פיתרון לתדגיל מספר 9

תשובה 1:

א. יהי $\varphi \in Aut(G\times H)$ אזי $\varphi(G\times\{1\}) \le G\times H$ כמו כ $\varphi(G\times 1)\cong G\times 1\cong G$ (חח"ע)
עתה $|G_1\times H_1| = |G_1||H_1|$ ו- $\gcd(|G_1|,|H_1|)=1$ לכל $G_1<G, H_1<H$ עהה , מאחר ש
$|\varphi(G\times\{1\})| = |G|$, משיקולי סדרים נקבל $\varphi(G\times 1) = G\times 1$. באופן דומה מוכיחים
$\varphi(1\times H) = 1\times H$ לכן הצימצום של φ ל $G\times 1$ ול- $1\times H$ מגדירים $\varphi_G \in Aut(G)$ ו-
$\varphi_H\in Aut(H)$. בכיוון ההפוך, בהינתן אוטומורפיזמים $\varphi_G\in Aut(G)$ ו- $\varphi_H \in Aut(H)$. נגדיר
$\varphi = \varphi_G\times\varphi_H \in Aut(G\times H)$ בצורה רכיבית.העתקות הנ"ל מגדירות הומומורפיזמים הפוכים.

ב. $Aut(Z_2)=Z_2$ אבל $Aut(Z_2\times Z_2)\cong S_3 \ncong Z_2\times Z_2$.

תשובה 2:

נניח בשלילה ש $G = H_1H_2$ היא מכפלה ישרה של H_1 ו- H_2 כך שהן שונות מ $\{1\}$.
אזי $|H_2| = p^{s_2}$ ו- $|H_1| = p^{s_1}$ באשר $r = s_1+s_2$. נניח בלי הגברת הכלליות ש
$0 < s_2 \le s_1 < r$. יהי $a\in G$ איבר מסדר p^r ונרשם $a = b_1b_2$ נאשר $b_i\in H_i$.
מאחר ש $p^{s_2} | p^{s_1}$ נובע ש $a^{p^{s_1}} = {b_1}^{p^{s_1}}\left({b_2}^{p^{s_2}}\right)^{\frac{p^{s_1}}{p^{s_2}}} = 1\cdot 1 = 1$ בסתירה לכך ש $p^{s_1} < p^r$.

תשובה 3:

תהי G חבורה לא קומוטטיבית מסדר $6 = 3\cdot 2$, עפ"י משפט קושי יש ב- G איבר a מסדר 3 ואיבר b
מסדר 2 . לכן $ab \ne ba$ אחרת ab איבר מסדר 6 $\gcd(|a|,|b|) = \gcd(3,2) = 6$
ואז מקבלים ש G ציקלית (נוצרת ע"י ab) בסתירה להנחה ש-G איננה אבלית. אזי $1,a,a^2,b,ba,ba^2$
הם איברים שונים ב-G (בידקו) כמו כן ab שונה מ- $1,a,a^2,b,ba$ (לדוגמא $ab\ne 1$ כי $b^2=1$) ולכן
$ab = ba^2$. בהתאם לרשום לעיל יש רק דרך אחת למלא את לוח הכפל:

$(G,\cdot)$	1	a	a^2	b	ba	ba^2
1	1	a	a^2	b	ba	ba^2
a	a	a^2	1	ba^2	b	ba
a^2	a^2	1	a	ba	ba^2	b
b	b	ba	ba^2	1	a	a^2
ba	ba	ba^2	b	a^2	1	a
ba^2	ba^2	b	ba	a	a^2	1

זוהי בידיוק S_3 שאזומורפית כמובן ל D_3

ב.אם חבורה מסדר 6 היא אבלית אזי היא ציקלית (שכן $Z_6 \cong Z_2 \times Z_3$) אחרת, ראינו בסעיף 1 שהיא איזומורפית ל D_3 . ב- A_4 אין איבר מסדר 6 לכן אין לה ת"ח אבלית מסדר 6. ב D_3 יש 3 איברים מסדר 2 b, ba, ba^2 והם אינם מתחלפים, לדוגמא $b(ba) = b^2a = a \neq a^2 = bba^2 = b(ab) = (ba)b$
ב- A_4 יש 3 איברים מסדר 2 $(12)(34), (13)(24), (14)(23)$ והם מתחלפים ביניהם לכן D_3 אינה ניתנת לשיכון (איזומורפית לת"ח) של A_4.

