גירסה 1.01 – 23.2.2007

גירסה 1.00 - 14.7.2002

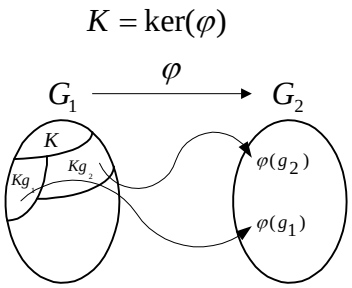
סיכום נקודות באלגברה מודרנית - חלק שני

ניר אדר

Nir Adar
Email: nir@underwar.co.il
Home Page: http://www.underwar.co.il

אנא שילחו תיקונים והערות אל המחבר.

משפטי הומומורפיזמים



משפט האיזומורפיזם הראשון

יהיו G_1, G_2 חבורות, ויהי $\varphi: G_1 \to G_2$ הומומורפיזם, אזי מתקיים כי $\frac{G_1}{\ker(\varphi)} \cong \mathrm{Im}(\varphi)$.

הגדרה

תהא G חבורה, ויהיו $H, K \subseteq G$ תת חבורות. נגדיר:

$$HK = \{hk \mid h \in H, k \in K\}$$

משפט האיזומורפיזם השני

G חבורה. $N \lhd G$, H תת חבורה, אזי:

1. HN היא תת חבורה.
2. $N \lhd NH$
3. $N \bigcap H \lhd H$
4. $\frac{HN}{N} \cong \frac{H}{H \bigcap N}$

משפט האיזומורפיזם השלישי

G חבורה, $N \subseteq G, K \lhd G$, $N \lhd G$ אזי:

$$\frac{G}{N} \cong \frac{\left(\frac{G}{K}\right)}{\left(\frac{N}{K}\right)}$$

חוגים

חוג זו קבוצה (נסמנה R) עם שתי פעולות: $+,\cdot$ (חיבור, כפל), עבורה מתקיימות הדרישות הבאות:

1. R חבורה אבלית לגבי הפעולה + (סגירות לפעולה, אסוציאטיביות, קיום איבר אדיש, קיום איבר נגדי, הפעולה היא קומוטטיבית). האיבר הנטרלי יסומן ב0, והנגדי של a יסומן ב-$-a$.
2. R תהיה סגורה לגבי הפעולה $\cdot$. $ab \in R \Leftarrow a,b \in R$
3. פעולה הכפל הינה פעולה אסוציטיבית. $a,b,c \in R \Rightarrow (ab)c = a(bc)$
4. $a(b+c) = ab + ac,\ (b+c)a = ba + ca \Leftarrow a,b,c \in R$

דוגמא

$2\mathbb{Z}$ - זהו חוג לגבי השלמים, (מתקיימות התכונות) אולם לא קיים איבר יחידה (איבר אדיש לכפל).

הגדרות בסיסיות בנושא חוגים

חוג עם יחידה הינו חוג R שיש בו איבר נטרלי לגבי הפעולה $\cdot$. איבר זה יסומן ב-1.
מתקיים: $\forall a \in R,\ 1 \cdot a = a \cdot 1 = a$

חוג קומוטטיבי הינו חוג שבו $\cdot$ קומוטטיבי, כלומר $\forall a,b \in R,\ ab = ba$

מחלק אפס בחוג R זה איבר $0 \neq a \in R$, כך שקיים $0 \neq b \in R$, כך שמתקיים $ab = 0$ או $ba = 0$.

תחום שלמות זהו חוג קומוטטיבי שאין בו מחלקי אפס.

איבר הפיך בחוג עם יחידה R זה איבר $a \in R$ כך שקיים $b \in R$ המקיים $ab = ba = 1$.

חוג עם חילוק זהו חוג עם יחידה שבו כל איבר שונה מאפס הוא הפיך.

שדה הוא חוג קומוטטיבי עם חילוק.

