מכון ויצמן למדע

תוכנית רוטשילד ויצמן

עבודת גמר בנושא: בניות גיאומטריות בעזרת סרגל ומחוגה

מנחה : ד"ר אברהם איזנבוד

מגיש : ממדוח בשיר

מועד הגשה : אוגוסט 2016

מבוא

בניה בעזרת סרגל ומחוגה בלבד היא אחת הבניות הקלאסיות הקיימות במתמטיקה, והיא העסיקה מתמטיקאים מאז יוון העתיקה שהצליחו לבנות בניות רבות אך נכשלו באחרות, חקר בניות כאלה נמשך אלפי שנים, גאוס למשל, הראה שלא ניתן באמצעות סרגל ומחוגה בלבד לבנות כל מצולע משוכלל. וחלק מבעיות הבניה המפורסמות הוכחו כבלתי אפשריות ע"י pierre wantzel בשנת 1837 תוך שימוש בתורת השדות.

למה חשוב למתמטיקאים לחקור בניות כאלה ?

היוונים המציאו וניסחו חלק גדול מאד ממה שאנחנו מכירים בגיאומטריה של המישור, ובעיקר אוקלידיס שטרח לכתוב את הידע העצום שלו בספר שנקרא " Elements" שנחשב עד היום לספר מרכזי בגיאומטריה של המישור והמרחב, בספר זה אוקלידיס השתמש בצורה מורחבת בבניות בעזרת סרגל ומחוגה ובכך הפכו לחלק אינטגראלי בלתי נפרד מחקר הגיאומטריה של המישור, שסיפקו גם תובנה למושגים גיאומטריים ונתנו כלים לשרטט עצמים מסוימים כאשר מדידות ישירות לא מתאימות.

וכאן נשאלת השאלה: למה אוקלידיס עשה זאת?

למה אוקלידס לא מדד בפשטות דברים בעזרת סרגל וחישב את אורכם, אחת הבניות הבסיסיות למשל, היא לחצות קטע ישר לשני קטעים שווים, אז למה לא למדוד את אורכו ולחצות אותו לשניים?

היוונים התעניינו בבניות בעזרת סרגל ומחוגה בגלל הפשטות בשימוש בשני כלים אלה, למשל בעזרת חבל פשוט אפשר לשרטט ישרים ולחוג מעגלים, לכן שני כלים אלה נגישים לכל אחד ואחד והם קלים מאד להפעלה, אך בכל זאת אפשר לפתור בעזרתם בעיות מורכבות מאד וברמות שונות של עומק ומחשבה, ולכן האסתטיקה שנמצאת בתוך השימוש בשני כלים אלה יחד עם היכולת הגדולה שטמונה בתוכם לפתרון בעיות מורכבות הוא זה מה שמשך ועניין את היוונים לחקור בניות בעזרת סרגל ומחוגה.

המתמטיקאים ביוון העתיקה שהתחילו בבניות בעזרת סרגל ומחוגה גילו איך לבצע חיבור, חיסור, כפל, חילוק והוצאת שורש ריבועי בעזרת שני כלים אלה בלבד. הם הצליחו גם לחצות זווית לשניים, לבנות ריבוע ששטחו כפול משטח ריבוע נתון, לבנות מצולע משוכלל עם 3, 4, 5 צלעות, אך היו בניות שהיוונים לא הצליחו לבצע כאשר המפורסמות מהם היו

i. ריבוע העיגול : הבעיה היא לבנות ריבוע ששטחו שווה לשטח מעגל נתון.

החשיבות של בניה כזו קשורה לשיטת השוואת השטחים שהייתה נהוגה בימי היוונים, כי אז, כדי למצוא את היחס בין שני שטחים היו מרבעים אותם קודם , כלומר בונים שני ריבועים ששטח כל אחד מהם שווה לאחד השטחים הנתונים, ומחשבים את היחס בין שטחי שני הריבועים ,ורק כך יכלו למצוא את היחס בין שני השטחים המקוריים, ולכן ריבוע המעגל היה נחוץ מאד ליוונים כדי להרחיב את שיטת ההשוואה גם למעגלים, הם הצליחו למצוא שיטות איך לרבע משולשים ומצולעים שונים , אך ריבוע המעגל העסיק המתמטיקאים לאורך כל התקופה היוונית, והם המשיכו לחקור אותה ובכך תרמו רבות להתפתחות וצמיחה מהותית של הגיאומטריה.

בעיה זו נשארה פתוחה במשך 2000 שנה, והוצעו כל כך הרבה פתרונות לבעיה שהתגלו כשגויים, עד שבשנת 1775 החליטה האקדמיה הצרפתית למדעים שלא לבדוק פתרונות חדשים לבעיה זו, ורק לאחר פיתוח תורת השדות וההוכחה שהמספר π הוא טרנסנדנטי היה אפשר להראות שבעיה זו אינה פתירה.

ii. הכפלת נפח קובייה: הבעיה היא לבנות קובייה שנפחה כפול מנפח קובייה נתונה. המקורות המיתולוגיים לבעיה זו נמצאים בסיפור הזה : בסוף המאה החמישית לפני הספירה פרצה מגפה באתונה, פריקלס עצמו - שהיה מדינאי רטוריקן ואיש צבא בולט בתקופה בה הגיעה אתונה לשיא כוחה - נפטר במגפה בשנת 429 לפני הספירה יחד עם רבע מתושבי אתונה. התושבים המודאגים פנו בבקשת עזרה למגדת העתידות האוראקל, שנמצאת במקדשו של האל אפולו וביקשו ממנה איך ניתן לעצור את המגפה. והיא ענתה להם שיש לבנות לאפולו מזבח חדש שיהיה כפול מהמזבח הקיים שהיה בצורת קובייה, ואז התושבים בנו מזבח חדש בצורת קובייה שאורך צלעו כפול מאורך צלע המזבח הישן, אך זה כמובן לא גרם לעצירת המגיפה כי המזבח החדש נפחו היה גדול פי 8 מנפח המזבח הישן, ומאז ידועה בעיית הכפלת הקובייה.

iii. חלוקת זווית נתונה לשלוש זוויות שוות: הבעיה היא, בהינתן זווית מסוימת איך לחלק אותה לשלוש זוויות שוות, היוונים הצליחו לחלק זוויות ספציפיות לשלוש זוויות שוות, אך ניסו למצוא דרך שמתאימה לכל זווית.

כאמור, שלושת הבעיות האלו לא נפתרו ע"י היוונים באמצעות סרגל ומחוגה בלבד אך הם חשבו שהפתרון קיים, ולכן המשיכו בחיפוש אחרי הפתרון, וניסיונות חוזרים ונשנים להתרתן גרמו להתקדמות והעשרת המתמטיקה. עד שהוכח במאה התשע עשרה שהן בעיות לא

פתירות באמצעות סרגל ומחוגה תוך שימוש בכלים אלגבריים שפיתח אותם המתמטיקאי גאוס למטרת חקירת שדות והרחבותיהם, אותם כלים שהשתמש בהם pierre wantzel בשנת 1837 כדי להראות שאי אפשר למצוא פתרון לבעיות אלו באמצעות סרגל ומחוגה בלבד.

יש לציין שהיוונים עצמם הצליחו לפתור בעיות אלה אבל תוך שימוש בעקומות מסדר גבוה, חתכי חרוט כגון אליפסות ופרבולות ושימוש בכלים מכנים , חקר בעיות אלה גרם לעיון בחתכים הקוניים ולהמצאת עקומות אחרות, שמטרתן הייתה לפתור את הבעיות הקלאסיות שהעסיקו את היוונים.

פרק 1 - הרחבת שדות

אחד המבנים האלגבריים החשובים במתמטיקה הוא השדה, שנתמקד בו בעבודה זו ובפרט בהרחבת שדות, ההתמקדות הזו ולמידת אפיונם של הרחבות כאלה , תספק לנו תשובה נחרצת לבעיות הבניה הקלאסיות באמצעות סרגל ומחוגה שנרחיב עליהם בהמשך.

שדות

הגדרה של שדה : קבוצה $\mathbb{F}$ נקראת שדה אם מוגדרות עליה שתי פעולות שנקרא להן כפל וחיבור ונסמן אותן ב- $(+,\cdot)$ כך שקבוצה $\mathbb{F}$ סגורה תחת פעולות אלו , כלומר

$$\forall\, x,y \in \mathbb{F} \Longrightarrow \begin{cases} x \cdot y \in \mathbb{F} \\ x + y \in \mathbb{F} \end{cases}$$

והקבוצה $\mathbb{F}$ מקיימת את התכונות הבאות : $\forall\, x,y,z \in \mathbb{F}$ מתקיים

i. חוק החילוף : $\begin{cases} x + y = y + x \\ x \cdot y = y \cdot x \end{cases}$

ii. חוק הצירוף : $\begin{cases} (x + y) + z = x + (y + z) \\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \end{cases}$

iii. חוק הפילוג : $(x + y) \cdot z = x \cdot z + y \cdot z$

iv. קיום איבר ניטראלי ביחס לפעולת החיבור : קיים איבר ב- $\mathbb{F}$ שנסמן אותו ב- 0 שמקיים $\forall\, x \in \mathbb{F} \;:\; x + 0 = 0 + x = x$

v. קיום איבר נגדי ביחס לפעולת החיבור : $\forall\, x \in \mathbb{F}$ קיים איבר ב- $\mathbb{F}$ שנסמן אותו $-x$ כך שמתקיים : $x + (-x) = (-x) + x = 0$

vi. קיום איבר ניטראלי ביחס לפעולת הכפל : קיים איבר ב- $\mathbb{F}$ שנסמן אותו ב- 1 ששונה מהאיבר הניטראלי של השדה ביחס לפעולת החיבור $(1 \neq 0)$ שמקיים : $\forall\, x \in \mathbb{F} \;:\; x \cdot 1 = 1 \cdot x = x$

vii. קיום איבר הופכי ביחס לפעולת הכפל : $\forall\, x \in \mathbb{F}$ ששונה מהאיבר הניטראלי קיים איבר ב- $\mathbb{F}$ שנסמן אותו x^{-1} שמקיים : $x \cdot x^{-1} = x^{-1} \cdot x = 1$

<u>הרחבת שדות</u>

אם F ו- K שדות כך ש- $\mathrm{F} \subset \mathrm{K}$ נאמר ש K הוא שדה הרחבה של F.

