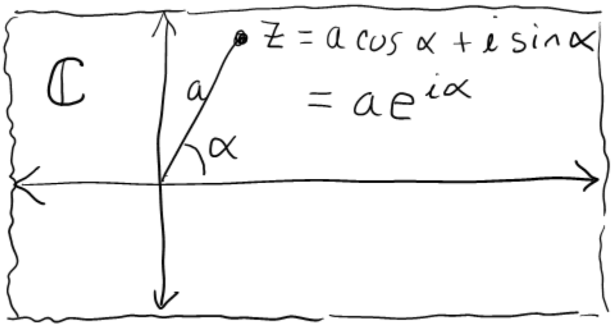
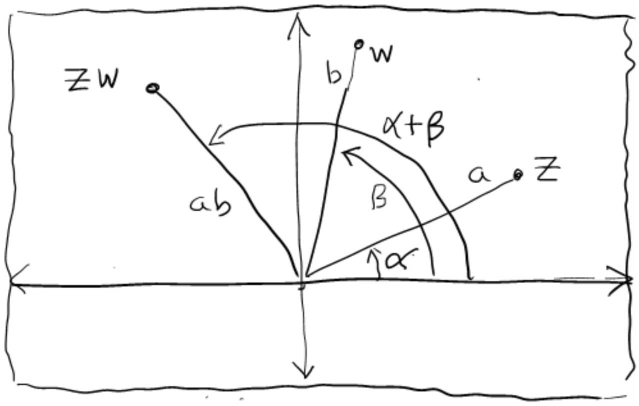
Section 13.4 Splitting Fields

We will be factoring polynomials all over the place, but especially in $\mathbb{C}$, so this may be a good time to review complex multiplication.

Recall the polar representation of complex numbers:



Geometric interpretation of multiplication of complex #'s:



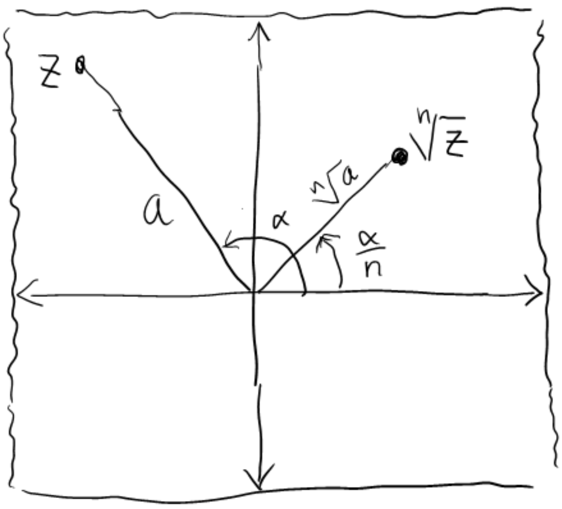
If $z = ae^{i\alpha}$ and $w = be^{i\beta}$ then $zw = ae^{i\alpha}be^{i\beta} = abe^{i(\alpha+\beta)}$ has polar angle $\alpha+\beta$ and modulus ab.

N^{th} Roots

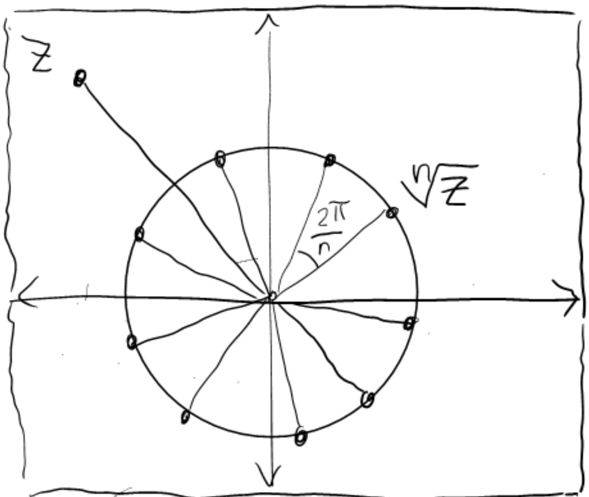
If $a \in \mathbb{R}$, $\sqrt[n]{a}$ denotes the positive $x \in \mathbb{R}$ with $x^n = a$

Other n^{th} roots of a are negative or complex.