משפט

R חוג, אזי:

1. האיבר 0 הוא יחיד.
2. $a \Leftarrow a \in R$ יחיד.
3. $\forall a \in R, 0a = a0 = 0$
4. $\forall a \in R, a \cdot (-b) = (-a)b = -(ab)$
5. $(-a)(-b) = ab$
6. בהינתן ש-R חוג עם יחידה, מתקיים $(-1)a = -a$.

משפט

1. אם D הוא תחום שלמות, ונתון ש- $ab = ac$ ($a \neq 0$), אז $b = c$.
2. בשדה אין מחלקי אפס, כלומר כל שדה הוא תחום שלמות.

משפט

1. מספר האיברים בשדה סופי הוא חזקה של מספר ראשוני.
2. אם p ראשוני, ו n מספר טבעי, אז יש שדה בן p^n איברים.

הגדרה

יהי שדה F, המספר m הקטן ביותר כך ש $\underbrace{1+1+...+1}_{\text{m times}}=0$ נקרא **המציין של השדה**, והוא מסומן ב- $char(F)$. אם אין m כזה, אז המציין של F הוא 0.

מסקנה

המציין של שדה סופי הוא מספר ראשוני.

טענה

כל תחום שלמות סופי הוא שדה.

תתי חוגים

הגדרה

יהי R חוג ו-S תת קבוצה לא ריקה של R. אם S היא בעצמה חוג ביחס לפעולות בR, אזי אומרים ש-S היא **תת חוג**.

טענה

יהי R חוג, ו-S תת קבוצה לא ריקה של R, אזי S היא תת חוג של R אמ"מ:

1. $a-b\in S$ עבור כל $a,b\in S$ (נדרוש שS חבורה - $ab^{-1}\in H$ לכל a,b)
2. $a\cdot b\in S$ עבור כל $a,b\in S$ (סגירות לכפל).

הערה: לכל חוג יש שני תתי חוגים טריוויאליים: החוג עצמו ו- $\{0\}$.

הגדרה

יהי R חוג, I קבוצה ב-R שמקיימת:

1. $I\neq\phi$
2. $a+b\in I \Leftarrow a,b\in I$
3. $-a\in I \Leftarrow a\in I$
4. $ax\in I, xa\in I \Leftarrow x\in R, a\in I$

קבוצה שמקיימת דרישות אלו נקראת **אידיאל** ב-R.
שלושת התכונות הראשונות זוהי פשוט דרישה ש-I תהיה תת חבורה.
דרישה 4 כוללת את דרישות תת חוג, ודרישות נוספות, חזקות יותר.

אידיאל משמש לאותו תפקיד בו משמשת תת חבורה נורמלית בחבורות.

הגדרה (שקולה)

יהי R חוג ויהי I תת חוג של R.
אומרים ש-I **אידיאל שמאלי** של R אם מתקיים $rx \in I$ עבור כל $r \in R, x \in I$
אומרים ש-I **אידיאל ימני** של R אם מתקיים $xr \in I$ עבור כל $r \in R, x \in I$
אומרים ש-I **אידיאל** אם הוא אידיאל ימני ואידיאל שמאלי.

טענה

תהי S תת קבוצה לא ריקה של חוג R, אזי:
א. S אידיאל שמאלי של R אמ"מ:
1. $a-b \in S \Leftarrow a,b \in S$
2. $r \cdot a \in S \Leftarrow r \in R, a \in S$
ב. S אידיאל ימני של R אמ"מ:
1. $a-b \in S \Leftarrow a,b \in S$
2. $a \cdot r \in S \Leftarrow r \in R, a \in S$
ג. S אידיאל אמ"מ מתקיימים א', ב'.

הומומורפיזם בין חוגים

הומומורפיזם זו פונקציה $\varphi : R_1 \to R_2$, R_1, R_2 חוגים, כך שמתקיים:

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

גרעין של הומומורפיזם φ:

$$\ker(\varphi) = \{x \in R_1 \mid \varphi(x) = 0\}$$

מסקנות

יהי $\varphi : R_1 \to R_2$ הומומורפיזם בין חוגים, אזי:
1. $\varphi(0) = 0$
2. $\varphi(-\alpha) = -\varphi(a)$
3. φ ח.ח.ע אמ"מ $\ker\varphi = \{0\}$.

