אלגברה מופשטת 2, 88־212

פרופ׳ ע. וישנה

מועד א׳ ־ פתרון חלקי, תשע״א

ענו על כל חמש השאלות. הניקוד המלא לשאלה, מן הטובה לפחות טובה, הוא $10, 15, 20, 25, 30$.
משך המבחן. שעתיים וחצי.

1. (א) הראה ששלושת החוגים $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $R_3=(\mathbb{Z}/2\mathbb{Z})[\epsilon]/\langle\epsilon^2\rangle$ אינם איזומורפיים זה לזה.

   (ב) קבע לאיזה מהם איזומורפי $\mathbb{Z}[i]/\langle 2\rangle$.

   (ג) מצא חוג (עם יחידה) נוסף בן ארבעה אברים, שאינו איזומורפי לאף אחד מהנ״ל.

פתרון. שלושת החוגים קומוטטיביים, בעלי ארבעה אברים, ואף אחד מהם אינו תחום שלמות. בחוג $\mathbb{Z}_4=\mathbb{Z}/4\mathbb{Z}$ מתקיים $2\neq 0$, בעוד ש־$1+1=0$ בחוגים האחרים; לכן הוא אינו יכול להיות איזומורפי להם. בחוג $\mathbb{Z}_2\times\mathbb{Z}_2$ כל איבר מקיים את היחס $x^2=x$ (ולא קיימים איברים שונים מאפס שריבועם אפס); לעומת זאת ב־$\mathbb{Z}_2[\epsilon]/\langle\epsilon^2\rangle$ החוק $x^2=x$ אינו נכון, ויש איברים שונים מאפס שריבועם אפס. כעת, $\mathbb{Z}[i]/\langle 2\rangle\cong\mathbb{Z}[x]/\langle 2,x^2-1\rangle\cong\mathbb{Z}[y]/\langle 2,y^2\rangle$ על־ידי ההצבה $y=x+1$, ולכן הוא איזומורפי לחוג השלישי ברשימה. החוג הרביעי מסדר 4 הוא השדה בן 4 אברים, $\mathbb{F}_4=\mathbb{Z}_2[t]/\langle t^2+t+1\rangle$. אפשר למצוא אותו כך: יש רק חוג אחד עם מאפיין 4, הנמצא כבר ברשימה, ולכן אפשר להניח שהמאפיין הוא 2; מכאן ש־$\mathbb{Z}_2$ הוא תת־חוג, אבל החוג שלנו גדול יותר ולכן יש בו איבר נוסף, שאפשר לקרוא לו a. לכן אפשר להציג $R=\mathbb{Z}_2[a]$. המימד של R מעל $\mathbb{Z}_2$ הוא $\log_2(4)=2$, ולכן a מקיים משוואה ריבועית; יש בדיוק ארבע אפשרויות: $a^2=0$, $a^2=1$, $a^2=a$, $a^2=a+1$. המקרה הראשון הוא החוג R_3; שני האמצעיים הם $\mathbb{Z}_2\times\mathbb{Z}_2$; והאחרון הוא השדה שלנו כי הפולינום המינימלי אי־פריק. הוכחנו שיש בדיוק ארבעה חוגים עם ארבעה איברים. תרגיל לא קל: הראה שיש בדיוק 11 חוגים עם שמונה איברים, מהם רק אחד שאינו קומוטטיבי.

2. א. מצא את המחלק המשותף המקסימלי של $a=16+5\sqrt{-2}$ ושל $b=1+12\sqrt{-2}$ בחוג $\mathbb{Z}[\sqrt{-2}]$.

   ב. פרק את $16+5\sqrt{-2}$ לגורמים אי־פריקים בחוג זה. מדוע הם ראשוניים?

