تی. اس. بلایث – ای. اف. رابرتسون

جبر به روش تمرین

مجموعه‌ای از مسائل در جبر با حل

حلقه، میدان‌ها و مدول‌ها

ترجمه : دکتر حمید رضا میمنی

دانشگاه تربیت دبیر شهید رجائی

بسم الله الرحمن الرحیم

جبر به روش تمرین

مجموعه‌ای از مسائل در جبر با حل

حلقه، میدان‌ها و مدول‌ها

نوشتهٔ:

تی. اس. بلایث ـ ای. اف. رابرتسون

ترجمهٔ:

دکتر حمید رضا میمنی

دانشگاه تربیت دبیر شهید رجائی

بلایث، تامس اسکات Blyth, Thoms Scott
جبر به روش تمرین: مجموعه‌ای از مسائل در جبر با حل حلقه، (میدانها و مدولها) / نوشته‌ی تی. اس. بلایث، ای. اف. رابرتسون ؛ ترجمه حمید رضا میمنی، تهران: دانشگاه تربیت دبیر شهید رجائی، ۱۳۸۳.
۱۲۷ ص.: مصور.
۱۵۰۰۰ ریال ISBN: 964-95589-1-8
فهرست‌نویسی بر اساس اطلاعات فیپا.
عنوان اصلی Algebra through practice: a collection of problems in algebra with solutions
این کتاب در همین سال به صورت جلد منتشر شده است.
کتابنامه: ص. [۱۲۶] - ۱۲۷.
۱. جبر -- مسائل، تمرینها و غیره. الف. رابرتسون، ادموند Robertson, Edmund F.
ب. میمنی، حمید رضا، ۱۳۴۶ - ، مترجم. ج. دانشگاه تربیت دبیر شهید رجائی د. عنوان.
۲ ج ۸ ب / QA ۱۵۷ ۵۱۲/۰۰۷۶
الف ۱۳۸۳
کتابخانه ملی ایران ۲۳۶۰۸-۸۳م

جبر به روش تمرین

مجموعه‌ای از مسائل در جبر با حل

حلقه، میدانها و مدولها

تألیف: تی. اس. بلایث ـ ای. اف. رابرتسون

ترجمه: دکتر حمید رضا میمنی

ویراستار علمی: دکتر علی زعیم‌باشی

وزیری، ۱۲۸ صفحه، ۲۰۰۰ نسخه، چاپ اوّل، زمستان ۱۳۸۳

امور فنّی و چاپ: مؤسسهٔ چاپ و انتشارات دانشگاه فردوسی مشهد

بها: ۱۵۰۰۰ ریال

فهرست مطالب

پیش گفتار مولفین

هدف این سری از کتابهای حل مسئله ، ارائه یک دسته از مثالهای کار شده در جبر جهت پشتیبانی از درس جبر دوره کارشناسی است . در این تمرینات متنوع توجه ما معطوف به توانایی دانشجویان متوسط بوده ولی چند تمرین که ورزیدگی بیشتری برای حل آنها نیاز است گنجانده شده است . با وجود اینکه حل کامل مسائل ضمیمه است ولی خواننده بهتر است بعد از توجه کافی به سوالات به این جوابها رجوع کند . در این صورت است که امید می رود دانشجو به توانایی خود برای حل مسائل ، که ریاضیات چیزی جز آن نمی باشد ، اعتماد پیدا کند .

ترتیب مسائل در فصل ها بر حسب درجه بندی آنها نمی باشد . بنابراین اگر خواننده نتواند مسئله n ام را حل کند ، این دلیلی نمی باشد که از حل مسئله $(n+1)$ام نا امید شود .

تعدادی سوالات امتحانی (بدون حل) در انتهای کتاب ارائه شده است که این سوالات مبتنی بر مطالب مورد بحث کتاب است .

تی . اس . بلایث
ای. اف رابرتسون

فصل ۱

ایده الها

در این بخش اساساً روی ایده الهایی از هر دو حلقه تعویض پذیر و غیر تعویض پذیر تمرکز می کنیم . یک ایده ال (چپ ، راست و یا دو طرفه) I از حلقه R ماکسیمال است ، اگر تنها ایده ال (چپ ، راست و یا دو طرفه) محض R شامل I ، ایده آل I باشد . یک ایده ال I از R اول است ، اگر $I \neq R$ و $xy \in I$ ایجاب کند $x \in I$ یا $y \in I$ [1] . این مفاهیم برای توسعه تئوری حلقه ها و سوالاتی که مربوط به ایده هایی از قبیل پوچتوانی و شرایط زنجیره ای می باشند دارای اهمیت هستند . یک عنصر پوچ توان از حلقه R ، عنصر x از R است که برای $n \in N$ ای ، $x^n = 0$. یک حلقه (ایده ال) پوچتوان حلقه ای (ایده الی) است که هر عنصر آن پوچتوان باشد . یک حلقه R در شرط زنجیر صعودی روی ایده الهای (چپ ، راست ، دو طرفه) صدق می کند ، اگر برای هر زنجیر صعودی

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_n \subseteq I_{n+1} \subseteq \dots$$

از ایده الهای (چپ ، راست ، دوطرفه) ، عدد صحیح مثبتی مانند k موجود باشد به طوری که برای هر $n \geq k$ ، $I_n = I_k$. شرط زنجیر نزولی به صورت مشابه تعریف می شود .

۱- این تعریف در حلقه های جابجایی برقرار است و در حلقه های ناجابجایی تعریف دیگری ارائه می دهند . مترجم

۱-۱- فرض کنید R یک حلقه تعویض پذیر یکدار باشد . اگر I یک ایده ال R باشد ، ثابت کنید که

a) I اول است اگر و فقط اگر $\frac{R}{I}$ یک حوزه صحیح باشد ؛

b) I ماکسیمال است اگر و فقط اگر $\frac{R}{I}$ یک میدان باشد .

نتیجه بگیرید که هر ایده ال ماکسیمال ، اول است . مثالی از یک حلقه ارائه دهید که شامل یک ایده‌ال اول غیر ماکسیمال است .فرض کنید R یک حلقه غیر تعویض پذیر یکدار باشد . ثابت کنید اگر M ایده الی از R باشد به طوری که هر عنصر غیر صفر از $\frac{R}{M}$ وارون پذیر باشد ، آنگاه M یک ایده ال ماکسیمال است .

