2018 בנים אלגבריים - 80446 פתרון מבחן מועד ב' 2018

2025 ביולי



. המספרים ששדה אלגברית סגור אלגברית.

הוכחה: נזכר בשתי טענות:

- $\lim_{t \to \infty} f(t) = \infty, \lim_{t \to -\infty} f(t) = -\infty$ מדרגה אי־זוגית שורש ב- \mathbb{R} זה נובע ממשפט ערך הביניים: $f \in \mathbb{R}[t]$ מדרגה אי־זוגית שורש ב- \mathbb{R} מדרגה וובע ממשפט ערך הביניים: $f(t) = -\infty$ מדרגה אי־זוגית שורש.
 - שורש סגור להוצאת שורש \mathbb{C} מגור להוצאת

. אלגברית ולכן בל אלגברית הרחבה L/\mathbb{C} יש אלגברית ולכן בניח כעת, נניח שלא כך ולכן יש

ונגדיר בילית ולכן ניקח אספרבילית ולכן אי־פריק הוא שכל פולינום אי־פריק פולינום אי־פריק נובע שכל בובע $\operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{C}) = 0$ היות ונ $G = \operatorname{Gal}(L^{\operatorname{gal}}/\mathbb{R})$

 $F=\left(L^{
m gal}
ight)^H$ כאשר ביניים $H\leq G$ ניקח $H\leq G$ ניקח הסילו ולכן $\{e\}\leq H\leq G$ ניקח ולכן לכל אי־זוגי, שכן $\{e\}\in H$ אי־זוגי, שכן אי־זוגי, שכן $\{e\}\in H$ מספר אי־זוגי, זה מכיוון ש- $\{e\}\in H$ חבורת ביסילו ולכן לכל $\{e\}\in H$ מספר אי־זוגי, זה מכיוון ש-

$$\deg \! \left(f_{\alpha/\mathbb{R}} \right) = \left[\mathbb{R}(\alpha) : \mathbb{R} \right] \mid [F : \mathbb{R}]$$

לכל פולינום כזה יש שורש ב־R מהטענה הראשונה מתהזכורת ולכן יש ל- f_{lpha} שורש ב־R מהטענה הראשונה מתהזכורת ולכן יש ל-G שורש ב־R מהטענה הרחבה מסדר זוגי ולכן G ביש ולכן איז הרחבה מסדר זוגי ולכן איז הרחבה מסדר זוגי ולכן איז ווא הרחבה מסדר זוגי ולכן איז ווא הרחבה מסדר זוגי ווא הרחבה מסדר זוגי ווא מסדר זוגי ווא הרחבה מסדר זוגי ווא הרחבה מסדר זוגי ווא מסדר ז

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G \qquad \left(|G_i| = 2^i\right)$$

מהצד השני, מהתאמת גלואה קיבלנו

$$K_n \supset \cdots \supset K_2 \supset K_1 \supset \mathbb{R}$$
 $([K_i : K_{i-1}] = 2)$

נניח ש־n < 2וו סתירה כי אז נקבל ($\mathbb{C} \subset L^{\mathrm{gal}}$ כי n > 1 מתקיים (בהכרח מתקיים n < 2

$$\mathbb{R} \neq K_1 = \mathbb{R}(\sqrt{a})$$

 $n=1\Rightarrow$ הכרח לטענה השנייה מהתזכורת, אבל $C\neq K_2=\mathbb{C}ig(\sqrt{a+bi}ig)$ אבל אבל הכרח a<0 האכל בהכרח אבל $a\in\mathbb{R}$ אבל אבל הכרח בהכרח לכך ש־L לא טריוויאלית, כנדרש.

 $\mathbb{Z}[x]$ בוכיח שכל פולינום פרימיטיבי $\mathbb{Z}[x]$ שהוא אי־פריק ב־ $\mathbb{Z}[x]$ הוא גם אי־פריק ב-

הוכחה: נזכר בשתי הגדרות

היות של f להיות ($f(t)=\sum_{i=0}^n a_i t^i$ הזכורת: $f(t)\in\mathbb{Z}[t]$ עבור פולינום (תכולה) עבור $f(t)=\sum_{i=0}^n a_i t^i$

$$cont(f) = \gcd(a_0, a_1, ..., a_n)$$

 $\mathrm{cont}(f)=1$ אם פרימיטיבי אקר $f(t)\in\mathbb{Z}[t]$ פולינום פרימיטיבי: פולינום פרימיטיבי:

. ביטיבים פרימיטיבי אוא פולינום כאשר $f=\mathrm{cont}(f)\cdot f_0(t)$ בידי על־ידי פרימיטיבי פרימיטיבי לכל פולינום איש פירוק ב־ $\mathbb{Z}[t]$ הנתון על־ידי

וניזכר בלמת גאוס הראשונה:

. בפרט, fg פרימיטיבי אם ורק אם fg פרימיטיבי אם fg פרימיטיביים. בפרט, אזי אזי אזי אזי אזי אזי אזי אזי פרימיטיביים. אזי אזי אזי אזי אזי אזי אזי אזי פרימיטיביים. אזי אזי אזי אזי אזי אזי אזי אזי פרימיטיביים. :: מספיק להוכיח כי להוכיח ולכן ולכן היכות: $f \cdot g = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$ הוא פרימיטיבי מההערה לעיל מהפערה הוא ולכן היכות: הוא פרימיטיבי

נניח שלא ולכן קיים $f_0=\sum_{i=0}^n a_it^i, g_0=\sum_{j=0}^m b_jt^j$ אבל $p \mid \mathrm{cont}(f_0\cdot g_0)$ הם פרימטיביים (ולכן פרימטיביים (ולכן קיים $p \nmid b_m$ השתקיים ברן m,n מינימליים כך שר a_i,b_j ו־ $p \nmid a_n$ מתחלקים ברן ונכל לבחור m,n מינימליים כך שר a_i,b_j נסתכל על המקדם של $c=\sum_{k=0}^{m+n} a_kb_{m+n-k}$ של $c=\sum_{k=0}^{m+n} a_kb_{m+n-k}$

$$\underbrace{a_0b_{m+n}+\ldots+a_{n-1}b_{m+1}}_{\text{kn}}+\underbrace{a_{n+1}b_{m-1}+\ldots+a_{m+n}+b_0}_{\text{k}}$$

אבל סתירה סתירה $p \nmid c$ ולכן ב־p לחלוקה לחלוקה זר מ $a_n b_m$

נוכיח למה שהייתה חלק מלמת גאוס השנייה:

 $\mathbb{Z}[t]$ שדה השברים של " $\mathrm{Frac}(\mathbb{Z})$ הוא $\mathbb{Q}[t]$ הוא קבוע. למה 1.0 $f \in \mathbb{Z}[t]$ שדה השברים של

 $\mathbb{Z}[t]$ פירוק ב־ $f=(c\cdot g)\cdot (c^{-1}\cdot h)$ ולכן $c\cdot g,c^{-1}\cdot h\in \mathbb{Z}[t]$ כך ש־ $0
eq c\in \mathbb{Q}^{ imes}$ אזי קיים $\mathfrak{g}[t]$ אזי קיים $f=g\cdot h$ אם

 $m \cdot n \cdot f = m \cdot g \cdot m$ ואז נקבל פירוק $m \cdot g, n \cdot h \in \mathbb{Z}[t]$ כך שי $0 < m, n \in \mathbb{Z}$ וניקח וניקח $g, h \in \mathbb{Q}[t]$ עבור מלמת התכולה בפליות התכולה בכפליות מרום ב $\ell=\mathrm{cont}(f), \alpha=\mathrm{cont}(m\cdot g), \beta=\mathrm{cont}(n\cdot h)$ מלמת החולה מכולה בפליות התכולה

$$\mathrm{cont}(m\cdot n\cdot f)=m\cdot n\cdot \ell=\alpha\cdot \beta=\mathrm{cont}(m\cdot g\cdot n\cdot h)$$

 $f=\ellrac{m}{lpha}\cdot g\cdotrac{n}{eta}\cdot h$ משמע לה משמע לה היה ביק משמע לה בקל ונקבל אם הא הטענה שלנו: נניח כי $f=\ellrac{m}{lpha}\cdot g\cdotrac{n}{eta}\cdot h$ ונקבל להוכיח את הטענה שלנו: נניח כי $f=\ellrac{m}{lpha}\cdot g\cdotrac{n}{eta}\cdot h$ ונקבל להוכיח את הטענה שלנו: נניח כי $f=\ellrac{m}{lpha}\cdot g\cdotrac{n}{eta}\cdot h$ ולכן בי להוכיח את הטענה שלנו: נניח כי לאי־פריק בי $\mathbb{Z}[t]$ ולכן בי להוכיח את הטענה שלנו: נניח כי לאי־פריק בי $\mathbb{Z}[t]$