פתרון. נזכר שכל איבר שהנורמה שלו היא מספר ראשוני, מוכרח להיות אי־פריק. החוג $\mathbb{Z}[\sqrt{-2}]$ הוא אוקלידי, ולכן האיברים האי־פריקים שלו הם כולם ראשוניים. אגב, יש איברים אי־פריקים שהנורמה שלהם אינה ראשונית (לדוגמא: 7).

נחשב $N(a)=16^2+2\cdot 5^2=306=2\cdot 3^2\cdot 17$, ו־$N(b)=1^2+2\cdot 12^2=289=17^2$. לכן הנורמה של המחלק המשותף המקסימלי מוכרחה לחלק את 17, שהוא ראשוני, וכדי למצוא אותו מספיק לעבור על כל האברים עם נורמה כזו: הפתרונות ל־$x^2+2y^2=17$ הם שמונת המספרים $x+y\sqrt{-2}=\pm 1\pm 3\sqrt{-2},\pm 3\pm 2\sqrt{-2}$. בחוג הזה אין אברים הפיכים פרט ל־± 1, ולכן יש ברשימה ארבעה מספרים אי־פריקים, עד כדי חברות, ויש לבדוק את כולם. לחילופין, אפשר לנסות חילוק עם שארית: $\frac{a}{b}=\frac{136}{289}+\frac{-187}{289}\sqrt{-2}$, והמספר השלם הקרוב ביותר הוא $q=-\sqrt{-2}$. למזלנו, הנורמה של $r=a-qb=-8+6\sqrt{-2}$, בעל נורמה $8^2+2\cdot 6^2=136=2^3\cdot 17$. כמובן, $\langle a,b\rangle=\langle b,r\rangle$. למעשה $r=-2(4-3\sqrt{-2})$, ומכיוון ש־2 זר ל־b, $\langle b,r\rangle=\langle b,4-3\sqrt{-2}\rangle$. נבצע שוב חילוק עם שארית: $\frac{b}{4-3\sqrt{-2}}=-2+\frac{3}{2}*\sqrt{-2}$, והפעם $b=(-2+\sqrt{-2})(4-3\sqrt{-2})+(3+2\sqrt{-2})$, כשהשארית $3+2\sqrt{-2}$ היא בעלת נורמה 17. בדיקה ישירה מראה ש־$3+2\sqrt{-2}$ מחלק את b, ולכן את a, והוא המחלק המשותף המקסימלי.

בסעיף הקודם מצאנו ש־$a=(3+2\sqrt{-2})(4-\sqrt{-2})$, כשהנורמה של הגורם השני היא 18. מבט עז בגורם הזה מגלה שהוא שווה ל־$-\sqrt{-2}(1+2\sqrt{-2})$, כשהנורמה של הגורם האחרון היא 9. יש בחוג בדיוק ארבעה אברים עם נורמה 3, והם $\pm 1\pm\sqrt{-2}$. בדיקה ישירה מראה ש־$(1-\sqrt{-2})^2=-(1+2\sqrt{-2})$, וכך הגענו לפירוק הסופי: $a=\sqrt{-2}(3+2\sqrt{-2})(1-\sqrt{-2})^2$; לכל הגורמים האלה נורמה ראשונית, ולכן הם ראשוניים.

3. (א) הוכח את ההכלה $R=\mathbb{Q}((x))[[y]]\subseteq\mathbb{Q}[[y]]((x))$.[1]

   (ב) הראה שזו הכלה אמיתית על־ידי שתצביע על איבר הנמצא בחוג הגדול אבל לא בחוג הקטן.

   (ג) כתוב במפורש מהו ההפכי של $1-x-y$ בחוג המנה R/y^3R.

[1] את החוגים בונים מבפנים החוצה: באגף שמאל מדובר בחוג $(\mathbb{Q}[[y]])((x))$, כלומר, החוג של טורי לורן ב־x מעל החוג של טורי החזקות הפורמליים $\mathbb{Q}[[y]]$; באגף ימין $(\mathbb{Q}((x)))[[y]]$ הוא החוג של טורי החזקות הפורמליים ב־y מעל לחוג של טורי לורן ב־x.