با در نظر گرفتن ایده آل

$$M = \left\{ \begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix} \middle| a, b, c, d \in Z \right\}$$

در حلقه $Mat_{2\times2}(Z)$ ، نشان دهید که عکس آن نادرست است .

۲-۱- ثابت کنید (8) یک ایده ال ماکسیمال حلقه $4Z$ است ، اما $\frac{4Z}{(8)}$ یک میدان نیست . توضیح دهید که چگونه این ممکن است .

۳-۱- حلقه بولی ، حلقه ای است یکدار که هر عنصرش خود توان (یعنی $x^2 = x$) است . ثابت کنید که یک حلقه بولی

a) از مشخصه 2 ؛

b) تعویض پذیر ؛

است .

اگر I یک ایده ال از حلقه بولی A باشد ، ثابت کنید که شرایط زیر هم ارزند :

(۱) I اول است ؛

(۲) $\frac{A}{I} \simeq \frac{Z}{2Z}$ ؛

۳) I ماکسیمال است .

۴-۱- فرض کنید F یک میدان و

$$J=\{f\in F[X,Y]\ |f(0,Y)=0\}.$$

ثابت کنید J یک ایده ال اصلی از $F[X,Y]$ است . آیا J اول است ؟ آیا J ماکسیمال است ؟

۵-۱- R را یک حلقه تعویض پذیر در نظر گرفته و فرض کنید A یک ایده ال از R باشد . قرار دهید

$$r(A)=\{\ x\in R|\ \ (\exists n\geq 1)\ x^n\in A\ \}\ .$$

اگر I و J ایده الهای R باشند ، ثابت کنید که

(a) $r(I+J)=r[r(I)+r(J)]\supseteq r(I)+r(J)$ ؛

(b) اگر به ازای $n\in N$ ای ، $I^n\subseteq J$ ، آنگاه $r(I)\subseteq r(J)$.

نشان دهید که اگر $r(I)=I$ ، آنگاه $\frac{R}{I}$ دارای عنصر پوچتوان غیر صفر نمی باشد .

آیا عکس مطلب برقرار است ؟ ثابت کنید که اگر P یک ایده ال اول از R باشد ، آنگاه $r(P)=P$.

۶-۱- اگر I و J ایده الهایی از حلقه تعویض پذیر R باشند ، تعریف کنید

$$(I:J)=\{\ x\in R\ |\ xJ\subseteq I\ \}$$

و ثابت کنید که برای ایده الهای I ، J ، K از R

(a) اگر $I\subseteq J$ ، آنگاه $(I:K)\subseteq(J:K)$ و $(K:I)\supseteq(K:J)$ ؛

(b) $(\forall n\in N)$ $\left(I:J^{n+1}\right)=\left(\left(I:J^n\right):J\right)=\left((I:J):J^n\right)$ ؛

(c) $(I:J)=R\Leftrightarrow J\subseteq I$ ؛

(d) $(I:J)=I:(I+J)$.

۷-۱- فرض کنید R یک حلقه تعویض پذیر یکدار باشد . ایده ال Q از R را اولیه گوئیم اگر $ab\in Q$ و $a\notin Q$ ، آنگاه برای $n\in N$ ای ، $b^n\in Q$.

ثابت کنید که ایده الهای اولیه حلقه Z دقیقاً توانی از ایده الهای اول هستند .

نشان دهید که ($4,X$) ایده ال اولیه ای از $Z[X]$ است . اما توانی از یک ایده ال اول $Z[X]$ نمی باشد .

با در نظر گرفتن مثال زیر همچنین نشان دهید که توانی از یک ایده ال اول لزوماً یک ایده ال اولیه نمی باشد . فرض کنید R زیر حلقه ای از $Z[X]$ باشد که تشکیل شده از چند جمله ایهایی که ضرایب X تقسیم پذیر به 3 می باشند . نشان دهید که $P=\left(3X,X^2,X^3\right)$ یک ایده ال اول از R است اما P^2 اولیه نیست .

۸-۱- فرض کنید F یک میدان باشد . ثابت کنید که در $F[X,Y,Z]$ ،

$$\left(Y^2Z^2,XYZ\right)=(Y)\cap(Z)\cap(X,Y)^2\cap(X,Z)^2.$$

آیا $\left(Y^2Z^2,XYZ\right)=(Y)(Z)(X,Y)^2(X,Z)^2$ درست است ؟ ادعای خود را ثابت کنید .

۹-۱- یک مجموعه را مرتب استقرایی گوئیم ، اگر هر زیر مجموعه غیر تهی کلاً مرتب آن دارای یک کران بالا باشد . اصل زرن می گوید که هر مجموعه مرتب استقرایی دارای عنصر ماکسیمال است .

فرض کنید A یک حلقه یکدار و $I\,(A)$ مجموعه ایده الهای A باشد . $I\in I(A)$ با $I\neq A$ داده شده است . تعریف کنید

$$F_I=\left\{J\in I(A)\;\middle|\;I\subseteq J\subset A\right\}$$

ثابت کنید F_I مرتب استقرایی است . با بکار بردن اصل زرن نتیجه بگیرید که هر ایده ال I از A که $I\neq A$ ، مشمول در یک ایده ال ماکسیمال از A است . در نتیجه نشان دهید که اگر A تعویض پذیر باشد ، آنگاه یک عنصر A یکه است اگر و فقط اگر به هیچکدام از ایده ال های ماکسیمال A تعلق نداشته باشد .

۱۰-۱- اگر F یک میدان باشد ، ثابت کنید که حلقه $Mat_{n\times n}(F)$ در هر دو شرط زنجیر روی ایده الهای راست و ایده الهای چپ صدق می کند .

زیر حلقه

$$R=\left\{\begin{bmatrix}\alpha & 0\\ \beta & 0\end{bmatrix} \,\middle|\; \alpha\in R\right\}$$

از حلقه $Mat_{2\times2}(\ R\ )$ را در نظر بگیرید . ثابت کنید که هر ایده ال محض راست R به صورت $\left\{\alpha\begin{bmatrix}x & 0\\ y & 0\end{bmatrix} \,\middle|\; \alpha\in R\right\}$ است که در آن x و y دو عنصر ثابت R می باشند .

نشان دهید که R در هر دو شرط زنجیر روی ایده الهای راست صدق می کند . اما در هیچکدام از شرطهای زنجیر از ایده الهای چپ صدق نمی کند .