דוגמא : $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ שדות ומתקיים $\mathbb{Q} \subset \mathbb{R}$ לכן $\mathbb{R}$ הוא שדה הרחבה של $\mathbb{Q}$, ו- $\mathbb{C}$ הוא שדה הרחבה של $\mathbb{R}$ כי $\mathbb{R} \subset \mathbb{C}$

אם L, F שדות כך ש- $\mathrm{F} \subset \mathrm{L}$ *הרחבת שדות,* ו- X קבוצה לא ריקה $X \subset L$

<u>נסמן ב F(X)</u> את השדה הקטן ביותר שמכיל *את* F *ואת* X , לכן F(X) הוא שדה הרחבה של F כי מתקיים $\mathrm{F} \subset \mathrm{F}(X)$

<u>הגדרה</u> : אם הקבוצה X מכילה רק איבר יחיד $\mathrm{X} = \{\alpha\}$ אז מתקיים $\mathrm{F} \subset \mathrm{F}(\alpha)$ ונאמר שההרחבה $\mathrm{F}(\alpha)$ היא הרחבה פשוטה של F.

<u>הגדרה</u> : איבר a נקרא איבר אלגברי מעל שדה F אם קיים פולינום $0 \not\equiv p(x) \in F[x]$ כך ש- $p(a) = 0$ ($F[x]$ מציין את חוג הפולינומים עם מקדמים מתוך השדה F)

<u>הגדרה</u> : הרחבה פשוטה $\mathrm{F} \subset \mathrm{F}(\alpha)$ נקראת הרחבה אלגברית אם האיבר α אלגברי מעל השדה F

<u>דוגמא</u>

נסתכל על הקבוצה : $\mathrm{A} = \{a + b\sqrt{2} \mid \mathrm{a,b} \in \mathbb{Q}\}$, קבוצה זו מקיימת את כל האקסיומות של שדה , הוכחה :

נשים לב כי מתקיים $\mathrm{A} \subset \mathbb{R}$ ובשדה המספרים הממשיים מתקיימים חוקי החילוף , הצירוף והפילוג , ולכן הם מתקיימים בהכרח בקבוצה A .

קבוצה A סגורה תחת פעולת החיבור והכפל : ניקח שני איברים כלשהם מתוך הקבוצה

$$\{a + b\sqrt{2} \ , c + d\sqrt{2} \mid \mathrm{a,b,c,d} \in \mathbb{Q}\}$$

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = \underbrace{(a + c) + (b + d)\sqrt{2}}_{a+c\,,b+d\in\mathbb{Q}} \in A$$

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = \underbrace{(ac + 2bd) + (ad + bc)\sqrt{2}}_{ac+2bd\,,ad+bc\in\mathbb{Q}} \in A$$

האיבר הניטראלי ביחס לחיבור בקבוצה A הוא $0 = 0 + 0\sqrt{2}$ ואיבר היחידה הוא $1 = 1 + 0\sqrt{2}$

קיום איבר נגדי : $(a + b\sqrt{2}) + ((-a) + (-b)\sqrt{2}) = 0$

קיום הופכי לכל איבר ששונה מאפס (a, b שניהם שונים מאפס) : נשים לב כי מתקיים

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

ואם a,b שני מספרים ששונים מאפס אז בהכרח $a^2-2b^2\neq 0$ כי אחרת נקבל סתירה , $\sqrt{2}=\frac{a}{b}\in\mathbb{Q}$

ולכן נוכל לחלק ב- a^2-2b^2 ונקבל : $\left(a+b\sqrt{2}\right)\cdot\left(\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\right)=1$

וברור שהאיבר ההופכי שייך לקבוצה A כי $\frac{a}{a^2-2b^2}\,,\frac{b}{a^2-2b^2}\in\mathbb{Q}$

לכן קיבלנו שקבוצה A היא שדה, וברור שהיא מכילה את שדה המספרים הרציונאליים , לכן השדה A הוא הרחבה של $\mathbb{Q}$, $\mathbb{Q}\subset A$, את השדה A הוא בעצם השדה $\mathbb{Q}(\sqrt{2})$ כי הוא השדה המינימאלי שמכיל $\mathbb{Q}$ ואת $\sqrt{2}$ (בהמשך נסביר יותר את המבנה של שדה הרחבה, מה שיבהיר יותר למה מתקיים $A\equiv\mathbb{Q}(\sqrt{2})$)

$A\equiv\mathbb{Q}(\sqrt{2})$ היא הרחבה אלגברית פשוטה של שדה המספרים הרציונאליים , כי היא הרחבה של שדה המספרים הרציונאלים באמצעות איבר יחיד $\sqrt{2}$ שהוא שורש של הפולינום $p(x)\in\mathbb{Q}[x]\,,\,p(x)=x^2-2$

<u>הגדרה</u> : איבר a נקרא איבר טרנסצנדנטי מעל שדה F אם לכל $p(x)\in F[x]$ מתקיים $p(a)\neq 0$

<u>הגדרה</u> : הרחבה פשוטה $F\subset F(\alpha)$ נקראת הרחבה טרנסצנדנטית אם α איבר טרנסצנדנטי מעל F

<u>הפולינום המינימאלי</u>

הגדרה : $p(x)\in F[x]$ הוא הפולינום המינימאלי של איבר אלגברי a מעל שדה F אם הוא פולינום מתוקן בעל דרגה מינימאלית כך ש- $p(a)=0$

<u>תכונות הפולינום המינימאלי</u>

i. **<u>טענה 1.1</u> – הפולינום המינימאלי הוא פולינום יחיד**

הוכחה : יהי a איבר אלגברי מעל שדה F ויהי $p_1(x),p_2(x)\in F[x]$ שני פולינומים מינימאליים שונים של a מעל F אז הפולינום $q(x)=p_1(x)-p_2(x)\in F[x]$ ומתקיים $q(a)=p_1(a)-p_2(a)\Rightarrow q(a)=0-0=0$, ומכיוון ששני הפולינומים $p_1(x),p_2(x)$ הם שני פולינומים מתוקנים בעלי דרגה שווה- כי אחרת לא שניהם פולינומים מינימאליים של a - אז בהכרח הדרגה של $q(x)$ היא יותר קטנה מזו של שניהם , ואם הפולינום $q(x)$ נכפול בהופכי של המקדם של החזקה הגבוהה ביותר ב $q(x)$ נקבל פולינום מתוקן בעל דרגה יותר נמוכה מזו של $p_1(x),p_2(x)$ ש a הוא

שורש שלו בסתירה לכך ש $p_1(x), p_2(x)$ הם פולינומים מתוקנים בעלי דרגה מינימאלית שמקימים $p_1(a) = p_2(a) = 0$

ii. **<u>טענה 1.2</u> - הפולינום המינימאלי הוא פולינום אי פריק**

הוכחה : נניח בשלילה שהפולינום $p(x)$ הוא פולינום פריק מעל השדה F לכן קיימים שני פולינומים $q(x), r(x) \in F[x]$

כך ש- $p(x) = q(x) \cdot r(x) \implies p(a) = q(a) \cdot r(a) \implies 0 = q(a) \cdot p(a)$

ולכן $q(a) = 0$ או $r(a) = 0$ ובהכרח מתקיים שהדרגה של שני הפולינומים $q(x), r(x)$ יותר קטנה מהדרגה של $p(x)$, בסתירה לכך שהפולינום $p(x)$ הוא בעל דרגה מינימאלית ש- a הוא שורש שלו

iii. **<u>טענה 1.3</u> - אם $h(x)$ הוא פולינום שמקיים $h(a) = 0$ אז בהכרח $p(x)|h(x)$**

הוכחה : נניח בשלילה כי $p(x) \nmid h(x)$ לכן קיימים שני פולינומים $q(x), r(x) \in F[x]$

כך ש $h(x) = p(x) \cdot q(x) + r(x)$ ומתקיים $\deg r(x) < \deg p(x)$ ואם נציב $x = a$ נקבל $h(a) = p(a) \cdot q(a) + r(a) \implies 0 = 0 \cdot q(a) + r(a) \implies$

$r(a) = 0$ בסתירה לכך שהפולינום $p(x)$ הוא בעל דרגה מינימאלית ש- a הוא שורש שלו

<u>טענה 1.4</u> - אם $p(x) \in F[x]$ הוא פולינום מתוקן ואי פריק מעל השדה F שמקיים $p(a) = 0$ אז בהכרח פולינום זה הוא הפולינום המינימאלי של a מעל השדה F ,

הוכחה : אם $q(x) \neq p(x) \ni F[x]$ הוא הפולינום המינימאלי של a מעל השדה F אז לפי **טענה 1.3** מתקיים $q(x)|p(x)$ בסתירה לכך ש- $p(x)$ הוא פולינום אי פריק .

<u>טענה 1.5</u>: יהי K תת שדה של המספרים המרוכבים , ויהי $p(x) \in K[x]$ פולינום מתוקן אי פריק , אזי קימת הרחבה $K \subset K(\alpha)$ כך ש- $p(x)$ הוא הפולינום המינימאלי של α מעל K .

הוכחה :

יהי $p(x) \in K[x]$ פולינום מתוקן ואי פריק , לפי המשפט היסודי של האלגברה לפולינום $p(x)$ קיים שורש α בשדה המספרים המרוכבים $\mathbb{C}$, $p(\alpha) = 0$, וכיוון ש- $p(x)$ הוא פולינום מתוקן ואי פריק , אז לפי **טענה 1.4** הוא הפולינום המינימלי של α מעל השדה K.