. הפיד הכים f פרימיטיבי $\operatorname{cont}(f)$

נניח ש־ $f = c \cdot g \cdot c^{-1} \cdot h$ עם ברגות אדולות מ־ $\deg(g), \deg(h) > 0$ עם דרגות דרגות וניח פריק ב־ $\mathbb{Q}[t]$ ולכן יש משמע הוא פריק בו, וזאת סתירה. $\mathbb{Z}[t]$

בכל סעיף נקבע האם הטענה נכונה או לא נכונה וננמק לספורט.

'סעיף א

 x^{-1} אוטומורפיזם של x^{-1} הנתונה על־ידי x^{-1} היא אוטומורפיזם של f:K o K אז ההעתקה

הוכחה: הטענה נכונה.

כדי להראות אוטומורפיזם עלינו להראות שזה הומומורפיזם, חד־חד ערכי ועל:

- מתקיים מחקיים בגלל שהשדה בגלל $f(x+y)=(x+y)^p=x^p+y^p$ אבל בגלל שהשדה פרפקטי מתקיים. 1

$$(x+y)^{\frac{1}{p}} = (x^p + y^p)^{\frac{1}{p}} \Longleftrightarrow (x+y)^{\frac{1}{p}} = \left(x^{\frac{1}{p}} + y^{\frac{1}{p}}\right)$$

$$f(x+y) = f(x) + f(y)$$
לכן

$$f(x+y)=f(x)+f(y)$$
 ולכן
$$f(xy)=(xy)^{\frac{1}{p}}=x^{\frac{1}{p}}y^{\frac{1}{p}}=f(x)f(y) \ .2$$

ייחודי p ייחודי שורש שורש לכל איבר השדה מושלם, לכל היות מסדר ייחודי כי מההנחה על היות השדה מושלם, לכל איבר יש

$$f(x) = f(y) \Longleftrightarrow x^{\frac{1}{p}} = y^{\frac{1}{p}} \Longleftrightarrow \left(x^{\frac{1}{p}}\right)^p = \left(y^{\frac{1}{p}}\right)^p \Longleftrightarrow x = y$$

 $f(x)=(z^p)^{rac{1}{p}}=z$ אז $x=z^p$ ונבחר $z\in K$ מיקח. 3

 $a\in\mathbb{F}_p$ אז זה אוטומורפיזם (הוא כמובן משמר גם את שדה הבסיס כי לכל $a\in\mathbb{F}_p$ מתקיים אז זה אוטומורפיזם (הוא כמובן משמר גם את שדה הבסיס

'סעיף ב

 $K\subset F\subset \overline{K}$ ו $K\subset L\subset \overline{K}$ שדות כך שדות K,L,F יהיו

.Gal(L/K)

הוכחה: הטענה נכונה.

ראינו אותה בהרצאה אבל אין לי מושג על מה מדובר.

'סעיף ג

pהרחבה עם על פרידה אי הרחבה יש $\mathbb{F}_p(t)$ לשדה לש

הוכחה: הטענה נכונה.

ניקח שכל שכל אומר $f'(x)=px^{p-1} \equiv 0$ (כי שונים שונים שורשים ובשדה p ובשדה p ובשדה פולינום אומר p וזה אומר p ווזה אומר p ובשדה p ווזה אומר p עם אומר p ווזה אומר p עם אומר שכל השורשים וויקם אומר שכל השורשים וויקם אומר שכל השורשים וויקם אומר שכל השורשים וויקם וויקם אומר שכל השורשים וויקם וויקם וויקם אומר שכל השורשים וויקם שלו כפולים, זאת־אומרת הפולינום אי־פריד).

אנח המינימלי שלה שלנו הפולינום שלנו הפולינום שלנו הבחבה את ההרחבה אז ניקח את שלנו יהיו שלנו הפולינום שלנו הפולינום שלנו המינימלי שלה או הארחבה $\mathbb{F}_p(lpha)$ p מדרגה מדרגה ולכן ההרחבה ולכן

'סעיף ד

כל הרחבות שדות סופית K/\mathbb{Q} היא גלואה.

הוכחה: הטענה לא נכונה.