۱-۱۱- عنصر x از حلقه R را شبه منظم راست گوئیم ، اگر $y\in R$ ای موجود باشدکه $x+y+xy=0$. ثابت کنید که $x\in R$ شبه منظم راست است اگر و فقط اگر مجموعه $\{r+xr|r\in R\}$ برابر با R باشد .

فرض کنید R یکدار باشد . ثابت کنید که اگر x متعلق به هر ایده ال ماکسیمال راست R باشد ، آنگاه برای هر $r\in R$ عنصر xr منظم راست است . همچنین نشان دهید که اگر M یک ایده ال راست ماکسیمال از R باشد و $x\notin M$ ، آنگاه به ازای $m\in M$ ای و $r\in R$ ای ، $-1=m+xr$. نتیجه بگیرید که اشتراک ایده الهای راست ماکسیمال از R شامل آن دسته از عناصر $x\in R$ است که برای هر $r\in R$ ، xr یک شبه منظم راست است .

۱-۱۲- فرض کنید R یک حلقه و S یک زیر حلقه از R باشد . فرض کنید به ازای $i\in N$ ای ، $R^i=S^i+R^{i+1}$. ثابت کنید که برای کلیه $j\geq i$ ، $R^j=S^j+R^{j+1}$ و نتیجه بگیرید که برای همه $j,k\in N$ با $j\geq i$ ، $R^j=S^j+R^{j+k}$.

حال فرض کنید R پوچتوان باشد ، نتیجه بگیرید که

(a) اگر S یک زیر حلقه R باشد که به ازای $i\in N$ ای ، $R^i=S^i+R^{i+1}$ ، آنگاه برای همه $j\geq i$ ، $R^j=S^j$ ؛

(b) اگر $\dfrac{R}{R^2}$ با یک عنصر تولید شود ، آنگاه R نیز چنین است ؛

(c) اگر M یک ایده ال ماکسیمال از R باشد ، آنگاه $R^2\subseteq M$ ؛

(d) اگر M یک ایده ال ماکسیمال از R باشد ، آنگاه تعداد عنصرهای $\frac{R}{M}$ یک عدد اول است .

۱-۱۳- حلقه R را حلقه پوچ می گوئیم ، اگر هر عنصر R پوچتوان باشد .
ثابت کنید که هر زیر حلقه و هر حلقه خارج قسمتی از یک حلقه پوچ ، یک حلقه پوچ است.

سپس ثابت کنید که اگر A یک ایده ال دو طرفه از حلقه B باشد به طوری که A و $\frac{B}{A}$ حلقه‌های پوچ باشند ، آنگاه B نیز یک حلقه پوچ است . نتیجه بگیرید که حاصل جمع دو ایده ال پوچ دو طرفه از یک حلقه ، یک ایده ال پوچ دو طرفه است .

فرض کنید R_p مجموعه دنباله های نامتناهی $a_1,a_2,a_3,\ldots$ باشد جائیکه هر $a_i \in Z_{p^i}$ و بجز تعداد متناهی i ، $a_i = 0$. R_p تشکیل یک حلقه تحت جمع و ضرب مولفه ای می دهد . همه عنصرهای پوچتوان R_p را پیدا کنید . ثابت کنید که این مجموعه از عنصرهای پوچتوان یک ایده ال پوچ دو طرفه است که ایده ال پوچتوان نمی باشد .

۱-۱۴- *(a)* A_1 را یک ایده ال از حلقه A_2 بگیرید . فرض کنید که I یک ایده ال از A_1 و J کوچکترین ایده ال A_2 شامل I باشد . ثابت کنید که $J^3 \subseteq I$.

(b) فرض کنید R یک حلقه باشد . زیر حلقه I از R را یک زیر ایده ال می نامیم ، اگر یک زنجیر

$$I = A_\circ \subseteq A_1 \subseteq A_2 \subseteq \ldots \subseteq A_n = R$$

موجود باشد که در آن برای $i = 1,2,\ldots,n$ هر A_{i-1} یک ایده ال از A_i می باشد . ثابت کنید که اگر I یک زیر ایده ال از R و $\bar{I}$ کوچکترین ایده ال از R شامل I باشد ، آنگاه $\bar{I}^{3n} \subset I$.

(c) از قسمت قبل نتیجه بگیرید که اگر یک زیر ایده ال I از حلقه R پوچتوان باشد ، آنگاه کوچکترین ایده ال شامل I از R پوچتوان است .

۱-۱۵- ایده ال Q از حلقه R را شبه اول گوئیم ، اگر برای هر ایده ال A از R که $A^2 \subseteq Q$ ، آنگاه $A \subseteq Q$.

ثابت کنید که اگر Q یک ایده ال شبه اول و A یک ایده ال از R باشند به طوری که به ازای $n \in N$ ای ، $A^n \subseteq Q$ ، آنگاه $A \subseteq Q$.

فرض کنید Q شبه اول و X یک ایده ال پوچتوان از $\frac{R}{Q}$ باشد . اگر Y نگاره معکوس X تحت ریختار طبیعی $\varphi : R \to \frac{R}{Q}$ باشد . ثابت کنید که $Y \subseteq Q$ و نتیجه بگیرید که $\frac{R}{Q}$ شامل هیچ ایده ال پوچتوان غیر صفر نمی باشد .

به عکس نشان دهید که اگر Q یک ایده ال از $\frac{R}{Q}$ باشد به طوری که شامل هیچ ایده ال پوچتوان غیر صفر نباشد ، آنگاه Q شبه اول است .

فصل ۲

بخش پذیری

اینجا تمرکز اصلی ما مبتنی بر مفهوم تقسیم پذیری در حوزه های صحیح می باشد . اگر R یک حوزه صحیح باشد و $x \in R$ عنصر $y \in R$ را عاد کند (یعنی $z \in R$ ای وجود داشته باشد به طوری که $y = xz$) ، آنگاه می نویسیم $x|y$.

اگر $x|y$ و $y|x$ ، آنگاه x و y را شریک گوئیم . شریک های 1 را یکه می نامیم ، آنها تشکیل یک گروه تحت ضرب R می دهند . برای مثال یکه های $Z[\sqrt{n}]$ عنصرهای با اندازه ± 1 می باشند جائیکه اندازه $a + b\sqrt{n}$ به صورت $\ell(a + b\sqrt{n}) = a^2 - nb^2$ تعریف می شود .