הערה : הטענה נכונה גם לשדה כללי

אם K הוא שדה כלשהו , $p(x) \in K[x]$ פולינום אי פריק , אז קיימת הרחבה $K \subset L$ כך ש- $p(x)$ הוא הפולינום המינימלי של הרחבה זו

תמצית ההוכחה : יהי הפולינום $p(x)$ מדרגה $n + 1$, נגדיר

$$L = \{a_0 + a_1 x + \cdots \ldots + a_n x^n \mid a_i \in K\}$$

נגדיר חיבור ב – L כחיבור רגיל בין שני פולינומים , ונגדיר כפל ב – L באמצעות $f * g = f \cdot g \ (mod\ p)$ כאשר $f \cdot g$ הוא כפל רגיל של פולינומים , קל להראות ש- L *הוא* חוג ושמתקיים $p(x) = 0$, ותוך שימוש בעובדה ש- $p(x)$ הוא אי פריק ניתן להראות ש- L הוא שדה .

<u>המימד של הרחבת שדות</u>

אם F ו- K שדות כך ש- $F \subset K$, ניתן לראות את השדה K כמרחב וקטורי מעל השדה F ואז אפשר לחשב את המימד של K כמרחב וקטורי מעל השדה F

<u>הגדרה</u>

תהי $F \subset K$ הרחבת שדות , דרגת ההרחבה $F \subset K$ שתסומן $[K: F]$ היא המימד של K כמרחב וקטורי מעל השדה F

<u>טענה 1.6</u>

יהי K, F, L שדות כך שמתקיים $K \subset F \subset L$ הרחבת שדות אזי

$$[L: K] = [L: F] \cdot [F: K]$$

<u>הוכחה</u>

נניח $[L: F] = m$ אז קיימים m איברים $\{x_1, x_2, x_3, \dots \dots . x_m\} \in L$ שמהווים בסיס ל- L כמרחב וקטורי מעל F , ולכן לכל $a \in L$ קיימים m סקלרים $\{\alpha_1, \alpha_2, \alpha_3, \dots ., \alpha_m\} \in F$ כך שמתקיים $a = \sum_{i=1}^{i=m} \alpha_i \cdot x_i$

נניח $[F: K] = n$ אז קיימים n איברים $\{y_1, y_2, y_3, \dots \dots ., y_n\} \in F$ שמהווים בסיס ל- F כמרחב וקטורי מעל K , לכן לכל $\{\alpha_i\}_{i=1}^{i=m} \ni F$ קיימים n סקלרים

$\{\beta_{i1}, \beta_{i2}, \beta_{i3}, \dots ., \beta_{in}\} \in K$ כך שמתקיים $\alpha_i = \sum_{j=1}^{j=n} \beta_{ij} \cdot y_j$

לכן לכל $a \in L$ מתקיים $a = \sum_{i=1}^{i=m} \sum_{j=1}^{j=n} \beta_{ij} \cdot y_j \cdot x_i$

ובכך הראינו שהקבוצה $\{x_i \cdot y_i\}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ שמכילה $m \cdot n$ איברים היא קבוצה פורשת של השדה L כמרחב וקטורי מעל השדה K

נותר להראות שזו קבוצה בלתי תלויה מעל K , ובכן צריך להראות שאם

$0 = \sum_{i=1}^{i=m} \sum_{j=1}^{j=n} \beta_{ij} \cdot y_j \cdot x_i$ אז $\beta_{ij} = 0$ לכל $1 \le i \le m, 1 \le j \le n$

כיוון ש- $\{x_1, x_2, x_3, \dots \dots . x_m\}$ מהווים בסיס ל- L כמרחב וקטורי מעל F ומתקיים $0 = \sum_{i=1}^{i=m} (\sum_{j=1}^{j=n} \beta_{ij} \cdot y_j) \cdot x_i$ ו- $(\sum_{j=1}^{j=n} \beta_{ij} \cdot y_j)$ הם איברים מתוך F אז בהכרח מתקיים $\sum_{j=1}^{j=n} \beta_{ij} \cdot y_j = 0$ לכל $1 \le i \le m$ כי הקבוצה $\{x_1, x_2, x_3, \dots \dots . x_m\}$ היא בלתי תלויה.

הקבוצה $\{y_1, y_2, y_3, \dots \dots ., y_n\} \in F$ היא בסיס לשדה F כמרחב וקטורי מעל K

ולכן אם מתקיים $\sum_{j=1}^{j=n} \beta_{ij} \cdot y_j = 0$, עבור $\beta_{ij} \in K$ אז בהכרח $\beta_{ij} = 0$ לכל $1 \le i \le m, 1 \le j \le n$ כי הקבוצה $\{y_1, y_2, y_3, \dots\dots, y_n\} \in F$ בלתי תלויה מעל K.

לכן בסך הכל קיבלנו שהקבוצה $\{x_i \cdot y_i\}_{\substack{1\le i\le m \\ 1\le j\le n}}$ שמכילה $m \cdot n$ איברים היא בסיס לשדה L כמרחב וקטורי מעל K

ומתקיים $[L:K] = m \cdot n = [L:F] \cdot [F:K]$

<u>מסקנה 1.7</u> אם $K_0 \subset K_1 \subset K_2 \subset \cdots\cdots \subset K_n$ סדרה של הרחבות שדה אז באינדוקציה ולפי טענה 1.6 מתקיים

$$[K_n:K_0] = [K_n:K_{n-1}] \cdots\cdots [K_1:K_0]$$

<u>טענה 1.8</u>

אם $K \subset K(\alpha)$ היא הרחבה אלגברית פשוטה , $m(x) \in K[x]$ הוא הפולינום המינימאלי של α מעל K , ומתקיים $\deg m(x) = n$ אז האיברים $\{1, \alpha, \alpha^2, \alpha^3, \dots\dots, \alpha^{n-1}\}$ מהווים קבוצה בלתי תלויה מעל K

<u>הוכחה</u> :

נניח בשלילה שהקבוצה $\{1, \alpha, \alpha^2, \alpha^3, \dots\dots, \alpha^{n-1}\}$ היא תלויה , לכן קיימים סקלרים $\{\beta_0, \beta_1, , , , , , \beta_{n-1}\} \in K$ לא כולם איבר האפס כך שמתקיים $0 = \sum_{i=0}^{i=n-1} \beta_i \alpha^i$

לכן אם נסתכל על הפולינום $K[x] \ni p(x) = \sum_{i=0}^{i=n-1} \beta_i x^i$ הוא פולינום שמקיים $p(\alpha) = 0$ ו- $\deg p(x) < \deg m(x)$ בסתירה לכך ש- $m(x)$ הוא הפולינום בעל הדרגה המינימאלית שמקיים $m(\alpha) = 0$

<u>טענה 1.9</u>

אם $K \subset K(\alpha)$ היא הרחבה אלגברית פשוטה , $m(x) \in K[x]$ הוא הפולינום המינימאלי של α מעל K , ומתקיים $\deg m(x) = n$ אז האיברים $\{1, \alpha, \alpha^2, \alpha^3, \dots\dots, \alpha^{n-1}\}$ מהווים קבוצה פורשת של $K(\alpha)$ כמרחב וקטורי מעל השדה K , ולכל $\beta \in K(\alpha)$ קיימת הצגה יחידה $\beta = p(\alpha)$ כאשר $p(x) \in K[x]$ ו- $degp(x) \le n-1$

<u>הוכחה :</u>

נסתכל על הקבוצה

$$A=\left\{\frac{f(\alpha)}{g(\alpha)}\ \middle|\ f(x),g(x)\in K[x],g(\alpha)\neq 0\right\}$$

קבוצה זו סגורה לחיבור וכפל כי אם $\frac{f_1(\alpha)}{g_1(\alpha)},\frac{f_2(\alpha)}{g_2(\alpha)}\in A$, $g_1(\alpha),g_2(\alpha)$ שונים מאפס אזי

$$\frac{f_1(\alpha)}{g_1(\alpha)}+\frac{f_2(\alpha)}{g_2(\alpha)}=\frac{f_1(\alpha)\cdot g_2(\alpha)+f_2(\alpha)\cdot g_1(\alpha)}{g_1(\alpha)\cdot g_2(\alpha)}\in A$$

$$\frac{f_1(\alpha)}{g_1(\alpha)}\cdot\frac{f_2(\alpha)}{g_2(\alpha)}=\frac{f_1(\alpha)\cdot f_2(\alpha)}{g_1(\alpha)\cdot g_2(\alpha)}\in A$$

קבוצה זו מכילה גם את איבר האפס ואיבר היחידה $0=\frac{0}{1},1=\frac{1}{1}$

לכל $\frac{f(\alpha)}{g(\alpha)}\in A$ גם הנגדי $\frac{-f(\alpha)}{g(\alpha)}\ni A$

לכל $\frac{f(\alpha)}{g(\alpha)}\neq 0\in A$ גם ההופכי $\frac{g(\alpha)}{f(\alpha)}\in A$ כי $f(\alpha)\neq 0$ בגלל ש- $\frac{f(\alpha)}{g(\alpha)}\neq 0$.

נשים לב כי $f(x),g(x)\in K[x]\ \Leftarrow\ f(\alpha),g(\alpha)\in K(\alpha)$ שהיינו שדה ולכן גם

$\frac{f(\alpha)}{g(\alpha)}=f(\alpha)\cdot g(\alpha)^{-1}$ שייך לשדה $K(\alpha)$, ולכן הקבוצה A בהכרח מקיימת את חוק החילוף , חוק הצירוף וחוק הפילוג כי חוקים אלה מתקיימים בשדה $K(\alpha)$ והקבוצה A מוכלת באותו שדה .