<u>תשובה 4:</u>
לפי משפט קושי קיימים ב- G איבר a מסדר p ואיבר b מסדר 2 . תהי H תת החבורה הציקלית הנוצרת ע"י a ותהי K הת החבורה הצקלית הנוצרת ע"י b. $[G:H] = 2$ כמו כן $H \cap K = \{1\}$ כי $\gcd(2,p) = 1$ לכן $G = \{1, a, \dots, a^{p-1}, b, ba, \dots, ba^{p-1}\}$. a ו- b מקיימים את היחסים $a^p = 1$, $b^2 = 1$ ו- $bab^{-1} = a^k$ עבור $k \in \{1, \dots p-1\}$ (הוכחה: $[G:H] = 2$ לכן H נורמלית ב-G לכן $bHb^{-1} \in H = \langle a \rangle$ לכן קיים k כך ש $bab^{-1} = a^k$). יחסים אלו קובעים את טבלת הכפל של G ולכן מגדירים את החבורה G עד כדי איזומורפיזם.
$b^2 = 1$ לכן $a = b^2ab^2 = b(bab^{-1})b^{-1} = ba^kb^{-1} = (bab^{-1})^k = (a^k)^k = a^{k^2}$
מצמצמים ומקבלים $a^{k^2-1} = 1$ לכן $p|k^2 - 1$ ומכאן $p|(k-1)(k+1)$. p ראשוני לכן $p|(k-1)$ או $p|(k+1)$ לכן $k = \mp 1 \mod p$. מאחר ש $k \in \{1, \dots p-1\}$ נקבל ש $k = 1$ או $k = p-1$. אם $k = 1$ אזי $ab = ba$ ולכן G קומוטטיבית. במקרה זה $G = Z_p \times Z_2 \cong Z_{2p}$. אם לעומת זאת, $k = p-1$ נקבל $G = \langle a, b \mid a^p = 1, b^2 = 1, ab = ba^{p-1} \rangle \cong D_p$.

השאלה הזו אינה פשוטה לכן כל מי שפתר ולו חלקית יקבל בונוס של 10 נקודות לתרגיל.

<u>תשובה 5:</u>

א. בסוגריים הימניים הפירוק ובשמאליים הפירוק הקנוני. החבורות השונות מופרדות בפסיקים.
(הסימון: $(2^5, 3^3, 5)$ משמעו $Z_{2^5} \times Z_{3^3} \times Z_5$)

$(2^5, 3^3, 5)$ (4320) , $(2^4, 2, 3^3, 5)$ $(2,2160)$, $(2^3, 2^2, 3^3, 5)$ $(4,1080)$,
$(2^3, 2, 2, 3^3, 5)$ $(2,2,1080)$, $(2^2, 2^2, 2, 3^3, 5)$ $(2,5,540)$, $(2^2, 2, 2, 2, 3^3, 5)$ $(2,2,2,540)$
$(2,2,2,2,2,3^3,5)$ $(2,2,2,2,270)$, $(2^5, 3^2, 3, 5)$ $(3,1440)$, $2^4, 2, 3^2, 3, 5)$ $(6,720)$
$(2^3, 2^2, 3^2, 3, 5)$ $(12,360)$, $(2^3, 2, 2, 3^2, 3, 5)$ $(2,6,360)$, $(2^2, 2^2, 2, 3^2, 3, 5)$,
$(2,12,180)$ $(2^2, 2, 2, 2, 3^2, 3, 5)$, $(2,2,6,180)$,
$(2,2,2,2,2,3^2,3,5)$, $(2,2,2,6,90)$ $(2^5, 3, 3, 3, 5)$, $(3,3,480)$ $(2^4, 2, 3, 3, 3, 5)$, $(3,6,240)$
$(2^3, 2^2, 3, 3, 3, 5)$, $(3,6,240)$ $(2^3, 2, 2, 3, 3, 3, 5)$, $(6,6,120)$ $(2^2, 2^2, 2, 3, 3, 3, 5)$,
$(6,12,60)$ $(2^2, 2, 2, 2, , 3, 3, 3, 5)$, $(2,6,6,60)$ $(2,2,2,2,2,3,3,3,5)$, $(2,2,6,6,30)$

ב. $U_{30}=\{1,7,11,13,17,19,23,29\}$, זוהי חבורה אבלית עם 8 איברים. ניתן לבדוק את סדרי האיברים, ולראות שהם 2 או 4 (או 1) בלבד.
כמו כן ניתן לראות שיש שתי תתי-חבורות שחיתוכן הוא 1 מסדרים 2 ו-4. $\{1,7,13,19\}$ ו - $\{1,11\}$ (הזכרו בהגדרת מכפלה חיצונית ישרה).
משני הנימוקים ניתן לקבל ש- $Z_8=Z_4\times Z_2$.

<u>תשובה 6:</u>

א) $Z\left[\frac{1}{p}\right]=\{\frac{a}{p^n}:a,n\in Z\}$ כש- p מספר ראשוני.
נוכיח ש-A_p תת-חוג ב-Q:
סגירות לחיבור:
$$\frac{a_1}{p^n}+\frac{a_2}{p^k}=\frac{a_1p^k+a_2p^n}{p^{n+k}}\in A_p$$
נייטרלי לחיבור:
$$0\epsilon A: 0=\frac{0}{p}$$
נגדי לחיבור:

יחידה לכפל: $\frac{1}{p^0}=1$ (למשל)
סגירות לכפל:
יהיו $x=\frac{a_1}{p^k},y=\frac{a_2}{p^l}\in A_p$ אזי $xy=\frac{a_2}{p^l}\frac{a_1}{p^k}=\frac{a_1a_2}{p^{l+k}}$ ב-A_p.
לכן A_p תת-חוג ב- Q.
אבל A_p אינו שדה:
למשל:$\frac{p+1}{p}$ אינו הפיך ב-A_p (כיוון ש- $\frac{p}{p+1}$ אינו ב- A_p).
A_p תחום שלימות :מושרה מ-Q.