مفهوم معمولی اعداد صحیح اول در حوزه صحیح دلخواه به دو مفهوم مجزای عنصر تحویل ناپذیر و عنصر اول گسترش پیدا می کند . عنصر x تحویل ناپذیر است ، اگر صفر و یکه نباشد و تنها مقسوم علیه هایش شریک های آن یا یکه ها باشند . x را اول گوئیم ، اگر صفر و یکه نباشد و اگر یک حاصلضربی را عاد کند ، آنگاه یکی از عاملها را عاد کند . این دو مفهوم در حوزه های ایده ال اصلی (هر حوزه صحیحی که هر ایده ال آن اصلی باشد) بر هم منطبق می باشند .

در ارتباط با ایده تقسیم پذیری ، بزرگترین عامل مشترک ($h.c.f.$) یا بزرگترین مقسوم علیه مشترک ($g.c.d.$) و کوچکترین مضرب مشترک ($\ell.c.m.$) تعریف می شود در حالت کلی

وجود اینها لازم نیست . اما در حوزه های اقلیدسی (حوزه صحیح D با تابع $N : D\setminus\{0\} \to \mathbb{N}$ که تابع نرم نامیده می شود به طوری که اگر $b|a$ ، آنگاه $N(b) \le N(a)$ و اگر $b \neq 0$ و a ، آنگاه $a = bq + r$ جائیکه $r=0$ یا $(N(r) < N(b))$ مهم هستند .

۱-۲- فرض کنید x ، y ، u عنصرهای حوزه صحیح R باشند . ثابت کنید که

(a) $x|y$ اگر و فقط اگر $(y) \subseteq (x)$ ؛

(b) x و y شریک هستند اگر و فقط اگر $(x) = (y)$ ؛

(c) u یکه است اگر و فقط اگر $(u) = R$ ؛

(d) y یک عامل سره است اگر و تنها اگر $(x) \subset (y) \subset R$ ؛

(e) x تحویل ناپذیر است اگر و فقط اگر (x) در میان ایده الهای اصلی R ماکسیمال باشد .

۲-۲- در گزاره ها ی زیر R یک حوزه صحیح است و $R^* = R - \{0\}$. برای هر گزاره درست دلیل بیاورید و برای هر گزاره نادرست یک مثال نقض بزنید .

(a) اگر یک رابطه هم ارزی روی R^* باشد، آنگاه R میدان است ؛

(b) اگر برای همه x و y در R^* ، $x\sim y$ ، آنگاه R میدان است ؛

(c) اگر $a\sim b$ و $c\sim d$ ، آنگاه $ac\sim bd$ ؛

(d) اگر $a\sim b$ و $c\sim d$ ، آنگاه $(a+c) \sim (b+d)$ ؛

(e) اگر هر عنصر R^* یکه یا اول باشد ، آنگاه R میدان است .

۳-۲- تعیین کنید که آیا 5 در هر یک از حلقه های

$$Z \text{ ، } Z[X] \text{ ، } Z[i] \text{ ، } Z[\sqrt{-2}]$$

تحویل ناپذیر است .

۴-۲- $43i - 19$ را به صورت حاصلضرب تحویل ناپذیرها در $Z[i]$ بنویسید .

۵-۲- عناصر زیر را به صورت حاصلضرب عوامل تحویل ناپذیر نمایش دهید .

(a) $11+7\sqrt{-1}$ در $Z[\sqrt{-1}]$ ؛

(b) $4+7\sqrt{2}$ در $Z[\sqrt{2}]$ ؛

(c) $4-\sqrt{-3}$ در $Z[\sqrt{-3}]$.

۲-۶- (a) آیا $\sqrt{6}\times\sqrt{6}=3.2$ یکتایی تجزیه را در $Z[\sqrt{6}]$ نقض می کند ؟

(b) نشان دهید $Z[\sqrt{10}]$ یک دامنه تجزیه یکتا می باشد .

۲-۷- با پیدا کردن دو تجزیه متفاوت از 10 ، ثابت کنید که $Z[\sqrt{-6}]$ دامنه تجزیه یکتا نیست .

برای هر عبارت زیر مثالی در $Z[\sqrt{-6}]$ بزنید و ادعای خود را ثابت کنید ،

(a) یک عنصر تحویل ناپذیر که اول نباشد ؛

(b) عنصرهای غیر صفر a و b وجود دارد به طوری که $g.c.d.(a,b)$ وجود ندارد ؛

(c) عنصرهای غیر صفر a و b وجود دارد که $g.c.d.(a,b)=1$ ، اما α و β در $Z[\sqrt{-6}]$ موجود نمی باشد به طوری که $\alpha a+\beta b=1$.

۲-۸- ثابت کنید در $Z[\sqrt{-7}]$ عنصر 8 را هم می توان به صورت حاصلضرب دو عنصر تحویل ناپذیر و هم به صورت حاصلضرب سه عنصر تحویل ناپذیر نوشت . نتیجه بگیرید که برای هر عدد صحیح مثبت k یک عضو از $Z[\sqrt{-7}]$ وجود دارد که می‌توان آن را به صورت حاصلضربی از $t+1, t+2, \ldots, t+k$ ، از عنصرهای تحویل ناپذیر برای $t\in N$ ای نوشت .

مثالی از یک عنصر تحویل ناپذیر در $Z[\sqrt{-7}]$ ارائه دهید که اول نباشد . مثالی از عنصرهای α و β در $Z[\sqrt{-7}]$ ارائه دهید به طوری که $g.c.d.(\alpha,\beta)=1$ ، اما عنصرهای δ و γ با $\gamma\alpha+\delta\beta=1$ در $Z[\sqrt{-7}]$ وجود ندارد . ادعای خود را ثابت کنید.

۲-۹- اگر I یک ایده ال غیر صفر از $Z[i]$ باشد ، با استفاده از این واقعیت که I اصلی بوده و با استفاده از الگوریتم اقلیدسی ، نشان دهید که $\dfrac{Z[i]}{I}$ دارای تعداد متناهی عنصر می باشد .

۲-۱۰- فرض کنید $\alpha\in Z[i]$ اول باشد . ثابت کنید دقیقاً یکی از گزاره های زیر درست است ،

$(a$ $\alpha \sim 1+i$ ؛

$(b$ $\alpha \in Z$ اول است و $\alpha \equiv 3$ (هنگ 4) ؛

$(c$ α عدد اول $p \in Z$ که $p \equiv 1$ (هنگ 4) را عاد می کند .