Principal n^{th} root of $z \in \mathbb{C}$



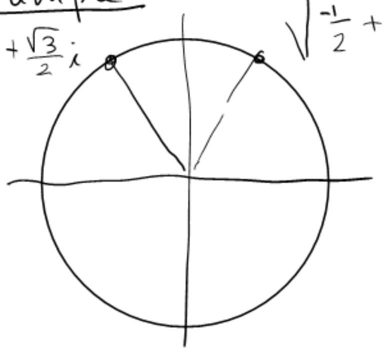
Other n^{th} roots of z



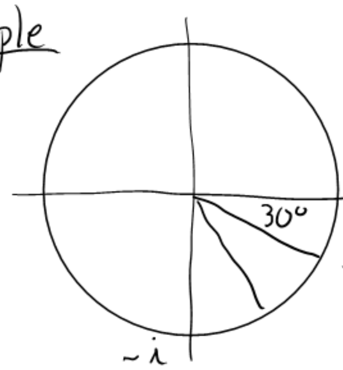
Example

$z = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$

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



Example



$\sqrt[3]{-i} = \frac{\sqrt{3}}{2} - \frac{i}{2}$

Definitions

$f(x) \in K[x]$ splits in $K[x]$ (or "over K") if $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ for $\alpha_1\ \alpha_2 \cdots \alpha_n \in K$

Given $f(x) \in F[x]$, extension K/F is a splitting field for $f(x)$ if $f(x)$ splits in $K[x]$ but does not split in any $L[x]$ for $F \subseteq L \subset K$

Example $\mathbb{C}$ is splitting field for $f(x) = x^2+1 \in \mathbb{R}[x]$

Example $\mathbb{R}$ not splitting field for $f(x) = x^2-2 \in \mathbb{Q}[x]$
Even though we have $f(x) = (x+\sqrt{2})(x-\sqrt{2})$ in $\mathbb{R}[x]$, there is a field smaller than $\mathbb{R}$ that does the job: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$

(splitting field for $f(x)$)

Theorem 25 If $f(x) \in F[x]$, then there is an extension K/F that is a splitting field for $f(x)$

Proposition 26 If K is a splitting field for $f(x) \in F[x]$ and $\deg f = n$, then $[K:F] \le n!$

Proof

$$
\begin{array}{lcl}
 & F(\alpha_1 \alpha_2 \alpha_3 \cdots \alpha_n) & \leftarrow f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \\
\le 1 & | & \\
\vdots & \vdots & \\
\le n-2 & | & \\
 & F(\alpha_1 \alpha_2) & \leftarrow f(x) = (x-\alpha_1)(x-\alpha_2) f_2(x) \\
\le n-1 & \| & \\
 & F(\alpha_1) & \leftarrow f(x) = (x-\alpha_1) f_1(x) \\
\le n & | & \\
 & F & \leftarrow f(x) \quad (\text{degree } n)
\end{array}
$$

Theorem 27 and **Corollary 28**

Any two splitting fields for $f(x) \in F[x]$ are isomorphic.

Example Find splitting field of $x^2-5 \in \mathbb{Q}[x]$ and its degree over $\mathbb{Q}$

Roots of x^2-5 are $\pm\sqrt{5}$

Splitting field: $\mathbb{Q}(\sqrt{5}) = \{a+b\sqrt{5} \mid a,b \in \mathbb{Q}\}$ (degree 2)

Example Find splitting field of $x^2-5x+1 \in \mathbb{Q}[x]$ and its degree over $\mathbb{Q}$

Roots $\dfrac{5 \pm \sqrt{(-5)^2-4\cdot 1\cdot 1}}{2\cdot 1} = \dfrac{5 \pm \sqrt{21}}{2} = \frac{5}{2} \pm \frac{1}{2}\sqrt{21}$

Splitting field: $\mathbb{Q}(\sqrt{21}) = \{a+b\sqrt{21} \mid a,b \in \mathbb{Q}\}$ (degree 2)

Example Find splitting field for $x^4-5x^3-4x^2+25x-5$

$= (x^2-5)(x^2-5x+1)$. Roots: $\pm\sqrt{5}$, $\dfrac{5 \pm \sqrt{21}}{2}$

Thus $\mathbb{Q}(\sqrt{5}) \subseteq K$

Note: $\sqrt{21} \notin \mathbb{Q}(\sqrt{5})$

Otherwise $\sqrt{21} = a + b\sqrt{5}$

$21 = a^2 + 2ab\sqrt{5} + 5b^2$

$\sqrt{5} = \dfrac{21 - a^2 - 5b^2}{2ab}$ (rational)

but $\sqrt{5}$ is not rational!