הערה

בחוג כל תת חבורה לגבי החיבור היא תת חבורה נורמלית (חוג הוא חבורה אבלית לגבי החיבור).

משפט

יהי $\varphi : R_1 \to R_2$ הומומורפיזם בין חוגים, אזי:
1. $\ker(\varphi)$ הוא תת חבורה של R_1 לגבי +.
2. $ax, xa \in \ker(\varphi) \Leftarrow x \in R_1, a \in \ker(\varphi)$

הערה

כל גרעין של הומומורפיזם בין חוגים הוא אידיאל.

הגדרה - חוג מנה

יהי I אידיאל בחוג R. ניקח $b \in R$ ונגדיר את **הקוסט** של b.

$$I + b = \{x + b \mid x \in I\}$$

זוהי בדיוק הגדרת הקוסט בחבורות, מלבד זאת שהכפל נהפך ל+.
מתקיים: $I + b = b + I$ כי I קומוטטיבית, ולכן בפרט I תת חבורה נורמלית ב-R לגבי הפעולה +.
נסמן $\frac{R}{I}$ בתור אוסף כל הקוסטים של I ב-R.

$$\frac{R}{I} = \{I + b \mid b \in R\}$$

משפט

R חוג, K אידיאל, אזי:

1. $\frac{R}{K}$ הוא חוג ביחס לפעולות:

$$(K + a) + (K + b) = K + (a + b)$$
$$(K + a) \cdot (K + b) = K + ab$$

ההגדרות בדומה להגדרת הפעולות על חבורות מנה.

2. אם יש ב-R יחידה, אזי $K + 1$ היא יחידה של $\frac{R}{K}$.
3. אם R קומוטטיבי, אזי גם $\frac{R}{K}$ קומוטטיבי.

הערה: יש לשים לב כי אם R תחום שלמות, $\frac{R}{K}$ איננו בהכרח תחום שלמות, ולהפך.

הערה: אם K הוא אידיאל, אז K הוא גרעין של הומומורפיזם. ההומומורפיזם:

$$\varphi : R \to \frac{R}{K}$$
$$\varphi(a) = K + a$$

טענה

אם U אידיאל בחוג R עם יחידה I+1 מכיל איבר הופכי ביחס לכפל, אזי I=R. (כלומר האידיאל היחידי הוא האידיאל הטריוויאלי).

הערה

אידיאל נקרא אמיתי אם $I \neq R$ וגם $I \neq \{0\}$

טענה

בשדה אין אידיאלים אמיתיים. (אם זאת, יתכן חוג שאיננו שדה אבל בכל זאת אין בין אידיאלים אמיתיים)

טענה

שלושת משפטי ההומומורפיזמים נכונים גם לגבי הומומורפיזמים של חוגים.

המשפט הראשון

$\varphi: R_1 \to R_2$ הומומורפיזמים בין חוגים, אזי $\frac{R_1}{\ker(\varphi)} \cong \mathrm{Im}(\varphi)$.

המשפט השני

I, J אידיאלים בחוג R, אזי $\frac{I+J}{I} \cong \frac{J}{I \bigcap J}$.

המשפט השלישי

יהיו שני אידיאלים I, J בחוג R, כך ש- $J \subseteq I \subseteq R$, אזי

$$\frac{\left(\frac{R}{J}\right)}{\left(\frac{I}{J}\right)} \cong \frac{R}{I}$$

משפט

כל אידיאל ב- $\mathbb{Z}$ הוא מהצורה $m\mathbb{Z}$ עבור m טבעי כלשהו.

הגדרה

$$\varphi: \mathbb{Z} \to \mathbb{Z}_n$$
$$\varphi(a) = a (\mathrm{mod}\, n)$$

מתקיים כי φ הוא **הומומורפיזם בין חוגים**.

מסקנה

$\frac{\mathbb{Z}}{n\mathbb{Z}}$ הוא שדה אמ"מ n מספר ראשוני.

