Math 5402

4/27/20

week 14

4/27 13, 6 Ch. 14	4/29 Ch. 14
5/4 Ch. 14	5/6 review
	5/13 Final

13.6 continued...

Last time

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

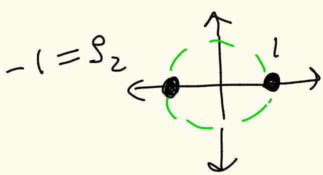
where

$$\Phi_d(x) = \prod_{\substack{1 \le a \le d \\ \gcd(a,d)=1}} (x - \zeta_d^a)$$

Ex:

$$\Phi_1(x) = x - 1 \quad \leftarrow \quad \zeta_1 = 1$$

$$\Phi_2(x) = (x - (-1)) \quad \leftarrow \quad x^2 - 1 = 0$$
$$= x + 1$$



Let's calculate $\Phi_3(x)$

$$x^3 - 1 = \prod_{d|3} \Phi_d(x) = \Phi_1(x)\,\Phi_3(x)$$

$$\Phi_3(x) = \frac{x^3-1}{\Phi_1(x)} = \frac{x^3-1}{x-1} = \underbrace{x^2+x+1}$$

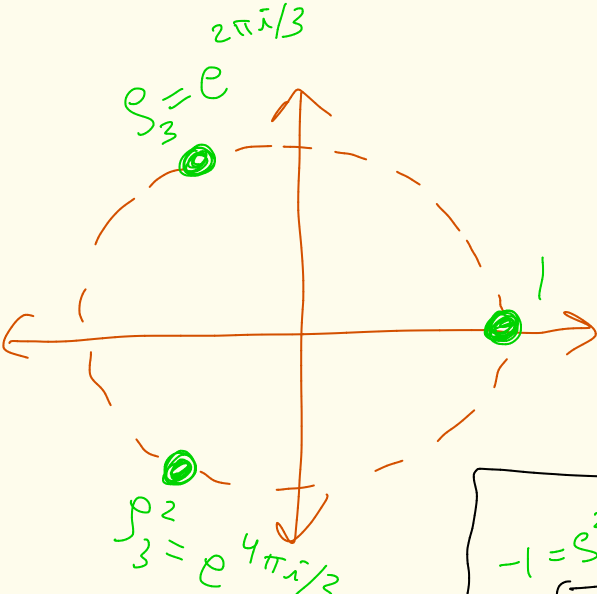
roots are

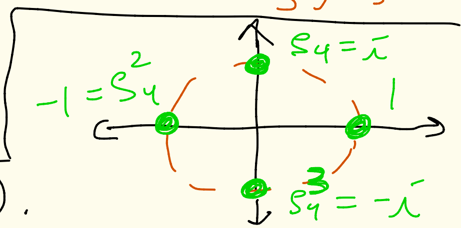
$$x = \frac{-1 \pm \sqrt{1^2-4}}{2}$$

$$= \frac{-1 \pm \sqrt{-3}}{2}$$

$$= \frac{-1 \pm \sqrt{3}\, i}{2}$$

$$= \zeta_3,\ \zeta_3^2$$





Let's calculate $\Phi_4(x)$.

$$x^4 - 1 = \prod_{d|4} \Phi_d(x) = \Phi_1(x)\,\Phi_2(x)\,\Phi_4(x)$$

$$\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\Phi_2(x)} = \frac{(x^2-1)(x^2+1)}{(x-1)(x+1)} = x^2+1$$

$\boxed{\text{roots are } \zeta_4 = i,\ \zeta_4^3 = -i}$

Theorem: The cyclotomic polynomial $\Phi_n(x)$ is monic, irreducible, $\Phi_n(x) \in \mathbb{Z}[x]$, and $\deg(\Phi_n) = \varphi(n) = |\mathbb{Z}_n^\times|$

$$= \left| \left\{ a \in \mathbb{Z} \;\middle|\; \begin{array}{c} 1 \le a \le n \\ \gcd(a,n)=1 \end{array} \right\} \right|$$

pf of special case where $n = p$ and p is prime:

Since p is prime, $x^p - 1 = \prod_{d \mid p} \Phi_d(x) = \Phi_1(x)\Phi_p(x)$.