הקבוצה A מקיימת את כל התכונות של שדה ולכן מצד אחד היא שדה שמוכל בתוך השדה $K(\alpha)$ ומצד שני היא מכילה את כל האיברים מתוך K ואת האיבר α כי אם ניקח

$\alpha=\frac{f(\alpha)}{g(\alpha)}\in A$ נקבל $f(x)=x,g(x)=1$ ולכל $\beta\in K$ $\beta=\frac{f(\beta)}{g(\beta)}\in A$ מתקיים

לכן קיבלנו $K\subseteq A\subseteq K(\alpha)$ ומכיוון ש- $K(\alpha)$ הוא השדה המינימאלי שמכיל את K ואת α אז בהכרח $K(\alpha)=A$

הפולינום המינימאלי $m(x)$ הוא פולינום מתוקן אי פריק , לכן $\gcd\big(m(x),g(x)\big)=m(x)$ או $\gcd\big(m(x),g(x)\big)=1$ אם מתקיים $\gcd\big(m(x),g(x)\big)=m(x)$ אז קיים $q(x)\in K[x]$ כש ש- $g(x)=q(x)\cdot m(x)\ \Leftarrow\ g(\alpha)=q(\alpha)\cdot m(\alpha)=0$

כי $m(\alpha)=0$ בסתירה לכך ש- $g(\alpha)\neq 0$, ולכן בהכרח מתקיים $\gcd\big(m(x),g(x)\big)=1$

לפי אלגוריתם אוקלידיס קיימים $r(x),s(x)\in K[x]$ כך שמתקיים

$$1=r(x)\cdot m(x)+s(x)\cdot g(x)$$

ואם נציב $x=\alpha$ נקבל : $1=r(\alpha)\cdot m(\alpha)+s(\alpha)\cdot g(\alpha)$ וכיוון ש- $m(\alpha)=0$ נקבל

$$s(\alpha)=\frac{1}{g(\alpha)}\quad\Leftarrow\quad p(x)\in K[x]\ :\ \frac{f(\alpha)}{g(\alpha)}=f(\alpha)\cdot s(\alpha)=p(\alpha)$$

ובכך מצאנו שכל איבר $\beta \ni A = K(\alpha)$ ניתן לייצג אותו בצורה $\beta = p(\alpha)$ כאשר $p(x) \in K[x]$

נראה שלכל $\beta \ni A = K(\alpha)$ אפשר למצוא $p(x) \in K[x]$ כך ש- $degp(x) \leq n-1$ ומתקיים $p(\alpha) = \beta$

הוכחנו שכל איבר $\beta \ni A = K(\alpha)$ ניתן לייצג אותו בצורה $\beta = p(\alpha)$ כאשר $p(x) \in K[x]$, אם $degp(x) \leq n-1$ סיימנו , אחרת לפי אלגוריתם החלוקה של אוקלידס קיימים $h(x), r(x) \in K[x]$ כך ש- $p(x) = h(x) \cdot m(x) + r(x)$ ומתקיים $\deg r(x) < \deg m(x) \Leftarrow \deg r(x) \leq n-1$. ואם נציב $x = \alpha$ נקבל $p(\alpha) = h(\alpha) \cdot m(\alpha) + r(\alpha) \Leftarrow \beta = p(\alpha) = r(\alpha)$ כי $m(\alpha) = 0$,סיימנו.

נותר להראות יחידות הצגה , נניח כי $\beta = p(\alpha)$ וגם $\beta = q(\alpha)$ כאשר $p(x), q(x) \in K[x]$ הם שני פולינומים שונים מדרגה קטנה מ- n אז נקבל $\beta - \beta = p(\alpha) - q(\alpha)$

$\Leftarrow 0 = p(\alpha) - q(\alpha)$, ובכך קיבלנו פולינום $d(x) = p(x) - q(x) \in K[x]$ שמקיים $d(\alpha) = 0$ ו- $\deg d(x) < \deg m(x)$ בסתירה לכך ש- $m(x)$ הוא הפולינום בעל הדרגה המינימאלית ש- α הוא שורש שלו . לכן ההצגה של β היא יחידה .

<u>טענה 1.10</u>

אם $K \subset K(\alpha)$ היא הרחבה אלגברית פשוטה , $m(x) \in K[x]$ הוא הפולינום המינימאלי של α מעל K , ומתקיים $\deg m(x) = n$ אז $[K(\alpha):k] = n$

<u>הוכחה :</u>

לפי **טענות 1.9 + 1.8** הקבוצה $\{1, \alpha, \alpha^2, \alpha^3, \ldots\ldots, \alpha^{n-1}\}$ שמכילה בדיוק n איברים היא קבוצה בלתי תלויה ופורשת את $K(\alpha)$ כמרחב וקטורי מעל K לכן היא מהווה בסיס ל - $K(\alpha)$ כמרחב וקטורי מעל K $\Leftarrow$ $[K(\alpha):K] = \deg m(x) = n$.

<u>דוגמא</u>

$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ כי הפולינום המינימאלי של $\sqrt{2}$ מעל השדה $\mathbb{Q}$ הוא $m(x) = x^2 - 2$ כי זהו פולינום אי פריק מעל $\mathbb{Q}$ ו- $\sqrt{2}$ הוא שורש שלו , לכן $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = \deg m(x) = 2$ כאשר הקבוצה $\{1, \sqrt{2}\}$ מהווים בסיס לשדה $\mathbb{Q}(\sqrt{2})$, ולכן כל איבר β שנמצא בתוך $\mathbb{Q}(\sqrt{2})$ ניתן לייצג אותו בצורה $\beta = a \cdot 1 + b \cdot \sqrt{2}$, $a, b \in \mathbb{Q}$

<u>טענה 1.11</u>

אם α הוא איבר טרנסצנדנטי מעל שדה K אז מתקיים $[K(\alpha):K] = \infty$

<u>הוכחה</u>

לכל n טבעי קבוצת האיברים $\{1, \alpha^1, \alpha^2, \alpha^3, , , , , , \alpha^n\}$ היא בלתי תלויה מעל K, כי אחרת היה קיים פולינום $p(x) \in K[x]$ מדרגה לכל היותר n שמקיים $p(\alpha) = 0$ בסתירה לכך ש-α הוא איבר טרנסצנדנטי

לכן לכל n טבעי יש קבוצה בתוך $K(\alpha)$ שמכילה n איברים בלתי תלוים , ולכן ב-$K(\alpha)$ יש אינסוף איברים בלתי תלויים מעל K ולכן $[K(\alpha):K] = \infty$.

<u>טענה 1.12</u>

α הוא איבר אלגברי מעל השדה K אם ורק אם הדרגה של ההרחבה $[K(\alpha):K]$ היא סופית

<u>הוכחה :</u>

אם α הוא איבר אלגברי מעל הדשה K , אז המימד של ההרחבה שווה לדרגת הפולינום המינימאלי של α מעל K , ולכן דרגת ההרחבה סופית .

אם הדרגה של ההרחבה היא n אז האיברים $1 , \alpha , \alpha^2, \ldots\ldots, \alpha^n$ הם איברים תלוים מעל השדה K , ולכן α הוא שורש של פולינום מעל K שדרגתו לכל היותר n

בהמשך נזדקק לכלי מסוים שבעזרתו יהיה אפשר להוכיח שפולינום מסוים הוא אי פריק , הכלי הזה הוא :

<u>טענה 1.13 – קריטריון אייזנשטיין</u>

פולינום $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots \ldots . + a_1 x + a_0$ בעל מקדמים שלמים מקיים את תנאי אייזנשטיין אם קיים מספר ראשוני p כך ש-

i. p מחלק את a_i לכל $0 \leq i < n$

ii. p לא מחלק את a_n

iii. p^2 לא מחלק את a_0

פולינום המקיים תנאי אייזנשטיין לא ניתן לפירוק מעל המספרים הרציונאליים

פרק 2 - בניות בעזרת סרגל ומחוגה

בניה בעזרת סרגל ומחוגה היא בניה גיאומטרית של עצם מסוים, תוך שימוש רק בסרגל ומחוגה שיש להם תכונות מסוימות

הסרגל הוא כלי שבעזרתו אפשר לשרטט קו ישר בין שתי נקודות נתונות והוא אינו מכויל ואינו בעל יכולת מדידה

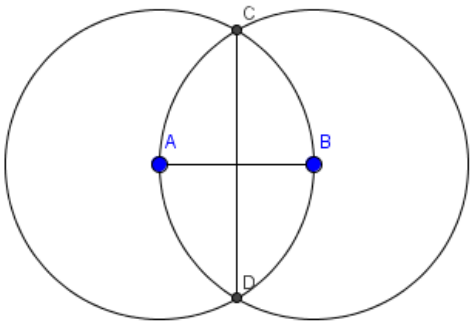
המחוגה הגיאומטרית היא כלי שבעזרתו ניתן לשרטט מעגל אם נתון המרכז שלו ונקודה עליו .

במצב ההתחלתי תהיה נתונה קבוצה p_0 של נקודות במישור, וכל נקודה שנוצרת ע"י חיתוך בין שני ישרים, ישר ומעגל, שני מעגלים שאפשר לשרטט אותם מתוך הקבוצה p_0 לפי התנאים לשימוש בסרגל ומחוגה, היא נקודה במישור שניתנת לבניה, ואפשר להשתמש בה לצורך בניית נקודות אחרות.

<u>הגדרה</u>: כל עצם שניתן לבנות אותו תוך מספר סופי של שימושים בסרגל ומחוגה נקרא לו עצם ניתן לבניה.