ב) B אינו חוג: אין סגירות ביחס לכפל: $\sqrt[3]{2}*\sqrt[3]{2}=\sqrt[3]{4}\notin B$.
ג) C הוא למעשה שדה. ההוכחה היא טכנית (הבדיקה היחידה שהיא קשה יחסית היא סגירות להופכי, את ההופכי מוצאים באופן הבא : $\frac{1}{a+b\sqrt{5}}=\frac{1}{a+b\sqrt{5}}\cdot\frac{a-b\sqrt{5}}{a-b\sqrt{5}}=\left(\frac{a}{a^2+5b^2}\right)+\left(\frac{-b}{a^2+5b^2}\right)\sqrt{5}$)

<u>תשובה 7:</u>

א) $(2x)^2=2x \Leftarrow 4x^2=2x \Leftarrow 4x=2x \Leftarrow 2x=0 \Leftarrow x=-x$
אם $x,y\in A$, $(x+y)^2=x+y \Leftarrow x^2+y^2=x+y=x^2+xy+yx+y^2 \Leftarrow$
$xy+yx=0 \Leftarrow xy=-yx=yx$ לכן A קומוטטיבי (יחסית לפעולת הכפל).
ב) אם $x,y\in A$, אז $xy(x+y)=xyx+xy^2=x^2y+xy^2=2xy=0$

אם אין מחלקי אפס ב-A, אז אין יותר משני איברים ב-A : נניח בשלילה שקיימים X ו-Y ב-A שונים זה מזה ושונים מ-0 . לכן $(X+Y)\neq 0$ (אם לא : $X=-Y=Y$) ואז $XY(X+Y)\neq 0$ כי אין מחלקי אפס : סתירה

<u>תשובה 8:</u>

א) נוכיח רק את "חוק הבליעה" (כמובן שצ"ל גם ש- K היא תת חבורה חיבורית של R [x])
יהיו $g\in R[x]$ ו- $f\in K$ צ"ל $fg\in K$. ואכן $(gf)(137)=g(137)*f(137)=g(137)\cdot 0=0$

ב) נגדיר את הומומורפיזם ההצבה: R → R[x] על ידי f(137)→f(x). אזי הגרעין הוא K (בדקו זאת!) וזוהי העתקה על (לכל מספר נקח את הפולינום הקבוע המוגדר באמצעותו), ולכן, ע"פ משפט האיזומורפיזם הראשון: R[x] / K איזומורפי ל-R. מכיוון ש-R הוא שדה, K הוא אידיאל מקסימלי.
ג) M = { f ∈R[x] : f(1) = 10} לא – זו לא ת"ח חיבורית.
L = { f ∈R[x] : f(0) = 0} כן – זהו הגרעין של הומומורפיזם ההצבה כשמציבים x=0 (למעשה זהו האידיאל הראשי <x>).

<u>תשובה 9:</u>

I אידיאל של R. מכך ש I חבורה חיבורית מקבלים ישירות ש $\mathrm{M}_n(I)$ חבורה חיבורית. תהי $A=\left(\mathrm{a}_{\mathrm{i,j}}\right)\in$ $\mathrm{M}_n(I)$ דהיינו $\mathrm{a}_{\mathrm{i,j}}\in \mathrm{I}$ ותהי $B=\left(b_{\mathrm{i,j}}\right)\in \mathrm{M}_n(R)$ דהיינו $\mathrm{b}_{\mathrm{i,j}}\in \mathrm{R}$ תהי $C=\left(c_{\mathrm{i,j}}\right)=\mathrm{AB}$ אזי $c_{\mathrm{i,j}}=\sum \mathrm{a}_{\mathrm{i,k}}\mathrm{b}_{\mathrm{k,j}}$ מהבליעה של I נובע שלכל i,j,k מתקיים $\mathrm{a}_{\mathrm{i,k}}\mathrm{b}_{\mathrm{k,j}}\in \mathrm{I}$ שכן $\mathrm{a}_{\mathrm{i,k}}\in \mathrm{I}$ לכן כל נסכם נמצא ב I ומאחר ש I חבורה חיבורית הסכום כולו נמצא ב I לכן לכל i,j $c_{\mathrm{i,j}}\in \mathrm{I}$ ומכאן ש $\mathrm{AB}\in \mathrm{I}$.
באופן סימטרי מוכיחים ש $\mathrm{BA}\in \mathrm{I}$.