So, $\Phi_p(x) = \dfrac{x^p - 1}{\Phi_1(x)} = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$

$\boxed{\text{poly division}}$

$\boxed{\text{Ex: } \Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1}$

We see that $\Phi_p(x)$ is monic, in $\mathbb{Z}[x]$, and $\deg(\Phi_p) = p - 1 = \varphi(p)$.

Note that

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = \frac{(x+1)^p - 1}{x}$$

$$= \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \dots + \binom{p}{p-1}x + \binom{p}{p}x^0 - 1}{x}$$

$$= \frac{x^p + px^{p-1} + \frac{p(p-1)}{2}x^{p-2} + \dots + px + 1 - 1}{x}$$

$$= x^{p-1} + px^{p-2} + \frac{p(p-1)}{2}x^{p-3} + \dots + \binom{p}{p-2}x + p$$

Recall: $p \mid \binom{p}{k}$ when $1 \le k \le p-1$.

So, $\Phi_p(x+1)$ is irreducible over $\mathbb{Q}$ by Eisenstein with the prime p.

So, $\Phi_p(x)$ must also be irreducible. $\blacksquare$

[why? If $\Phi_p(x) = f(x)g(x)$, then $\Phi_p(x+1) = f(x+1)g(x+1)$]

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Corollary:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

proof: Since $\Phi_n(\zeta_n) = 0$ and Φ_n is irreducible, we have $\min_{\zeta_n, \mathbb{Q}}(x) = \Phi_n(x)$.

So, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(m_{\zeta_n, \mathbb{Q}}(x))$

$= \deg(\Phi_n(x))$

$= \varphi(n)$ $\blacksquare$

$$\mathbb{Q}(\zeta_n) = \left\{ a_0 + a_1 \zeta + a_2 \zeta^2 + \dots + a_{\varphi(n)-1} \zeta^{\varphi(n)-1} \,\middle/\, a_i \in \mathbb{Q} \right\}$$

Def: Let K be a field. The set of automorphisms of K is

$$\mathrm{Aut}(K) = \left\{ \sigma : K \to K \;\middle|\; \begin{array}{c}\sigma \text{ is a field} \\ \text{isomorphism}\end{array} \right\}$$

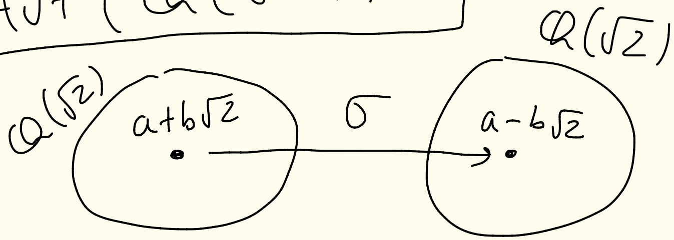
Ex: $\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$

$\sigma : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$

$\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$

You can check that σ is a field isomorphism.

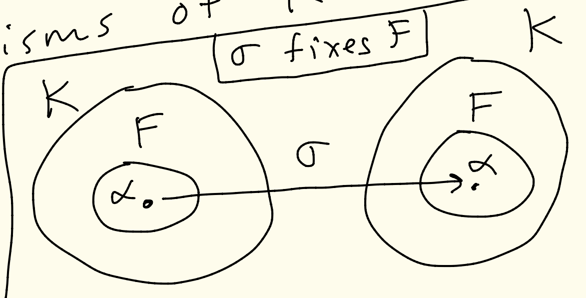
So, $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$.



Notation: If $\sigma \in \mathrm{Aut}(K)$ and $\alpha \in K$, sometimes we write $\sigma\alpha$ for $\sigma(\alpha)$.

Def: Let K and F be fields with $F \subseteq K$. So, K/F is an extension field.