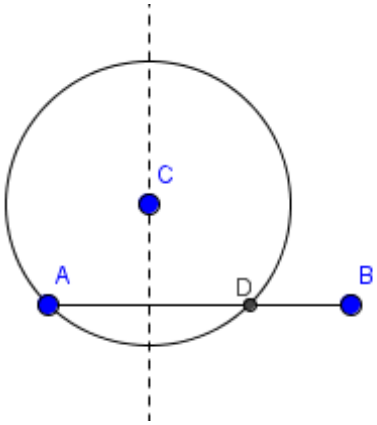
דוגמאות לבניות בסיסיות (בניות אלה חשובות בפרקים הבאים)

<u>בניה 1 - בניית אנך אמצעי לקטע</u>: אם נתון קטע ישר *AB*, משרטטים שני מעגלים, שהמעגל הראשון מרכזו הקצה הראשון של הקטע(*A*) ועובר בקצה השני (*B*), והמעגל השני מרכזו הקצה השני (*B*) ועובר בקצה הראשון (*A*) , והאנך האמצעי לקטע הוא בעצם הישר שמחבר בין שתי נקודות החיתוך בין שני המעגלים ⇐ *CD* הוא האנך האמצעי לקטע *AB*



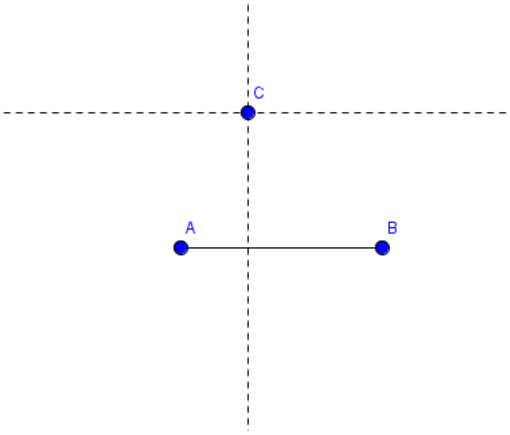
<u>בניה 2 - בניית אנך לקטע נתון דרך נקודה נתונה שנמצאת על הקטע או מחוצה לו</u>

אם נתון קטע ישר *AB* , ונקודה כלשהי *C*, נשרטט מעגל שמרכזו הנקודה הנתונה *C*, ועובר בנקודה *A*, מעגל זה חותך את הקטע AB (או את המשכו) בנקודה D, האנך האמצעי (לפי בניה 1) לקטע AD הוא האנך הנדרש.



<u>בניה 3 - בניית מקביל לקטע נתון העובר דרך נקודה מחוץ לקטע</u>

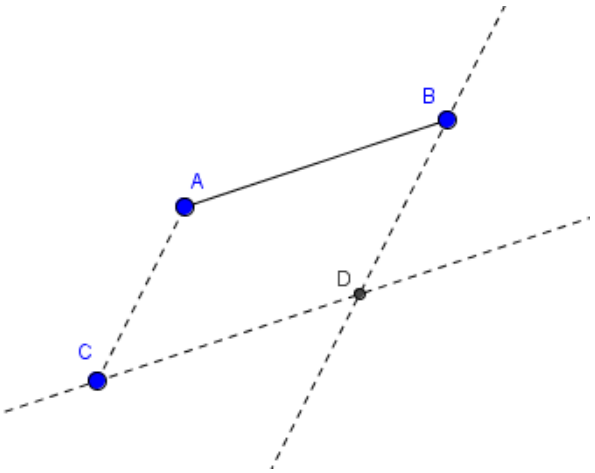
אם נתון קטע *AB* , ונקודה *C* שלא נמצאת עליו, מנקודה *C* מורידים אנך לקטע (לפי בניה 2), ועל האנך שנוצר בונים ישר שמאונך לו ועובר דרך הנקודה *C* (לפי בניה 2) , ובכך קיבלנו ישר המקביל לקטע *AB* ועובר דרך הנקודה *C*,



<u>בניה 4 - העתקת קטע</u>

אם נתון קטע *AB* ונקודה *C*, אפשר לבנות קטע שמתחיל בנקודה *C* ומקביל לקטע *AB* ואורכו שווה לאורך הקטע *AB*

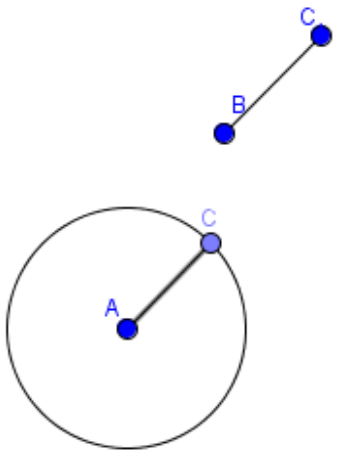
נחבר את הנקודה *A* עם הנקודה *C* , מנקודה *C* נעביר מקביל לקטע *AB* (לפי בניה 3), ומנקודה *B* נעביר קטע מקביל לקטע *AC* (לפי בניה 3), שני המקבילים שהעברנו נחתכים בנקודה *D* , ונקבל שהקטע *CD* יוצא מנקודה *C* ומקביל לקטע *AB* ואורכו שווה לאורך הקטע *AB*.



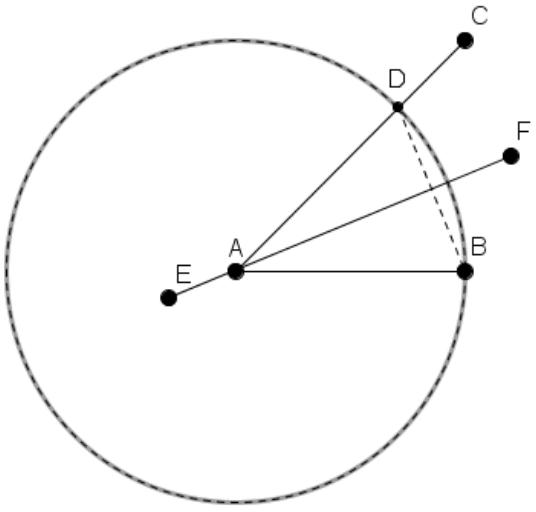
<u>בניה 5 - בניית מעגל עם מרכז ואורך רדיוס נתון</u>

כפי שציינו המחוגה שלנו מאפשרת לבנות מעגל דרך מרכז ונקודה על המעגל , אלא מסתבר שניתן לבנות גם מעגל אם נתון המרכז שלו ואורך הרדיוס שלו.

אם נתונה נקודה *A* ורוצים לבנות מעגל שמרכזו בנקודה זו ורדיוסו שווה לאורך הקטע *BC*, מעתיקים את הקטע *BC* לנקודה *A* (לפי בניה 4) ואז נשרטט מעגל שמרכזו *A* ועובר דרך נקודה *C* המועתקת.

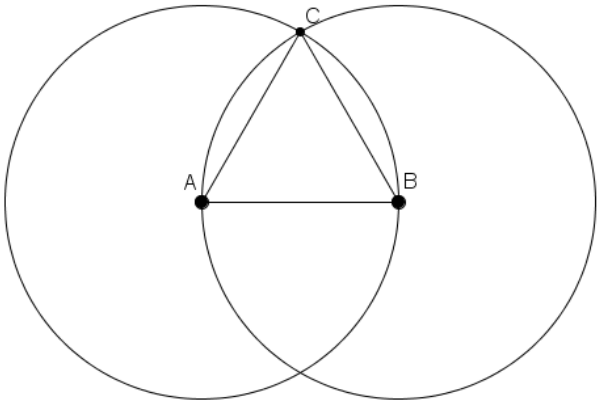


<u>בניה 6 - חציית זווית</u> אם נתון שני קטעים AB , AC ורוצים לחצות את הזויות שביניהם, נבנה מעגל שמרכזו בנקודה A ועובר בנקודה B , מעגל זה חותך את הקטע AC בנקודה *D* (או את המשכו), נחבר הקטע DB , ונבנה את האנך האמצעי לקטע זה, אנך זה חוצה את הזוית CAB כי המשולש ADB שווה שוקיים.



בניה 7 - בניה של זווית 60^0

בהינתן שתי נקודות A , B נשרטט מעגל שמרכזו בנקודה A ועובר בנקודה B , נשרטט מעגל שני שמרכזו בנקודה B ועובר בנקודה A , תהי C אחת נקודות החיתוך של שני המעגלים , אז המשולש ABC שווה צלעות ולכן זוויותיו שוות ל- 60^0



בניית מספרים ונקודות במערכת צירים

הגדרה: מספר ממשי m ניתן לבניה בעזרת סרגל ומחוגה אם אפשר לבנות קטע שאורכו שווה ל- $|m|$.

טענה 2.1 :

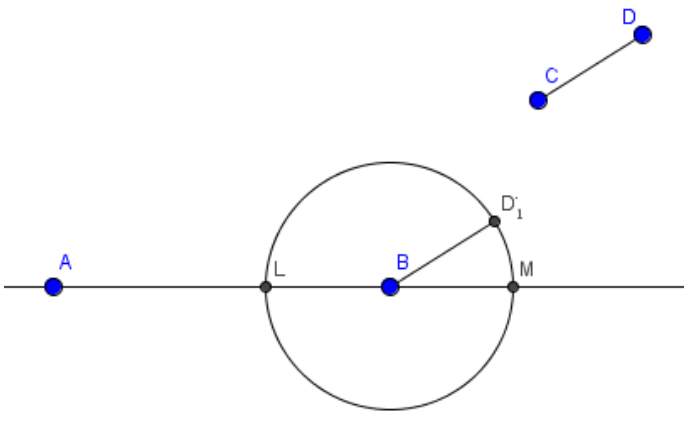
בהינתן שני קטעים באורכים a , b וקטע נוסף באורך יחידה ניתן לבנות בעזרת סרגל ומחוגה את פעולות החשבון הבסיסיות : חיבור , חיסור , כפל , חלוקה ושורש ריבועי

הוכחה :

אם נתון שני קטעים AB , CD כך שאורך AB שווה ל- a ואורך CD שווה ל- b אז ניתן לבנות את הפעולות הבאות בעזרת סרגל ומחוגה

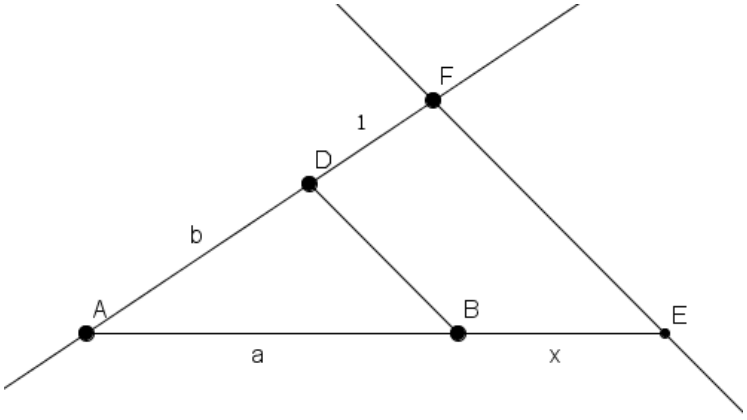
$$a+b\,,a-b\,,a\cdot b\,,\frac{a}{b}\,,\sqrt{a}$$