۲-۱۱- برای یک دامنه مربعی $Z[\sqrt{n}]$ که n یک مربع آزاد است ، ثابت کنید که

$(a$ اگر $n < -1$ ، آنگاه گروه یکه های $Z[\sqrt{n}]$ برابر با $\{1,-1\}$ است ؛

$(b$ اگر $n > 1$ و گروه یکه های $Z[\sqrt{n}]$ بیش از دو عنصر داشته باشد ، آنگاه نامتناهی است ؛

$(c$ گروه یکه های $Z[\sqrt{2}]$ ، $\left\{ \pm\left(1+\sqrt{2}\right)^k \middle| k \geq 1 \right\}$ است .

۲-۱۲- فرض کنید $p \in Z$ اول باشد . زیر حلقه از Q که به صورت زیر داده شده است را در نظر بگیرید

$$R = \{ \frac{m}{n} | m, n \in Z, n \neq 0 \text{ و } \text{عدد p را عاد نمی کند n} \}$$

ثابت کنید که هر ایده ال حلقه R اصلی است و R شامل یک ایده ال ماکسیمال یکتا است .

۲-۱۳- فرض کنید D یک دامنه ایده ال اصلی باشد . ثابت کنید که

$(a$ اگر $\{0\}$ \ y_1 ،...، $y_n \in D$ ، x موجود باشند به طوری که برای هر i ، x و y_i نسبت به هم اول باشند ، آنگاه x و $y_1 y_2 \dots y_n$ نیز نسبت به هم اول می باشند ؛

$(b$ اگر p_1 ، p_2 ، ... ، p_n عناصری تحویل ناپذیر از D باشند به طوری که هیچ زوجی از آنها شریک نباشند ، آنگاه برای همه اعداد صحیح مثبت r_n ، ... ، r_2 ، r_1 عنصرهای $p_1^{r_1}$ ، $p_2^{r_2}$ ،...، $p_n^{r_n}$ دو بدو نسبت به هم اول هستند .

بنابراین نشان دهید که اگر F میدان خارج قسمتی D باشد و $x = \frac{a}{b} \in F$ که در آن $b = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n}$ تجزیه یکتایی از حاصلضرب تحویل ناپذیرها باشد که هیچ دو p_i متفاوتی شریک نباشند ، آنگاه a_1 ،...، $a_n \in D$ وجود دارد به طوری که

$$x=\frac{a_1}{p_1^{r_1}}+\ldots+\frac{a_n}{p_n^{r_n}}\ .$$

۱۴-۲- اگر A یک حلقه تعویض پذیر یکدار باشد ، آنگاه A

(a) را نوتری گوئیم ، اگر هر زنجیر صعودی از ایده الهای A ایستا باشد ،

(b) در شرط ماکسیمم صدق می کند ، اگر هر خانواده از ایده الهای A دارای عنصر ماکسیمال باشد.

ثابت کنید که عبارتهای زیر معادلند :

(۱) A نوتری است ؛

(۲) A در شرط ماکسیمم صدق می کند ؛

(۳) هر ایده ال A متناهی - مولد است .

نتیجه بگیرید که اگر A یک دامنه صحیح باشد ، آنگاه عبارتهای زیر معادلند

(α) A دامنه ایده ال اصلی است ؛

(β) A نوتری است و مجموع هر دو ایده ال اصلی یک ایده ال اصلی است .

۱۵-۲- اگر R دامنه اقلیدسی با نرم N باشد ، ثابت کنید که

(a) اگر $a|b$ و $N(a)=N(b)$ ، آنگاه a و b شریک هستند ؛

(b) اگر a و b عنصرهای غیر صفر از R باشند که هیچ کدام دیگری را عاد نکند، آنگاه $\alpha,\beta,d\in R$ وجود دارد که $a\alpha+b\beta=d$ و $N(d)<\min(N(a),N(b))$.

۱۶-۲- ثابت کنید که در تعریف نرم اقلیدسی δ خارج قسمتها و باقیمانده ها منحصر به فرد هستند، اگر و فقط اگر $\delta(a+b)\le\max(\delta(a),\delta(b))$.

مثالی در $Z[i]$ ارائه دهید که خارج قسمتها و باقیمانده ها منحصر به فرد نباشد .

۱۷-۲-(a) $-1+3i$ را به صورت حاصلضرب عنصرهای اول در $Z[i]$ بنویسید ،

(b) فرض کنید R دامنه تجزیه یکتایی باشد و قرار دهید

$$f(X) = a_\circ + a_1X + a_2X^2 + \dots + a_nX^n \in R[X]$$

به طوری که $g.c.d.(a_\circ, \dots, a_n) = 1$. فرض کنید عنصر اول $p \in R$ وجود دارد که برای $i=0, 1, \dots, n-1$، $p|a_i$، $p^2 \nmid a_\circ$ و $p \nmid a_n$. ثابت کنید که $f(X)$ در $R[X]$ تحویل ناپذیر است.

(c) از (a) و (b) نتیجه بگیرید که

$$X^3 + 8iX^2 - 6X - 1 + 3i$$

در $Z[i][X]$ تحویل ناپذیر است.

۱۸-۲- آیا هر زوج از عنصرهای غیر صفر $Z[\sqrt{3}]$ دارای بزرگترین مقسوم علیه مشترک است؟ بزرگترین مقسوم علیه مشترک 13 و $7 + 5\sqrt{3}$ را پیدا کنید.

۱۹-۲- در حلقه $Z[\sqrt{-5}]$ ثابت کنید که

(a) یکه ها 1 و -1 هستند؛

(b) 3 و $2 + \sqrt{-5}$ و $2 - \sqrt{-5}$ تحویل ناپذیر هستند؛

(c) 9 دارای دو تجزیه متفاوت از حاصلضرب تحویل ناپذیر ها می باشند؛

(d) ایده الهای $(3, 2 + \sqrt{-5})$ و $(3, 2 - \sqrt{-5})$ اول هستند؛

(e) اگر چه 3 تحویل ناپذیر است، اما ایده ال (3) را می توان به صورت حاصلضربی از ایده الهای اول نمایش داد.