פתרון. האיבר הכללי באגף שמאל הוא $f=\sum_{n=-N}^{\infty} f_n x^n$ עבור $f_n\in\mathbb{Q}[[y]]$ ו־N שלם כלשהו. לכל n אפשר לכתוב $f_n=\sum_{i=0}^{\infty} a_{in}y^i$ עבור $a_i\in\mathbb{Q}$ מתאימים, ואז $f=\sum_{n=-N}^{\infty}\sum_{i=0}^{\infty} a_{in}y^ix^n = \sum_{i=0}^{\infty}\left(\sum_{n=-N}^{\infty} a_{in}x^n\right)y^i$, השייך ל־$\mathbb{Q}((x))[[y]]$ כי כל המקדמים $\sum_{n=-N}^{\infty} a_{in}x^n$ נמצאים ב־$\mathbb{Q}((x))$. באופן הזה קיבלנו איברים שבהם המקדם המוביל של x בכל החזקות של y הוא קבוע. האיבר $\sum_n x^{-n}y^n$ שייך ל־$\mathbb{Q}((x))[[y]]$, אבל אינו שייך ל־$\mathbb{Q}[[y]]((x))$, משום שיש בו חזקות שליליות לא חסומות של x.

4. נקבע בסיס e_1,e_2 למודול $\mathbb{Q}[x]^2$ ...

5. יהי M מודול מעל חוג R. תת־מודול $N<M$ נקרא **תת־מודול קטן** של M אם לכל תת־מודול אמיתי $M_1<M$, גם $N+M_1<M$. את הטענה "N תת־מודול קטן של M" נסמן ב־$N\le_s M$.

   (א) הוכח שתת־מודול של תת־מודול קטן של M הוא קטן (אם $K\le N\le_s M$ אז $K\le_s M$).

   (ב) הוכח שסכום של שני תת־מודולים קטנים הוא קטן.

   (ג) יהי R תחום שלמות שאינו שדה, ו־F שדה השברים שלו.

      i. הראה שכל תת־מודול $0\ne L\le F$, כמודולים מעל R, כולל איבר $0\ne t\in R$.

      ii. הראה ש־$R\le F$ הוא תת־מודול קטן.[2]

פתרון. [שימו לב להבדל בין $<$ ו־$\le$, שהוא מהותי לשאלה הזו.] (א). יהי N תת־מודול קטן של M, ויהי K תת־מודול של N. יהי M_1 תת־מודול אמיתי של M. אז $M_1+K\subseteq M_1+N<M$ מכיוון ש־N קטן; לכן גם K קטן. (ב). נניח ש־N_1,N_2 שניהם תת־מודולים קטנים של M. יהי $M'<M$ תת־מודול אמיתי כלשהו, אז $M+N_1<M$ כי N_1 קטן, ו־$M+(N_1+N_2)=(M+N_1)+N_2<M$ כי N_2 קטן. מכאן שגם N_1+N_2 קטן. (ג). ראשית, כל תת־מודול $0\ne L\le F$ כולל איבר $0\ne\frac{a}{b}$, כאשר $a,b\in R$, ואיתו את הכפל שלו בסקרל b: $0\ne a=b\cdot\frac{a}{b}\in L$. כעת נניח ש־$F=R+L$, ויהי $0\ne a\in R\cap L$. אז $F=aF=a(R+L)=aR+aL=Ra+aL\subseteq L+L=L$; כלומר, אם $R+L=F$ אז $L=F$, ומכאן ש־R קטן.

[2] הצעה: נניח $R+L=F$, ויהי $0\ne b\in R$; הסבר מדוע $\frac{1}{tb}\in R+L$ והסק $\frac{1}{b}\in L$. כעת הוכח ש־$L=F$. נמק כל צעד.