ניקח $\sqrt[3]{2}$ זו הרחבה מדרגה 3 שאיננה נורמלית (ולכן בהכרח אינה גלואה) כי $\sqrt[3]{2}$ למרות שהשורש הזה צמוד ל $\sqrt[3]{2}$ ולכן ניקח $\sqrt[3]{2}$ ההרחבה לא מכילה את הפיצול של הפולינום ולכן לא נורמלית.

. נורמליות לא L/Kההרחבה כך F/K, L/Fוורמליות נבנה נבנה נבנה נבנה לא נורמליות

 $K=\mathbb{Q}, F=\mathbb{Q}\left(\sqrt{2}\right), L=\mathbb{Q}\left(\sqrt[4]{2}\right)$ בבחר: נבחר $K=\mathbb{Q}, F=\mathbb{Q}\left(\sqrt{2}\right), L=\mathbb{Q}\left(\sqrt[4]{2}\right)$ היא איננה נורמלית כי אנחנו כבר יודעים ש $F/K=\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ היא איננה נורמלית להפולינום המינימלי של ההרחבה הוא $K=\mathbb{Q}, F=\mathbb{Q}$ ולא כל השורשים נמצאים בהרחבה $K=\mathbb{Q}, F=\mathbb{Q}$ ולא כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים נמצאים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורשים בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית כל השורש בחוד בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית בחוד בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית בחוד בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית בחוד בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ הודמלית בחוד בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ היא נורמלית בחוד בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ הודמלית בחוד בחוד בחוד בהרחבה ($K=\mathbb{Q}, F=\mathbb{Q}$ הודמלית בחוד בחוד בחוד ב

נטען כעת שההרחבה $L/F=\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)$ היא נורמלית. בידיוק ההגדרה לנורמליות (כי הוא מתפצל לחלוטין $\mathbb{Q}(\sqrt{2})$ הוא אי־פריק מעל $\mathbb{Q}(\sqrt{2})$ ושורשיו הם $\mathbb{Q}(\sqrt{2})$ וזו בידיוק ההגדרה לנורמליות (כי הוא מתפצל לחלוטין עכשיו ב־L/F, ולכן ולכן ברחבה נורמלית. עכשיו

.7 מסדר פרימיטיבי חידה שורש אות ξ_7 כאשר כאשר השדות השדות השדות הדובת השדות האוא באנו נמצא נמצא הרחבת השדות הדובת האוא את בא

הוכחה: קודם כל

$$F_{11}^{\times} = \{1, \cdots, 10\} \cong C_{10}$$

אז אנחנו רוצים את החזקה המינימלית שבה נמצא את כל שורשי היחידה מסדר 7, וזה יקרה מתי שיתקיים 1 11^k-1 עכשיו $11 \mod 7=4$ אז אנחנו רוצים את החזקה של 4 שבמודלו 7 מביאה לנו 1 (כי אנחנו רוצים $(\xi_7 \in \langle \xi_{11^n-1} \rangle$

$$\underbrace{4^1=4 \operatorname{mod} 7}_{\mathbf{X}}, \underbrace{4^2=16 \operatorname{mod} 7=2}_{\mathbf{X}}, \underbrace{4^3=64 \operatorname{mod} 7=1}_{\mathbf{Y}}$$

6

. איננה נורמלית. $\mathbb{Q}\!\left(\sqrt{2}+\sqrt[3]{3}\right)\!/\mathbb{Q}$ השהרחבה נוכים, החיובים, החיובים הממשיים השורשים ל $\sqrt{2},\sqrt[3]{3}$

הוכחה: נסמן

$$\overline{\mathbb{Q}} = \{ \alpha \in \mathbb{C} \mid \mathbb{Q} \text{ מעל } \alpha \}$$

ניזכר ש־ $\overline{\mathbb{Q}}$ הרחבת שדות אלגברית, אז אלגברית, אז הרחבת שדות אלגברית, אז

$$\operatorname{Aut}\!\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) = \left\{\sigma \in \operatorname{Aut}\!\left(\overline{\mathbb{Q}}\right) \mid \forall x \in \mathbb{Q}, \sigma(x) = x\right\}$$

כך שמתקיים $\sigma\in \mathrm{Aut}ig(\overline{\mathbb{Q}}/\mathbb{Q}ig)$ שי ולכן יש $\sqrt{2},\sqrt[3]{3}\notin\mathbb{Q}$ וכמובן x^2-2,x^3-3 עבור הפולינומים עבור ואנחנו וודעים ש

$$\sigma\left(\sqrt{2}\right) = \pm\sqrt{2}, \sigma\left(\sqrt[3]{3}\right) = \sqrt[3]{3}\xi_3$$

אז בפרט הארחבה ועל־כן פרט ההרחבה ועל־כן פרט של אנמצא של $\sqrt{2}+\sqrt[3]{3}$ אות אומרת בהכרח יש לנו צמוד של $\sigmaig(\mathbb{Q}ig(\sqrt{2}+\sqrt[3]{3}ig)ig)
ightarrow\pm\sqrt{2}+\sqrt[3]{3}\xi_3$ איננה נורמלית.