۲۰-۲- ایده الهای زیر را در $Z[10]$ در نظر بگیرید

$$P_1 = (2, \sqrt{10}) ، P_2 = (3, 4 + \sqrt{10}) ، P_3 = (3, 4 - \sqrt{10}).$$

نشان دهید که این ایده الها اول هستند. ثابت کنید دو تجزیه به عوامل اول

$$6 = 2.3 = (4 + \sqrt{10})(4 - \sqrt{10})$$

تجزیه یکسان از (6) را به حاصلضربهایی از ایده الهای اول P_1، P_2 و P_3 بدست می دهد.

فصل ۳

میدانها

این بخش اساساً مربوط به مفهوم توسیع یک میدان می باشد . یعنی نشاندن یک میدان در یک میدان دیگر . اگر K یک توسیع از F باشد ، آنگاه K را می توان به عنوان یک فضای برداری روی میدان F در نظر گرفت . بعد این فضای برداری را درجه توسیع می نامیم و به صورت $[K:F]$ نمایش می دهیم . وقتی درجه متناهی باشد توسیع را متناهی گوئیم . یک عنصر a از K را روی F جبری گوئیم ، اگر به ازای $P(X)\in F[X]$ ای ، $P(a)=0$. چند جمله ای تکین از کوچکترین درجه با این خاصیت را چند جملهای مینیمال a می نامیم . توسیع K از F را جبری گوئیم ، اگر هر عنصر K روی F جبری باشد . در غیر این صورت K را متعالی یا غیر جبری گوئیم.

وقتی که K توسیع میدان F و $a_1،a_2،\ldots،a_n\in K$ ما از علامت (متعارف) $F(a_1,a_2,\ldots,a_n)$ برای نمایش کوچکترین زیر میدان K که شامل $F\cup\{a_1,\ldots,a_n\}$ می باشد استفاده می کنیم . در حالت خاص $F(a)$ را توسیع ساده F می نامیم . میدان F را میدان شکافنده برای $f(x)\in F[x]$ می نامیم ، اگر K توسیع F از کوچکترین درجه باشد که f را بتوان به صورت حاصلضربی از عاملهای خطی نمایش داد . K را توسیع نرمال F می نامیم ، اگر میدان شکافنده بعضی از چند جمله ایهای $f(x)\in F[x]$ باشد .

در پایان ، فرض می کنیم خواننده با جملات قضیه اساسی تئوری گالوا که ارتباط زیر گروههای گروه گالوای $Gal(K,F)$ ، با زیر میدانهای K شامل F را به دست می دهد آشنایی دارد .

۱-۳- فرض کنید F میدانی با مشخصه p باشد . ثابت کنید که

$$(\forall a,b\in F)\ \ (a\pm b)^p=a^p\pm b^p\ .$$

بنابراین با استقرا نتیجه بگیرید که برای هر عدد صحیح مثبت n

$$(\forall a,b\in F)\ \ (a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}\ .$$

۲-۳- فرض کنید F یک میدان و $D:F[X]\to F[X]$ نگاشت مشتق توصیف شده با

$$D\left(a_\circ+a_1X+a_2X^2+\ldots+a_nX^n\right)=a_1+2a_2X+\ldots+na_nX^{n-1}$$

باشد . اگر F از مشخصه صفر باشد ، ثابت کنید که $Df=0$ اگر و فقط اگر f چند جمله ای ثابت باشد . اگر F از مشخصه p باشد ، ثابت کنید که $Df=0$ اگر و فقط اگر f به صورت

$$a_\circ+a_pX^p+\ldots+a_{rp}X^{rp}$$

باشد .

۳-۳- اگر F یک میدان باشد ، ثابت کنید یکه های $F[X]$ چند جمله ایهای ثابت غیر صفر هستند .

فرض کنید $i:F\to F[X]$ نگاشت یک به یک کانونی باشد . ثابت کنید که اگر $\varphi:F[X]\to F[X]$ یک خود ریختی باشد ، آنگاه یک خود ریختی $v:F\to F$ وجود دارد به طوری که نمودار

$$\begin{tikzcd}
F \arrow[r, "i"] \arrow[d, "v"'] & F[X] \arrow[d, "\varphi"] \\
F \arrow[r, "i"'] & F[X]
\end{tikzcd}$$

تعویض پذیر است (بدین معنی که $\varphi\circ i=i\circ v$) . نتیجه بگیرید که $a,b\in F$ با $a\neq 0$ وجود دارد به طوری که $\varphi(X)=aX+b$.

۳-٤- فرض کنید F یک میدان باشد . $f \text{،} g \in F[X]$ داده شده است. f و g را هم ارز گوئیم، اگر به ازای هر $\alpha \in F$ ، $f(\alpha) = g(\alpha)$. اگر F نامتناهی باشد ، ثابت کنید f و g هم ارزند اگر و فقط اگر f=g. اگر F متناهی باشد ، برای مثال $F = \{a_1, a_2, ..., a_n\}$ ، ثابت کنید f و g هم ارزند اگر و فقط اگر چند جمله ای

$$m(X) = (X - a_1)(X - a_2)...(X - a_n)$$

f-g را عاد کند . در حالتی که $F = GF(p) = \frac{Z}{pZ}$ ، نشان دهید $m(X) = X^p - X$.

۳-۵- اگر F میدانی با مشخصه مخالف 2 باشد ، ثابت کنید که $X^2 - Y^2 - 1$ در $F[X,Y]$ تحویل ناپذیر است .

۳-۶- با در نظر گرفتن ریختار حلقه ای $Z[X] \to Z_n[X]$ که بوسیله ریختار طبیعی $Z \to Z_n$ القا شده است ، نشان دهید که اگر f روی Z_n تحویل ناپذیر باشد ، آنگاه روی Z تحویل ناپذیر است .

با در نظر گرفتن n=5 نشان دهید که اگر $f(X) = X^4 + 15X^3 + 7$ ، آنگاه f روی Q تحویل ناپذیر است .

۳-۷- یک پایه برای $Q(\sqrt{2}, \sqrt[3]{2})$ روی Q مشخص کنید . نتیجه بگیرید که $\sqrt[6]{2} \in Q(\sqrt{2}, \sqrt[3]{2})$. بنابراین نشان دهید که $Q(\sqrt{2}, \sqrt[3]{2})$ یک توسیع ساده از Q است.