Conclusion

$K = \mathbb{Q}(\sqrt{5}, \sqrt{21})$

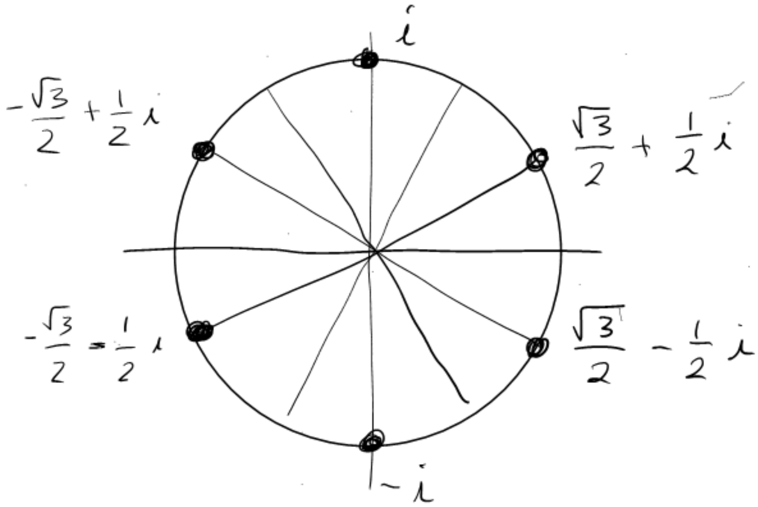
$= \{a + b\sqrt{5} + c\sqrt{21} + d\sqrt{5}\sqrt{21} \mid a,b,c,d \in \mathbb{Q}\}$

Degree is 4

$$\begin{tikzcd}
 & K \arrow[dl, dash, "2"'] \arrow[d, dash] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{5}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{105}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{21}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Example Find splitting field of $x^6+1 \in \mathbb{Q}[x]$

Roots:



$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{3}, i) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Splitting Field: $\mathbb{Q}(\sqrt{3}, i) = \{a + b\sqrt{3} + ci + d\sqrt{3}i \mid a,b,c,d \in \mathbb{R}\}$

Has basis $\{1, \sqrt{3}, i, i\sqrt{3}\}$. Degree is 4.

Algebraic Closure

Definitions A field K is algebraicly closed if every $f(x) \in K[x]$ has a root in K (and consequently splits over K).

Ex $\mathbb{Q}$ not algebraicly closed x^2-2 has no root
$\mathbb{Q}(\sqrt{2})$ not alg. closed since x^2-3 has no root
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ not algebraicly closed
$\mathbb{R}$ not algebraicly closed, x^2+1 has no root
$\mathbb{R}(i) = \mathbb{C}$ is algebraicly closed!

Given F an extension $\overline{F}/F$ is called an algebraic closure of F if

① Every $a \in \overline{F}$ is a root of a polynomial $f(x) \in F[x]$.
"Every a serves a purpose: $\overline{F}$ doesn't have too much stuff."

② Every $f(x) \in F[x]$ splits over $\overline{F}$
"$\overline{F}$ has enough stuff to get the job done"

Example $\overline{\mathbb{Q}} = \mathbb{C}$, $\overline{\mathbb{R}} = \mathbb{C}$

Proposition 30 Every field F has an algebraic closure $\overline{F}$

Proof is not hard but is very formal.

Proposition 29 $\overline{\overline{F}} = \overline{F}$ (i.e. $\overline{F}$ is all you need)

Proposition 31 The algebraic closure of F is unique up to isomorphism.

These results on algebraic closure are not particularly useful in and of themselves, but they provide a useful philosophical backdrop. In talking about a polynomial $f(x) = F[x]$, we can (and very often do!) bring into the discussion a root α of $f(x)$ without even saying what extension α belongs to. Blanket assumption: α belongs to "THE" algebraic closure of F.

In particular $F(\alpha) \subseteq \overline{F}$