חיבור וחיסור : נבנה מעגל שמרכזו בנקודה B ורדיוסו שווה לאורך CD לפי בניה 5 , נשרטט את הישר שעובר דרך שתי



הנקודות A,B שחותך את המעגל בשתי הנקודות L , M ונקבל $\mathrm{AM} = a + b$ ו- $\mathrm{AL} = a -$ b

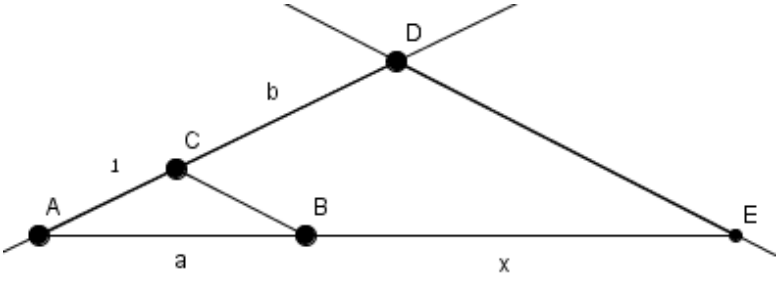
<u>חילוק</u>: נעתיק את הקטע *CD* (לפי בניה 4) כך שיתחיל בנקודה *A* (*CD* מועתק ל- *AD* בשרטוט) ונחבר את הקטע *DB* , נשרטט את הישר *AD* , בהינתן קטע שאורכו יחידת אורך אחת ,נבנה מעגל שמרכזו בנקודה *D* ורדיוסו 1 (לפי בניה 5) , F היא נקודת החיתוך של מעגל זה עם הישר *AD* , מנקודה F נעביר ישר מקביל לקטע *DB* (לפי בניה 3), שיחתוך את הישר *AB* בנקודה *E* , הקטע *BE* נסמן אותו ב- x , ולפי משפט תלס יתקיים



$$\frac{\mathrm{x}}{\mathrm{a}} = \frac{1}{\mathrm{b}} \Longrightarrow x = \frac{a}{b}$$

<u>כפל</u> **:** נעתיק את קטע היחידה שיתחיל מנקודה *A* (לפי בניה 4) ונקבל את הקטע *AC* באורך יחידה , נשרטט מעגל שמרכזו בנקודה *C* ורדיוסו b (לפי בניה 5) , *D* היא נקודת החיתוך של מעגל זה עם הישר *AC* , מנקודה *D* נשרטט ישר המקביל לקטע *CB* (לפי בניה 3) מקביל זה חותך את הישר *AB* בנקודה *E* , נסמן *BE=x* , ולפי משפט תלס יתקיים

$$\frac{\mathrm{x}}{\mathrm{a}} = \frac{\mathrm{b}}{1} \Longrightarrow x = ab$$



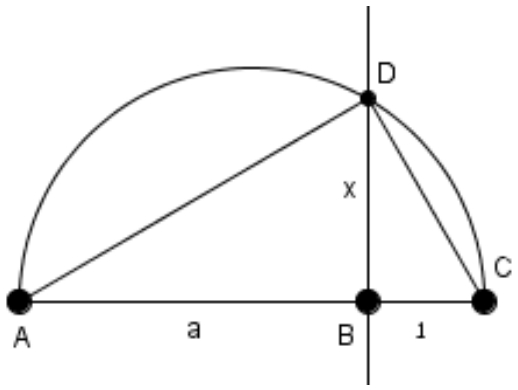
<u>הוצאת שורש ריבועי למספר ממשי חיובי</u> :בהינתן קטע באורך יחידה, נבנה את הקטע AC שאורכו שווה ל- a+1 (חיבור הקטע AB עם קטע היחידה , כפי שהסברנו בחיבור), נמצא את נקודת האמצע של הקטע AC (נקודת החיתוך של האנך האמצעי לקטע AC עם הקטע

עצמו, לפי בניה 1), נשרטט מעגל שמרכזו אמצע הקטע AC ועובר דרך הנקודה A , מנקודה B נעלה אנך לקטע AC (לפי בניה 2) שחותך את המעגל בנקודה D,

המשולש ADC הוא משולש ישר זווית כי זווית היקפית שנשענת על קוטר המעגל היא זווית ישרה,

לפי משפט בגיאומטריה אוקלידית : הגובה ליתר במשולש ישר זווית הוא הממוצע הגיאומטרי של היטלי שני הניצבים על היתר, נקבל

$$DB^2 = \mathrm{AB} \cdot \mathrm{BC} \Longrightarrow \mathrm{x}^2 = a \cdot 1 \Longrightarrow x = \sqrt{a}$$



<u>טענה 2.2</u> : בהינתן שתי הנקודות $(0,0), (1,0)$ אפשר לבנות את כל המספרים הרציונאלים $\mathbb{Q}$

הוכחה : אם נתונות שתי נקודות שאורך הקטע שמחבר ביניהם שווה ליחידת אורך אחת , ו- n הוא מספר שלם כלשהו , אז ניתן לחבר קטע היחידה לעצמו $|n|$ פעמים לקבל קטע באורך $|n|$, ובכך בנינו את המספר n

אם רוצים לבנות מספר רציונאלי $\frac{n}{\mathrm{m}}$ כלשהו , אז נבנה את שני המספרים n, m ואחר כך נחלק אותם כפי שהסברנו קודם ונקבל את המספר $\frac{n}{\mathrm{m}}$

<u>בנית מערכת צירים</u> : אם במצב ההתחלתי נתונות שתי נקודות A, B שהמרחק ביניהם שווה ליחידת אורך אחת , אז נעביר את הישר AB שיסמל ציר ה- *X*, ונעביר אנך לישר AB בנקודה A (לפי בניה 2) שיסמל את ציר ה-*Y*, ואז הנקודה A תסמל את הנקודה (0,0) והנקודה B תסמל את הנקודה (1,0)

<u>טענה 2.3</u> : בהינתן מערכת צירים ,נקודה במישור ניתנת לבניה אם ורק אם ניתן לבנות את שני המספרים שמייצגים את שיעורי הנקודה במישור

הוכחה : אם ניתן לבנות את שני המספרים $a\,,b$ אז לפי בניה 5 ניתן לבנות מעגל שמרכזו בנקודה $\mathrm{A}(0,0)$ ורדיוסו $|a|$, ונקודת החיתוך של המעגל עם ציר ה- X מסמלת את המספר a על ציר ה-X ,

(נבחר את הנקודה המתאימה מבין שתי נקודות החיתוך לפי הסימן של המספר a) מנקודה זו נעלה אנך לציר ה-X ,באותו אופן , נקודת החיתוך של המעגל שמרכזו בנקודה$\mathrm{A}(0,0)$ ורדיוסו $|b|$ עם ציר ה-Y מסמלת את המספר b על ציר ה- Y ומנקודה זו נעלה אנך לציר ה- Y , נקודת החיתוך של שני האנכים מסמלת את הנקודה $(a\,,b)$

אם נתונה הנקודה $(a\,,b)$ נוריד ממנה אנך לציר ה-X שחותך אותו בנקודה מסוימת, המרחק בין נקודה זו לבין הנקודה $\mathrm{A}(0,0)$ יהיה שווה ל- $|a|$ ובכך בנינו את המספר a, ובאותו אופן ניתן לבנות את המספר b.

<u>טענה 2.4</u> :

אם שיעורי נקודה במישור הם מספרים רציונאליים אז ניתן לבנות נקודה זו במישור בהינתן שתי הנקודות $(0,0)\,,\,(1\,,0)$

הוכחה לפי **טענה 2.2 וטענה 2.3**

<u>בנית מספר מרוכב</u> : מספר מרוכב ניתן לבניה אם ניתן לבנות את הנקודה שמסמלת את המספר במישור המרוכב .

<u>טענה 2.5</u> : אם נתון שני מספרים מרוכבים $\mathrm{Z}_2=(\mathrm{x}_2,\mathrm{y}_2)$, $\mathrm{Z}_1=(x_1,y_1)$, אז ניתן לבנות את $Z_1-Z_2\,,Z_1+Z_2\,,\frac{\mathrm{Z}_1}{\mathrm{Z}_2}\,,\mathrm{Z}_1\cdot\mathrm{Z}_2,\,\sqrt{Z_1}$,

<u>הוכחה</u>

לשם ביצוע פעולות אלה אנחנו צריכים לבצע פעולות חיבור , חיסור , כפל , חילוק על המספרים הממשיים $x_1,\mathrm{x}_2,\mathrm{y}_1,\mathrm{y}_2$, כי כפי שאנחנו יודעים מתקיים

$$\mathrm{Z}_1\cdot\mathrm{Z}_2=(x_1\cdot x_2-y_1\cdot y_2\ ,x_1\cdot y_2+x_2\cdot y_1)$$

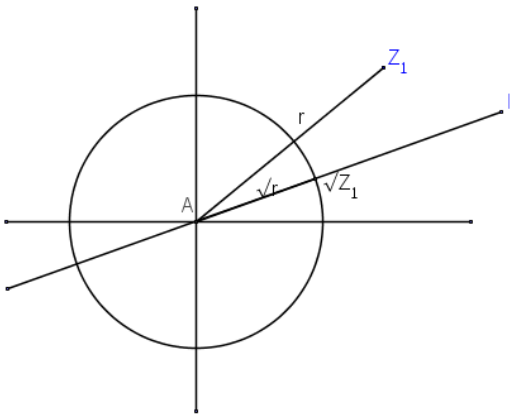
$$\frac{\mathrm{Z}_1}{\mathrm{Z}_2}=(\frac{\mathrm{x}_1\cdot\mathrm{x}_2+\mathrm{y}_1\cdot\mathrm{y}_2}{\mathrm{x}_2^2+\mathrm{y}_2^2}\,,\frac{\mathrm{x}_2\cdot\mathrm{y}_1-\mathrm{x}_1\cdot\mathrm{y}_2}{\mathrm{x}_2^2+\mathrm{y}_2^2})$$

$$\mathrm{Z}_1\odot\odot+Z_2=(x_1+x_2\,,y_1+y_2)$$

$$Z_1 - Z_2 = (x_1 - x_2, y_1 - y_2)$$

ולפי **טענה 2.1** אפשר לבצע כל הפעולות בצד ימין .