۳-۸- فرض کنید F یک میدان باشد و

$$Z = \frac{X^3}{X+1} \in F(X)$$

را در نظر بگیرید . ثابت کنید Z روی F متعالی است اما F(X) یک توسیع جبری ساده از F(Z) است . چند جمله ای مینیمال X روی F(Z) چیست ؟

۳-۹- نشان دهید X^2-3 و X^2-2X-2 هر دو روی Q تحویل ناپذیرند و دارای میدان شکافنده یکسان می باشند.

۳-۱۰- نشان دهید $(X^2-2X-2)(X^2+1)$ و $X^5-3X^3+X^2-3$ دارای میدان شکافنده یکسان K روی Q می باشند و $[K:Q]$ را پیدا کنید.

۳-۱۱- فرض کنید K یک میدان و $a,b\in K$. ثابت کنید که $X+a+b$ در حلقه $K[X]$، $X^3-3abX+a^3+b^3$ را عاد می کند و $q(X)\in K[X]$ را طوری تعیین کنید که

$$X^3-3abX+a^3+b^3=(X+a+b)q(X).$$

یک میدان شکافنده، S، برای X^6-6X^3+8 روی Q ارائه دهید.

درجه S روی Q چیست؟ نشان دهید S شامل عنصر $\sqrt[3]{4}+\sqrt[3]{2}$ است. چند جمله ای مینیمال این عنصر را روی Q پیدا کنید.

آیا این مطلب که $Q\left(\sqrt[3]{4}+\sqrt[2]{3}\right)$ میدان شکافنده ای برای X^6-6X^3+8 درست است؟

۳-۱۲- عاملهای درجه دوم برای $f(X)=X^4+2X^3-8X^2-6X-1$ در $Q[X]$ را پیدا کنید و سپس نشان دهید $Q\left(\sqrt{2},\sqrt{3}\right)$ میدان شکافنده برای f روی Q است. نشان دهید $\sqrt{3}\notin Q\left(\sqrt{2}\right)$. نتیجه بگیرید که $[Q(\sqrt{2},\sqrt{3}):Q]=4$ و یک پایه برای $Q\left(\sqrt{2},\sqrt{3}\right)$ روی Q پیدا کنید.

ثابت کنید $Q\left(\sqrt{2},\sqrt{3}\right)=Q\left(\sqrt{3}-\sqrt{2}\right)$ و چند جمله ای مینیمال $\sqrt{3}-\sqrt{2}$ روی $Q\left(\sqrt{3}\right)$ را پیدا کنید.

۳-۱۳- عاملهای تحویل ناپذیر $f(X)=X^4-X^2-2$ را در $Q[X]$ پیدا کنید. نشان دهید که $Q\left(i,\sqrt{2}\right)$ یک میدان شکافنده f روی Q است. همچنین نشان دهید که $\left(Q\left(i,\sqrt{2}\right):Q\right)=4$ و یک پایه برای $Q\left(i,\sqrt{2}\right)$ روی Q بنویسید. چند جمله ای مینیمال $i+\sqrt{2}$ روی Q را پیدا کنید.

نتیجه بگیرید که $Q(i,\sqrt{2})=Q(i+\sqrt{2})$ و ثابت کنید که $(Q(i,\sqrt{2}):Q)=4$. توجه داشته باشید که $Q(i)$ ، $Q(\sqrt{2})$ و $Q(i\sqrt{2})$ کلیه زیر میدانهای $Q(i+\sqrt{2})$ هستند که روی آنها از درجه 2 می باشند . چند جمله ای مینیمال $i+\sqrt{2}$ را روی هر یک از میدانهای

a) $Q(i)$ ؛

b) $Q(\sqrt{2})$ ؛

c) $Q(i\sqrt{2})$ ؛

پیدا کنید .

۳-۱٤- $r\in Q$ داده شده است . چند جمله ای $f(X)=X^4+r\in Q[X]$ را در نظر بگیرید . ثابت کنید که گزاره های زیر هم ارزند

(۱) f تحویل پذیر است ؛

(۲) f دارای عامل درجه دوم است ؛

(۳) یا $r=-p^2$ $(p\in Q)$ یا $r=\frac{1}{4}q^4$ $(q\in Q)$.

حال فرض کنید f روی Q تحویل ناپذیر باشد . فرض کنید $\xi\in C$ یک ریشه f بوده و قرار دهید $K=Q(\xi)$. ثابت کنید که

a) اگر $\sqrt{r}\in Q$ ، آنگاه $Q(\xi^2)$ تنها زیر میدان K به غیر از K و Q است ؛

b) اگر $\sqrt{r}\in Q$ ، آنگاه $Q(\xi^2)$ ، $Q(\sqrt{r}\xi+\xi^2)$ و $Q(-\sqrt{r}\xi+\xi^3)$ تنها زیر میدانهای K به غیر از K و Q می باشند .

۳-۱۵- مرتبه گروه گالوا $Q(\omega)$ روی Q را تعیین کنید وقتی که

a) $\omega=e^{\frac{2\pi i}{5}}$ ؛

b) $\omega=\sqrt[3]{2}$.

۱۶-۳- میدان شکافنده برای چند جمله ای $X^4 - 2$ روی Q را پیدا کنید. نشان دهید که گروه گالوای $X^4 - 2$ غیر آبلی و از مرتبه 8 است.

۱۷-۳- یک زیر میدان از C که میدان شکافنده روی Q برای چند جمله ای $X^3 - 2$ باشد را تعیین کنید. گروه گالوای این چند جمله ای رابسازید و زیر میدانهای، میدان شکافنده را مشخص کنید.

۱۸-۳- نشان دهید که اگر α ریشه $X^3 - 3X + 1 = 0$ باشد، آنگاه $\alpha^2 - 2$ و $2 - \alpha - \alpha^2$ ریشه های دیگر آن می باشند.
فرض کنید $f(X) = X^3 - 3X + 1$. نشان دهید که $Q(\alpha)$ یک میدان شکافنده برای f روی Q است و $[Q(\alpha):\alpha]$ را پیدا کنید.
نشان دهید که تنها یک Q- خود ریختی v از $Q(\alpha)$ با $v(\alpha) = \alpha^2 - 2$ وجود دارد و $Gal(Q(\alpha), Q)$ را تعیین کنید. آیا هر جایگشت از ریشه های f قابل توسیع به یک عنصر از $Gal(Q(\alpha), Q)$ می باشد؟

۱۹-۳- تعیین کنید که کدامیک از توسیعهای زیر از Q نرمال هستند،

a) $Q(\sqrt{2})$؛
b) $Q(\sqrt[3]{2})$؛
c) $Q(\sqrt[4]{2})$؛
d) $Q(\sqrt[5]{2})$.