משפט

נניח ש-R חוג קומוטטיבי עם יחידה. אם $R,\{0\}$ הם האידיאלים היחידים, אז R הוא שדה.

הגדרה

R חוג קומוטטיבי ויהי $a \in R$. נסמן ב: $(a) = \{ax \mid x \in R\}$.
(a) הוא אידיאל, והוא נקרא **האידיאל הראשי** הנוצר על ידי a.

הגדרה

יהי R חוג ו-I אידיאל בR. I נקרא אידיאל מקסימלי אם I לא מוכל בשום אידיאל אחר פרט ל-I, R.

משפט

יהי R חוג קומוטטיבי עם יחידה. יהי I אידיאל ב-R, אזי $\frac{R}{I}$ הוא שדה אם ורק אם I אידיאל מקסימלי.

הערה

יהיו שני חוגים R_1, R_2 איזומורפיים: $R_1 \cong R_2$.
אם R_1 הוא שדה, אזי גם R_2 הוא שדה. $\varphi(1)$ זהו היחידה של R_2.

חוגי פולינומים

יהי שדה F.
נסמן ב-$F[x]$ את אוסף כל הפולינומים עם מקדמים בF.

הגדרה

פולינום הוא צירוף ליניארי של חזקות של משתנה.

$$f(x)=a_0+a_1x+a_2x^2+...+a_nx^n$$

$a_1,a_2,...,a_n\in F$, X משתנה בשדה F.
ה-n הגדול ביותר, כך ש a_n שונה מ0, נקרא **הדרגה (המעלה)** של הפולינום.

סימון

נסמן את מעלת הפולינום $f(x)$ על ידי $\deg(f(x))$.

פולינום האפס

פולינום שכל מקדמיו הם אפסים, נקרא **פולינום האפס**.

$$0+0\cdot x+0\cdot x^2+...+0\cdot x^n$$

מעלתו של פולינום האפס איננה מוגדרת.

הערה

יהיו שני פולינומים $f(x),g(x)$, אזי:

$$\deg\left(f(x)+g(x)\right)\le\max\left(\deg f(x),\deg g(x)\right)$$

בתנאי ש $f(x)+g(x)$ איננו פולינום האפס.

משפט

$F\left[X\right]$ זהו חוג קומוטטיבי עם יחידה, ללא מחלקי אפס - תחום שלמות.

משפט

יהיו שני פולינומים $f(x),g(x)\in F\left[x\right]$, וגם $g(x)\neq 0$.
אזי קיימים שני פולינומים אחרים: $q(x),r(x)\in F\left[x\right]$ כך שמתקיים:

$$f(x)=g(x)\cdot q(x)+r(x)$$

$r(x)$ היא או פולינום האפס, או ש $def\left(r(x)\right)<\deg(g(x))$

משפט

כל אידיאל בחוג F[x] הוא ראשי.

סימון

נניח כי $f(x)=a(x)b(x)$, אזי נאמר כי $a(x)$ מחלק את $f(x)$, ומסמנים: $a(x)\big|f(x)$

הערה

כל חוג מנה של F[x] הוא מהצורה $\frac{F[x]}{(f(x))}$ עבור $f(x)\in F[x]$ כלשהו.

משפט

יהא $f(x)\in F[x]$. נניח כי $\deg(f(x))=n$ אזי כל איבר בחוג המנה $\frac{F[x]}{(f(x))}$ ניתן להצגה באופן יחיד בצורה:

$$a_0+a_1x+...+a_{n-1}a^{n-1}+(f(x))$$

כאשר $a_0,a_1,...,a_{n-1}\in F$.

מסקנה

נניח ש-F שדה בן q איברים. יהא $f(x)\in F[x]$ ממעלה n. מתקיים כי מספר האיברים בחוג המנה $\frac{F[x]}{(f(x))}$ הוא q^n .

שאלה

מתי $\frac{F[x]}{(f(x))}$ הוא שדה?

אנו יודעים כי $F[x]$ זהו חוג קומוטטיבי עם יחידה, ולכן כאשר $(f(x))$ הוא אידיאל מקסימלי, יש בידנו שדה.