- Given $\sigma \in \mathrm{Aut}(K)$ and $\alpha \in K$ we say that σ fixes α if $\sigma(\alpha) = \alpha$.
- Given $\sigma \in \mathrm{Aut}(K)$, we say that σ fixes F if $\sigma(\alpha) = \alpha$ for all $\alpha \in F$.
- Let $\mathrm{Aut}(K/F)$ be the automorphisms of K that fix F.

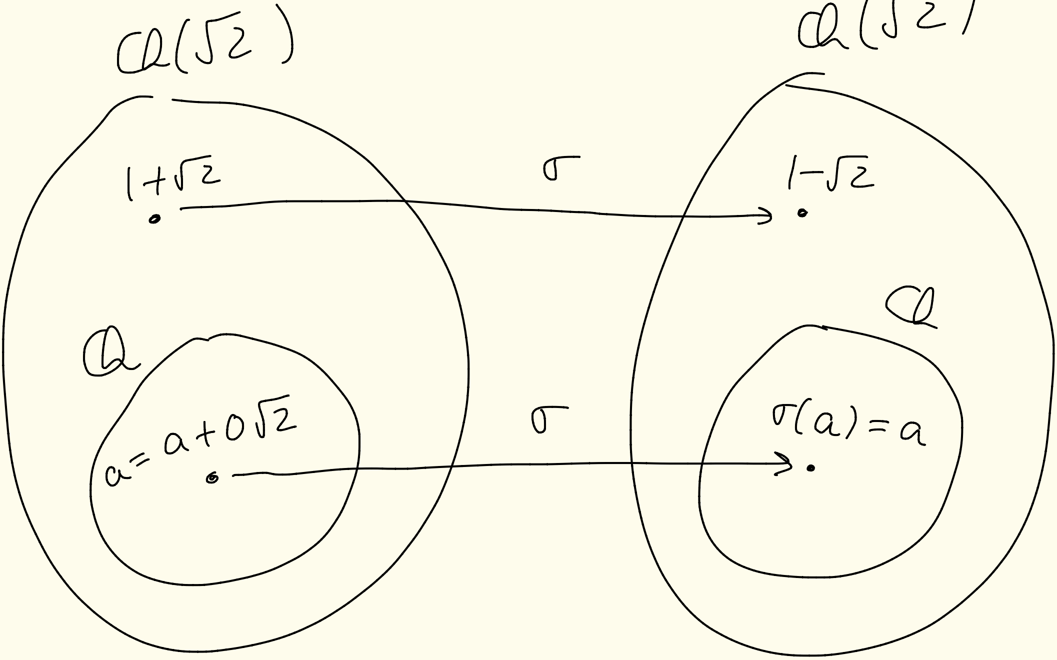


Ex: $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$

$$\sigma(a+b\sqrt{2}) = a - b\sqrt{2}$$

Then σ fixes $\mathbb{Q}$.

So, $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$



$$\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$$

$\mathbb{Q}$ corresponds to all the elements of the form $a + 0\sqrt{2} = a$

Ex: Let K be a field and F be its prime subfield (field generated by 1)

pg 10

[Ex: $K = \mathbb{R}$, $F = \mathbb{Q}$]

Let $\sigma \in \mathrm{Aut}(K)$.
Let $\alpha \in F$.
Then α is a product of elements of the form $1+1+\dots+1$ or $-1-1-\dots-1$ or $(1+1+\dots+1)^{-1}$ or $(-1-1-\dots-1)^{-1}$.

Since $\sigma: K \to K$ is an isomorphism, $\sigma(1) = 1$. Hence $\sigma(\alpha) = \alpha$.

Thus, $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$ where F is the prime subfield of K.

So, $\mathrm{Aut}(\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}/\mathbb{Q}) = \{id\} = \{1\}$ and $\mathrm{Aut}(\mathbb{Z}_p) = \mathrm{Aut}(\mathbb{Z}_p/\mathbb{Z}_p) = \{id\} = \{1\}$