 $\operatorname{Gal}(\mathbb{Q}(lpha)/\mathbb{Q})=\mathbb{Z}/5\mathbb{Z}$ ו גלואה הרחבת היא $\mathbb{Q}(lpha)/\mathbb{Q}$ כך כך שכע אלגברי מעל מצא מצא נמצא הרחבת היא

היה אלגברי (זה יהיה אלגברי מסדר בגודל המתאים אז $lpha=\xi_n$ כלשהו (זה יהיה אלגברי מסדר כלשהו שיתן לנו הרחבה בגודל המתאים אז מסדר (זה יהיה אלגברי מסדר מסדר שורש של הפולינום $lpha=\xi_n$).

ניזכר ש־

$$[\mathbb{Q}(\xi_n):\mathbb{Q}]=arphi_{\mathrm{Norm}}(n)=|\{k\mid 1\leq k\leq n,\gcd(k,n)=1\}|$$

 $.\varphi_{\mathrm{himit}}(5) = |\{1,2,3,4\}| = 4 \neq 5 = |\mathbb{Z}/5\mathbb{Z}|$ אבל חבא הוא הראשון הרא המועד המועד אבל

:אחר: באלימות כי אין לי רעיון

$$\mathbf{X} \varphi_{\mathsf{Normal}}(6) = |\{1,5\}| = 2 \neq 5 = |\mathbb{Z}/5\mathbb{Z}|$$

$$\mathbf{X}\varphi_{\gamma}$$
אניילר (7) = $|\{1, 2, 3, 4, 5, 6, 7\}| = 7 \neq 5 = |\mathbb{Z}/5\mathbb{Z}|$

$$\mathbf{X}\varphi_{\mathbf{x}}(9) = |\{1, 2, 4, 5, 7, 8\}| = 6 \neq 5 = |\mathbb{Z}/5\mathbb{Z}|$$

$$\mathbf{X} \varphi_{\text{think}}(10) = |\{1,3,7,9\}| = 4 \neq 5 = |\mathbb{Z}/5\mathbb{Z}| \mathbf{X} \varphi_{\text{think}}(11) = |\{1,2,3,4,5,6,7,8,9,10\}| = 10 \neq 5 = |\mathbb{Z}/5\mathbb{Z}|$$

אז אולי לא.

אנחנו חבורה ציקלית עם הבורה ביקלית שואלים עבור איזה n נקבל ש־ $\mathbb{Z}/n\mathbb{Z}$) הוא חבורה ציקלית עם סדר אנחנו רוצים למצוא הרחבת גלואה עם חבורת גלואה מסדר 5.

ואנחנו יודעים אנחנו קורה, $\operatorname{Gal}(\mathbb{Q}(\xi_{11})/\mathbb{Q})\cong\mathbb{Z}_{10}$ ואז $[\mathbb{Q}(\xi_{11}):\mathbb{Q}]=10$ ההרחבה על הסתכלים אלנו למעלה זה קורה כאשר מסתכלים אלה ההרחבה של ההרחבה על ההרחבה השאריות הסיני

$$\mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_5$$

אנחנו בהרחבה. בהתאמת להשתמש בהתאמת גלואה כדי לקבל את היחסים ההפוכים בין תתי־חבורות לבין תתי־שדות בהרחבה. כמובן שכל $\sigma \in G$ מזיזה רק את ξ_{11} אז אם נסתכל על

$$H = \langle \xi_{11} \mapsto \xi_{11}^2 \rangle = \{ \xi_{11} \mapsto \xi_{11}^{2n} \mid 1 \le n \le 5 \}$$

. מסיים $\alpha=\xi_{11}+\overline{\xi_{11}}$ אז אם נבחר (למה? מסדר למה? שכן מסדר היא היא מסיים.