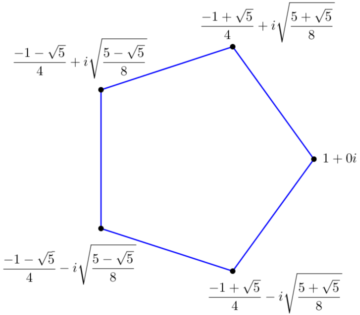
$$\frac{|\text{polynomials of degree} \leq d \text{ with coefficients bounded by } N|}{|\text{ditto} + \text{Galois group being } S_d|} \xrightarrow{N \to \infty} 1$$

- The Galois group $G(\mathbb{L}/\mathbb{Q})$ is rarely generated by a nice element

Solving polynomial equations over finite fields



The 4^{th} roots of unity



The 5^{th} roots of unity

- $p(X)=0$ has a solution in $\mathbb{F}_q \Leftrightarrow \gcd(p, X^q - X) \neq 1$ Surprisingly easy
- There is a nice and efficient algorithm to factor polynomials over $\mathbb{F}_q$ Berlekamp's algorithm
- Catch Freshman's dream implies that there are no primitive qth roots of unity

Thank you for your attention!

I hope that was of some help.