לגבי הוצאת שורש למספר מרוכב , אם $Z_1 = re^{i\theta}$ אז $\sqrt{Z_1} = \sqrt{r}e^{i\frac{\theta}{2}}$, נשים לב ש- r מספר ממשי חיובי , לכן ניתן לבצע לו שורש כפי שהוסבר קודם, לכן אפשר לבנות מעגל שמרכזו (0,0) ורדיוסו $\sqrt{r}$ (לפי בניה 5), נבנה את הקטע שחוצה את הזוית בין הכיוון החיובי לציר הממשי ובין הקטע שמחבר את הנקודה (x_1 , y_1) עם ראשית הצירים (לפי בניה 6), נקודת החיתוך בין המעגל לבין הקטע שחוצה את הזוית מסמלת את המספר $\sqrt{Z_1}$ במישור המרוכב.



<u>מסקנה 2.6</u> : נגדיר סדרה של קבוצות מספרים באופן הבא :

$$F_1 = \mathbb{Q}$$

$$F_n = \{a + b\sqrt{c} \mid \ a , b , c \in F_{n-1}\}$$

נשים לב שלכל n מתקיים $F_{n-1} \subset F_n$

וכל המספרים שנמצאים בתוך סדרת הקבוצות האלה ניתנים לבנייה , למשל

$$x = 1 + \sqrt{\sqrt{1 + 3\sqrt{2}}}$$

$$x = \sqrt{19} + (3 - \frac{7}{5}\sqrt{11}) \sqrt{\sqrt{\sqrt{2 - \sqrt{21}}}}$$

$$x = (2 - i) + (2 + 4i)\sqrt{5 - 3i}$$

פרק 3 - הניסוח האלגברי של בניה בעזרת סרגל ומחוגה

בפרק זה נוכיח את המשפט המרכזי שבעזרתו נוכיח ששלושת בעיות הבניה לא פתירות בעזרת סרגל ומחוגה, המשפט הוא : אם x הוא מספר שניתן לבניה באמצעות סרגל ומחוגה אז מתקיים : חזקה של $[\mathbb{Q}(x):\mathbb{Q}] = 2$

נניח שנתונה קבוצת נקודות במישור שנקרא לה p_0 , נגדיר שתי הפעולות הבאות

פעולת הסרגל : העבר ישר דרך שתי נקודות מהקבוצה p_0

פעולת המחוגה : שרטט מעגל שמרכזו באחת הנקודות מהקבוצה p_0 , ועובר דרך נקודה אחרת מתוך אותה קבוצה .

<u>הגדרה</u> : נקודה שנוצרת ע"י חיתוך שני ישרים , ישר ומעגל או שני מעגלים תוך שימוש בשתי הפעולות סרגל ומחוגה נקראת נקודה שנוצרת בצעד אחד מהקבוצה p_0 . ובאופן כללי, נקודה r במישור ניתנת לבניה מהקבוצה p_0 אם קיימת סדרה סופית של נקודות $\mathrm{r}_1, \mathrm{r}_2, \mathrm{r}_3, \ldots., \mathrm{r}_\mathrm{n} = r$

במישור , כך שלכל $j = 1, \ldots., n$ הנקודה r_j נבנית בצעד אחד מתוך הקבוצה

$$\mathrm{p}_0 \cup \{r_1, \ldots. \mathrm{r}_{\mathrm{j}-1}\}$$

אחת הדרכים להבנה מעמיקה של בניות בעזרת סרגל ומחוגה היא לקשור אותה לנושא הרחבת שדות , כך שבכל שלב משלבי הבניה נסתכל על המישור המינימאלי שמכיל את כל שיעורי הנקודות שנבנו עד כה .

ולכן , נסמן ב- K_0 את השדה המינימאלי שמכיל את שיעורי ה- *x* ושיעורי ה- *y* של הנקודות שנמצאות בתוך הקבוצה p_0 , ואם נקודה r_j יש לה את השיעורים (x_j, y_j) , אז השדה K_j הוא השדה המינימאלי שמכיל את השדה K_{j-1} ושני המספרים $\{x_j, \mathrm{y_j}\}$, כלומר

$$\mathrm{K_j} = \mathrm{K_{j-1}}(x_j, y_j)$$

<u>הערה</u> : לא מוסיפים את הנקודה (x_j, y_j) אלא את שני המספרים $\{\mathrm{x_j}, \mathrm{y_j}\}$

ובכך נקבל סדרה של הרחבת שדות :

$$K_0 \subseteq K_1 \subseteq \cdots\cdots \subseteq K_n$$

שנשתמש בה לצורך חקירת הבניות הגיאומטריות

<u>טענה 3.1:</u>

שני המספרים x_j , y_j שהזכרנו אותם קודם , כל אחד מהם הוא שורש ב- K_j לפולינום מעל K_{j-1} ממעלה ראשונה או שנייה

<u>הוכחה :</u>

הנקודה (x_j , y_j) יכולה להיווצר בשלושה מצבים שונים , חיתוך בין שני ישרים , חיתוך בין מעגל וישר, חיתוך בין שני מעגלים

<u>מקרה ראשון : חיתוך בין שני ישרים</u>

יהיה $A(p , q) , B(r , s), C(t , u), D(m , n)$ ארבע נקודות שהשיעורים שלהם נמצאים במישור K_{j-1} , הישר AB משוואתו : $\frac{y-q}{x-p} = \frac{s-q}{r-q}$ והישר CD משוואתו :

$$\frac{y-u}{x-t} = \frac{n-u}{m-t}$$

נשים לב כי שני המספרים $\frac{n-u}{m-t}$, $\frac{s-q}{r-q}$ שייכים לשדה K_{j-1} כי השדה סגור לפעולות החיבור (חיסור) והכפל (חילוק) . נסמן שני מספרים אלה ב- z , e בהתאמה .

ממשוואת הישר AB נקבל : $y = z(x-p)+q$, וממשוואת הישר CD נקבל : $y = e(x-t)+u$

לכן קיבלנו : $e(x-t)+u = z(x-p)+q$

$$(e-z)x - et + u + zp - q = 0$$

ובכן קיבלנו x_j הוא שורש של הפולינום:

$$h(x) \in K_{j-1}[x] , \qquad h(x) = (e-z)x - et + u + zp - q$$

באותו אופן נראה ש- y_j הוא גם כן שורש של פולינום ממעלה ראשונה ששיך ל- $K_{j-1}[x]$

<u>מקרה שני : חיתוך בין ישר ומעגל</u>

לפי הסימנים הקודמים קיבלנו שמשוואת הישר AB היא $y = z(x-p)+q$

משוואת המעגל שמרכזו בנקודה C ועובר דרך הנקודה D היא :

$$(x-t)^2+(y-u)^2=(t-m)^2+(u-n)^2$$

נשים לב שאגף ימין במשוואת המעגל הוא מספר ששיך לשדה K_{j-1} , כי שדה סגור לחיבור (חיסור) וכפל , נסמן מספר זה ב- v , נקבל שתי המשואות :

$$y = z(x-p)+q \quad \text{.i}$$
$$(x-t)^2+(y-u)^2=v \quad \text{.ii}$$

משתיהן נקבל : $(x-t)^2+(zx-zp+q-u)^2-v=0$

ובכך קיבלנו ש- x_j הוא שורש של הפולינום הריבועי :

$$h(x)=(x-t)^2+(zx-zp+q-u)^2$$

וכמובן מתקיים $h(x) \in K_{j-1}[x]$

באותו אופן ניתן להראות שגם y_j הוא שורש של פולינום ריבועי ששייך לחוג הפולינומים $K_{j-1}[x]$

<u>מקרה שלישי : חיתוך בין שני מעגלים</u>

משוואת המעגל שמרכזו בנקודה A ועובר בנקודה B היא :

$$(x-p)^2+(y-q)^2=(r-p)^2+(s-q)^2$$

נשים לב שאגף ימין זה בעצם מספר ששיך לשדה K_{j-1} , כי שדה זה סגור לפעולות החיבור (חיסור) והכפל , נסמן מספר זה ב- a , ונקבל שמשוואת המעגל היא

$$(x-p)^2+(y-q)^2=a$$

משוואת המעגל שמרכזו בנקודה C ועובר דרך הנקודה D היא (לפי סימנים במקרה השני)

$$(x-t)^2+(y-u)^2=v$$

מחיסור שתי המשוואות נקבל :

$$x\underbrace{(2t-2p)}_{b}+y\underbrace{(2y-2q)}_{n}+\underbrace{(p^2+q^2-t^2-u^2-a+v)}_{m}=0$$

נשים לב , כי שלושת הביטויים $b\ ,n,m$ הם מספרים ששיכים לשדה $K_{\mathrm{j}-1}$, כי שדה סגור לפעולות החיבור והכפל .

ממשוואה אחרונה נקבל : $y=\frac{-m-bx}{n}$, ואחרי ההצבה במשוואת המעגל שמרכזו A נקבל

$$(x-p)^2+\left(\frac{-m-bx}{n}-q\right)-v=0$$

ובכך קיבלנו ש- x_j הוא שורש של פולינום ריבועי :

$$,\ h(x)=(x-p)^2+\left(\frac{-m-bx}{n}-q\right)-v$$

שזהו פולינום ששיך לחוג הפולינומים $\mathrm{K}_{\mathrm{j}-1}[x]$

באותו אופן נראה ש- y_j הוא גם כן שורש של פולינום ריבועי מעל חוג הפולינומים $\mathrm{K}_{\mathrm{j}-1}[x]$.