נשאל כעת מתי אידיאל זה הוא אידיאל מקסימלי.

ניזכר בדוגמא שראינו לגבי המספרים השלמים: $\frac{\mathbb{Z}}{(n)}\cong\mathbb{Z}_n$.

הגענו למסקנה כי (n) הוא אידיאל מקסימלי אמ"מ n ראשוני.

תזכורת: אידיאל מקסימלי הוא אידיאל שלא מוכל בכל אידיאל אחר פרט לחוג.
נביט כעת בחוג הפולינומים.

הגדרה

יהי $f(x)\in F[x]$. $f(x)$ נקרא **פולינום אי פריק**, אם מחלקיו היחידים הם: איברי F (סקלרים) וכפולותיו באיברי F.

הערה

כל פולינום מתחלק באיברי F ובכפולותיו. פולינום פריק הוא פולינום שאלו מחלקיו היחידים.

הגדרה

פולינום פריק הוא פולינום שאיננו אי פריק.

משפט

יהי $f(x)$ פולינום שאיננו פולינום האפס. $\frac{F[x]}{(f(x))}$ הוא שדה אמ"מ הפולינום $f(x)$ הוא אי-פריק.

טענה

כל פולינום ממעלה ראשונה הוא אי פריק.

משפט

יהי $f(x)\in F[x]$, $a\in F$, אז:

א. $f(x)=(x-a)q(x)+f(a)$.

ב. $f(a)=0$ אמ"מ $(x-a)\mid f(x)$.

מכאן: אם לפולינום יש שורש בשדה, אזי הפולינום פריק.

מסקנה

יהי $f(x)\in F[x]$, כך ש $\deg(f(x))\geq 2$. אם יש ל $f(x)$ שורש בF, אז $f(x)$ פריק.
(כי אם a הוא שורש, $f(x)=(x-a)q(x)$).

הערה - אזהרה

לא לכל פולינום פריק יש בהכרח שורשים.

משפט

$f(x)\in F[x]$, כך ש $f(x)$ פולינום ממעלה 2 או 3. אם $f(x)$ פריק אז יש לו שורש ב-F.

מסקנה

אם $f(x)\in F[x]$ ממעלה 2 או 3, אזי $f(x)$ אי פריק מעל F, אמ"מ אין ל-$f(x)$ שורש בF.

הערה

כל פולינום ב-$\mathbb{C}[x]$ ממעלה גדולה מ-1, הוא פריק מעל $\mathbb{C}$.
(לפי המשפט היסודי של האלגברה, לכל פולינום עם מקדמים ב-$\mathbb{C}$ יש שורש ב-$\mathbb{C}$).

הערה

לכל פולינום בעל מעלה אי זוגית, קיים שורש אחד לפחות.

משפט

כל פולינום ממעלה גדולה או שווה מ-3 ב-$\mathbb{R}[x]$ הוא פריק מעל $\mathbb{R}$.

משפט

יהי $f(x)$ פולינום עם מקדמים ממשיים: $f(x)=a_0+a_1x+a_2x^2+...+a_nx^n$
בהנתן ש-$\frac{p}{q}$ הוא שבר מצומצם שהוא שורש של $f(x)$ יתקיים $p\mid a_0,\ q\mid a_n$.

משפט (אייזנשטיין)

יהי $f(x)$ מהצורה: $f(x)=a_0+a_1x+a_2x^2+...+a_nx^n$ כאשר $a_0,a_1,...,a_n$ הם מספרים שלמים.
נניח שקיים מספר ראשוני p כך ש $p\mid a_0, p\mid a_1,..., p\mid a_{n-1}$ (p מחלק את כל המקדמים, פרט לאחרון)
וגם $p\nmid a_n, p^2\nmid a_0$ אזי $f(x)$ אי פריק מעל הרציונליים.

דוגמא

$$f(x)=1+x+x^2+x^3+x^4$$

האם פולינום זה אי פריק מעל $\mathbb{Q}$?

תזכורת: פולינום פריק הוא מהצורה $f(x)=a(x)b(x)$.
מתקיים: הפריקות עבור $f(x)$ שקולה עבור פריקות של $f(x+1)=a(x+1)b(x+1)$
נבדוק את הפריקות של $f(x+1)$

$$f(x+1)=1+(x+1)+(x+1)^2+(x+1)^3+(x+1)^4=$$
$$=1+x+1+x^2+2x+1+x^3+3x^2+3x+1+x^4+4x^3+6x^2+4x+1=$$
$$=x^4+5x^3+10x^2+10x+5$$

פולינום זה מקיים את תנאי משפט אייזנשטיין עבור $x=5$.
לכן, פולינום זה אי פריק.

מחלק משותף מקסימלי

הגדרה

יהיו $f(x), g(x) \in F[x]$ השונים מפולינום האפס.
$d(x) \in F[x]$ יקרא **מחלק משותף מקסימלי** של $f(x), g(x)$ אם מתקיים:

1. $d(x) \mid f(x),\ d(x) \mid g(x)$.
2. כל פולינום אחר המחלק את $f(x)$ וגם את $g(x)$ יהיה ממעלה קטנה או שווה לזו של $d(x)$.
3. $d(x)$ הוא פולינום מתוקן - כלומר, מקדם החזקה הגבוהה ביותר שווה ל1.

משפט

יהיו שני פולינומים $f(x), g(x) \in F[x]$ שונים ויהי $d(x)$ הוא המחלק המשותף המקסימלי (מ. מ. מ.) שלהם.

1. קיימים $\alpha(x), \beta(x)$ ב$F[x]$, כך ש $d(x) = \alpha(x) f(x) + \beta(x) g(x)$.
   (ראינו משפט מקביל עבור מספרים שלמים).
2. כל מחלק משותף של $f(x), g(x)$ מחלק את המחלק המשותף המקסימלי $d(x)$.
3. המחלק המשותף המקסימלי הוא יחיד.

משפט

$a(x), b(x), f(x) \in F[x]$.
נתון כי $f(x) \mid a(x)b(x)$ וכי $f(x)$ זר ל$a(x)$, אזי $f(x) \mid b(x)$.

משפט (פריקות חד ערכית)

כל פולינום ב-$F[x]$ ניתן להצגה יחידה כמכפלת פולינומים אי פריקים (עד כדי כפל בסקלרים).
כלומר:

$$f(x) = p_1(x)^{l_1} \cdot p_2(x)^{l_2} \cdot \ldots \cdot p_k^{\ l_k} = q_1(x)^{n_1} \cdot q_2(x)^{n_2} \cdot \ldots \cdot q_s^{\ n_s}$$

כך ש-$q_i(x), p_i(x)$ אי פריקים, אזי מתקיים כי $k = s$, כל $q_i(x)$ שווה לכפולה בסקלר של $p_i(x)$ עם מעריך שווה.

האלגוריתם של אוקלידס

נתונים $f(x), g(x) \in F[x]$ השונים מפולינומים האפס.

נניח בלי הגבלת הכלליות כי $\deg(f(x)) \geq \deg(g(x))$.

נחלק את $f(x)$ ב-$g(x)$.

$$f(x) = g(x) \cdot q_1(x) + r_1(x), \ \deg(r_1(x)) < \deg(g(x))$$
$$g(x) = r_1(x) \cdot q_2(x) + r_2(x), \ \deg(r_2(x)) < \deg(r_1(x))$$
$$r_1(x) = r_2(x) \cdot q_3(x) + r_3(x), \ \deg(r_3(x)) < \deg(r_2(x))$$
$$r_2(x) = r_3(x) \cdot q_4(x) + r_4(x), \ \deg(r_4(x)) < \deg(r_3(x))$$
$$\ldots$$
$$r_{n-1}(x) = r_n(x) \cdot q_{n+1}(x) + r_{n+1}(x)$$
$$r_n(x) = r_{n+1}(x) \cdot q_{n+2}(x) + 0$$

נטען כי $r_{n+1}(x)$ הינו ה-מ. מ. מ., עד כדי תיקון.