אם בהרחבת שדה מסוים מצרפים שורשים של פולינום ריבועי או פולינום לינארי , נקבל הרחבה שהיא מדרגה 1 או 2 , בבניות גיאומטריות חוזרים על פעולה זו מספר סופי של פעמים, מה שנותן לנו ראיה אלגברית לבניית נקודה מסוימת .

<u>משפט 3.2 :</u>

אם הנקודה $r=(x\ ,y\ )$ ניתנת לבניה מתוך קבוצת נקודות p_0 , והשדה k_0 הוא השדה המינימאלי שמכיל את שיעורי הנקודות מתוך הקבוצה p_0 , אז הדרגות

$$[K_0(y):K_0]=2^n\ \ ,\ \ [K_0(x):K_0]=2^n$$ עבור *n* טבעי

הוכחה :

לפי **טענה 1.10** מתקיים $\left[K_{j-1}(x_j):K_{j-1}\right]=\deg m(x)$ כאשר $m(x)$ הוא הפולינום המינימאלי של x_j מעל $\mathrm{K}_{\mathrm{j}-1}$, ולפי **טענה 3.1** $\deg m(x)=1\ ,2$, הדרגה 2 מתקבלת כאשר הפולינום הריבועי מעל $K_{\mathrm{j}-1}$ ש- x_j הוא שורש שלו הוא פולינום אי פריק , ואחרת נקבל הדרגה 1 .

ובאותו אופן נקבל : $\left[K_{j-1}(y_j): K_{j-1}\right] = 1$ או 2

ולפי **טענה 1.6** מתקיים

$$\left[\underbrace{K_{j-1}(x_j\,, y_j)}_{K_j} : K_{j-1}\right] = \underbrace{\left[\underbrace{K_{j-1}(x_j\,, y_j)}_{K_j} : K_{j-1}(x_j)\right]}_{1} \cdot \left[K_{j-1}(x_j): K_{j-1}\right] = 1 \text{ או } 2$$

נשים לב שמתקיים : $\mathrm{K_{j-1}}(x_j\,, y_j) = \mathrm{K_{j-1}}(\mathrm{x_j})$ כי הנקודה $(x_j\,, y_j)$ בין אם היא נוצרת ע"י חיתוך בין שני ישרים , ישר ומעגל או שני מעגלים , y_j הוא שורש של פולינום מדרגה 1 ששיך לחוג הפולינומים $\mathrm{K_{j-1}}(x_j)[x]$,ניתן לראות את הפולינום בהוכחת **טענה 3.1** כאשר במקרה של :

חיתוך בין שני ישרים או ישר ומעגל : קיבלנו בשני המקרים את המשוואה

$$y = z(x - p) + q$$

חיתוך בין שני מעגלים : קיבלנו את המשוואה : $xb + yn + m = 0$

כאשר $\mathrm{K_{j-1}}(x_j\,, y_j) = K_{j-1}(x_j) \Leftarrow \mathrm{y_j} \in K_{j-1}(x_j) \Leftarrow z, p, q, b, n, m \in K_{j-1} \in K_{j-1}(x)$

$[K_{j-1}(x_j, y_j): K_{j-1}(x_j)]$=1 $\Leftarrow$

ובכן קיבלנו :

$$\left[K_j: K_{j-1}\right] = 1 \text{ או } 2$$

ולפי **מסקנה 1.7** מתקיים :

. $[K_n : K_0] = 2^N$, טבעי N

ושוב לפי **טענה 1.6** מתקיים

$$[K_n: K_0] = [K_n: K_0(x)] \cdot [K_0(x): K_0]$$

ובגלל שצד שמאל הוא חזקה של 2 (חזקה של מספר ראשוני) נקבל שגם

$$[K_0(x): K_0] = 2^n \text{ , טבעי } n$$

באותו אופן נראה ש- $[K_0(y): K_0] = 2^n$, טבעי n

פרק 4 - פתרון הבעיות הגיאומטריות

ניישם את מה שלמדנו עד כה, כדי להראות שלא ניתן לפתור את שלוש בעיות הבניה הקלאסיות בעזרת סרגל ומחוגה.

משפט 4.1

לא ניתן בעזרת סרגל ומחוגה להכפיל את הנפח של קובייה נתונה

הוכחה

נניח שנתונה קובייה מסוימת שאורך הצלע שלה שווה ליחידת אורך אחת , ונניח ש-

$p_0 = \{(0,0),(1,0)\}$ לכן לפי **טענה 2.2** נקבל ש- $K_0 = \mathbb{Q}$, המרחקים בין קודקודי הקובייה הם $1 , \sqrt{2} , \sqrt{3}$ שכולם ניתנים לבניה מתוך $\mathbb{Q}$ לפי **טענה 2.1** , על מנת להכפיל את נפח הקוביה יש לבנות את הנקודה $(\sqrt[3]{2} , 0)$, ולכן לפי **משפט 3.2**

$$\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right] = 2^n \text{ , טבעי } n$$

אבל $\sqrt[3]{2}$ הוא שורש של הפולינום $m(x) = x^3 - 2$ מעל $\mathbb{Q}$ שהוא פולינום אי פריק לפי **קריטריון איזנשטין** ,מקיים קריטריון אייזנשטיין עם המספר הראשוני 2 , ולכן לפי **טענה 1.4** $m(x)$ הוא הפולינום המינימלי של $\sqrt[3]{2}$ מעל $\mathbb{Q}$, ולכן לפי **טענה 1.10**

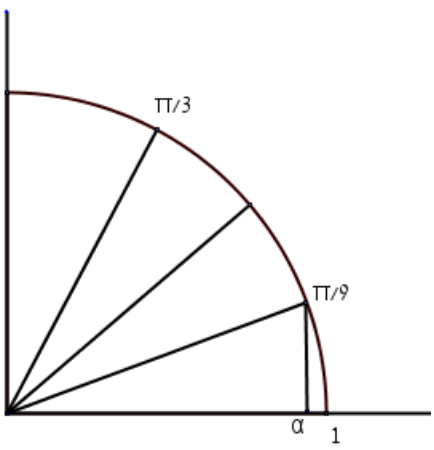
$$\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right] = 3$$

ומכיוון ש- 3 איננו חזקה של 2 אפשר להסיק לפי **משפט 3.2** שלא ניתן להכפיל את נפח הקובייה .

נוכיח עכשיו שלא ניתן לחלק זווית לשלוש זוויות שוות באמצעות סרגל ומחוגה , לזוויות מסוימות כן אפשרי כמו $\pi/2$, ז , אבל לא לכולם

משפט 4.2

לא ניתן באמצעות סרגל ומחוגה לחלק את הזווית $\pi/3$ לשלוש זוויות שוות



<u>הוכחה</u>

אם מתחילים מקבוצת הנקודות $p_0 = \{(0,0),(1,0)\}$, קל לבנות הזווית $\pi/3$ לפי **בניה 7**.

חילוק הזווית $\pi/3$ לשלוש זוויות שוות שקול לפי **טענה 2.3** להתחיל מקבוצת הנקודות $p_0 = \{(0,0),(1,0)\}$ ולבנות את הנקודה $(\alpha, 0)$ כאשר $\alpha = \cos(\pi/9)$, ומהנקודה $(\alpha, 0)$ אפשר לבנות את הנקודה $(\beta, 0)$ כאשר $\beta = 2\alpha$.

לפי נוסחת דה מואבר מתקיים

$$(cos\phi + isin\phi)^3 = cos3\phi + isin3\phi$$

מהשוואת החלקים הממשיים בשני האגפים נקבל

$$\cos^3\phi - 3\sin^2\phi cos\phi = cos3\phi$$

$$\cos^3\phi - 3(1-\cos^2\phi)cos\phi = cos3\phi$$

$$4cos^3\phi - 3cos\phi = cos3\phi$$

נציב $\phi = \pi/9$ ונקבל $4\cos^3(\pi/9) - 3\cos(\pi/9) = 0.5$

$$8\cos^3(\pi/9) - 6\cos(\pi/9) - 1 = 0$$

$$(2\cos(\pi/9))^3 - 3(2\cos(\pi/9)) - 1 = 0$$

$$\beta^3 - 3\beta - 1 = 0$$

ובכך קיבלנו ש- β היא שורש של הפולינום $m(x) = x^3 - 3x - 1$ מעל $\mathbb{Q}$

אם נציב $x = u + 1$ נקבל $m(x) = m(u+1) = u^3 + 3u^2 - 3$, שזהו פולינום אי פריק לפי קריטריון איזנשטיין – מקיים קריטריון אייזנשטיין עם המספר הראשוני 3 , לכן לפי **טענה 1.4 וטענה 1.10**

$$[\mathbb{Q}(\beta):\mathbb{Q}] = 3$$

ושוב 3 איננו חזקה של 2 בסתירה **למשפט 3.2** לכן אי אפשר לבנות β .

משפט 4.3

לא ניתן לרבע את המעגל באמצעות סרגל ומחוגה בלבד.

הוכחה

בניה כזו שקולה לבניית הנקודה $(\sqrt{\pi}\,,0)$ מקבוצת הנקודות ההתחלתית

$p_0=\{(0,0),(1,0)\}$, ואם זה אפשרי אז יהיה אפשרי לבנות את הנקודה $(\pi\,,0)$, וכן אם בניה כזו קיימת נקבל

$$[\mathbb{Q}(\pi):\mathbb{Q}]=2^n \text{ , טבעי } n$$

ולכן בפרט לפי **טענה 1.12** π הוא מספר אלגברי מעל $\mathbb{Q}$, בסתירה לכך ש- π הוא מספר טרנסצנדנטי מעל $\mathbb{Q}$.

<u>מקורות</u>

IAN STEWART , galios theory , third edition

- מבוא לתולדות המתמטיקה, חלק א', שבתאי אונגורו
- ויקיפדיה