۲۰-۳- فرض کنید E یک میدان از مشخصه صفر بوده و $K = E(X_1, X_2, \dots, X_n)$ میدان توابع گویای n متغیره روی E باشد. چند جمله ای متقارن مقدماتی در $X_1, \dots, X_n$ به صورت

$$\sigma_1 = \sum_{i=1}^{n} X_i \;،\; \sigma_2 = \sum_{i \neq j} X_i X_j \;،\dots،\; \sigma_n = X_1 X_2 \dots X_n .$$

فرض کنید $F = E(\sigma_1, \sigma_2, \dots, \sigma_n)$ و

$$f(X)=X^n-\sigma_1X^{n-1}+\sigma_2X^{n-2}-\ldots+(-1)^n\sigma_n\in F[X].$$

ثابت کنید که

a) K یک میدان شکافنده برای f روی F می باشد ؛

b) گروه گالوای K روی F یکریخت با گروه متقارن از درجه n است ؛

c) $(K:F)=n!$.

فصل ٤

مدولها

ساده ترین راه برای تعریف مدول آن است که بگوئیم مدول یک دستگاه جبری است که در اصول مشابه فضای برداری صدق می کند ، بجز اینکه اسکالرها در یک حلقه یکدار بجای یک میدان F قرار دارد . این تعمیم بظاهر نسبتاً کم به یک ساختار جبری بسیار مهم منتهی می شود . در اینجا از جمله R- مدول برای فهماندن اینکه اسکالرها در سمت چپ نوشته می شوند استفاده می کنیم .

مشابه با گروه ها و حلقه ها ، زیر ساختارها (زیر مدولها) و نگاشتهای حافظ ساختار (R- ریختی ها) دارای اهمیت خاصی بوده ، همانطور که ساختارهای جدیدی که از ساختارهای قدیم از قبیل مدولهای خارج قسمتی ، حاصلضرب دکارتی (یا مستقیم) و مجموع مستقیم ، بدست می آیند مورد علاقه خاص می باشند . ما فرض می کنیم خواننده با قضیه تناظر و قضایای اساسی یکریختی آشنایی دارد . اگر M و N دو R- مدول باشند ، آنگاه مجموعه R- ریختی های $f:M\to N$ تشکیل گروه آبلی جمعی (یک Z- مدول) می دهند که با $Mor_R(M,N)$ یا $Hom_R(M,N)$ نشان می‌دهیم. بعضی از نویسندگان به صورت درحالت N=M با $End_R(M)$ نمایش می دهند .

قسمتی از مباحث شامل دنباله های دقیق (تصویر R- ریختی ورودی برابر با هسته R- ریختی خروجی است) نمودارهای تعویض پذیر (ترکیب همه R- ریختی‌های تعریف شده از یک R- مدول به R- مدول دیگر برابر هستند) ، شرطهای زنجیره ای (با توجه به حلقه ها در بخش یک) و سری جردن- هولدر از زیر مدولها (برای مثال سریهای ترکیبی در گروه ها) می باشد . همچنین از نمادهای R- مدول آزاد (آن دسته از مدولها که دارای پایه هستند) و R- مدول تصویری (که یک جمع مستقیم از R- مدولهای آزاد می باشند) استفاده می کنیم .

۱-٤- فرض کنید M یک گروه آبلی و EndM حلقه درون ریختی های روی M (یعنی گروه ریختار های $f: M \to M$ با عملهای جمع و ترکیب) باشد . ثابت کنید M یک (EndM)- مدول با قانون خارجی $EndM \times M \to M$ توصیف شده بوسیله $(f,m) \to fm = f(m)$ می باشد .

۲-٤- فرض کنید R حلقه یکدار و M یک گروه آبلی باشد . ثابت کنید M یک R- مدول است اگر و فقط اگر یک ریختار حلقه ای $\mu : R \to EndM$ که M را به EndM می برد موجود باشد .

۳-٤- ثابت کنید که حلقه درون ریختی های گروه آبلی Z یکریخت با حلقه Z است و حلقه درون ریختی های گروه آبلی Qیکریخت با میدان Q است .

٤-٤- فرض کنید R حلقه تعویض پذیر یکدار و $f: R\times R \to R$ یک نگاشت باشد . ثابت کنید f یک R- ریختی است اگر و فقط اگر $\alpha, \beta \in R$ وجود داشته باشد به طوری که

$$f(x,y) = \alpha x + \beta y \qquad (\forall x, y \in R)$$

۵-٤- فرض کنید $Z[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in Z\}$ و نگاشت $f: Z[\sqrt{2}] \to Z[\sqrt{2}]$ ارائه شده با $f(a+b\sqrt{2}) = a+b$ را در نظر بگیرید .

تعیین کنید که آیا f خاصیت های زیررا دارد یا خیر ،

(a) یک ریختار حلقه ای ؛

(b) یک $Z[\sqrt{2}]$- ریختی ؛

c) یک Z - ریختی .

۴-۶- فرض کنید M یک R- مدول بوده و برای هر R- ریختی $f : R \to M$ و هر $\lambda \in R$ نگاشت $\lambda f : R \to M$ به صورت $(\lambda f)(r) = f(r\lambda)$ داده شده باشد . ثابت کنید که $\lambda f \in Mor_R(R,M)$ و نتیجه بگیرید که $Mor_R(R,M)$ یک R- مدول است. همچنین نشان دهید که نگاشت $v : Mor_R(R,M) \to M$ داده شده با $v(f) = f(1_R)$ یک R- یکریختی است .

۴-۷- فرض کنید $f : M \to N$ یک R- ریختی باشد . اگر A یک زیر مدول M باشد ، قرار دهید $f^{\to}(A) = \{f(a) | a \in A\}$ و اگر B زیر مدول N باشد ، قرار دهید $f^{\leftarrow}(B) = \{x \in M | f(x) \in B\}$. ثابت کنید که

a) $f^{\leftarrow}[\vec{f}(A)] = A + Ker f$ ؛

b) $f^{\to}[f^{\leftarrow}(B)] = B \cap \operatorname{Im} f$ ؛

c) $f^{\to}\left(A \cap f^{\leftarrow}(B)\right) = f^{\to}(A) \cap B$.

۴-۸- R- تکریختی $f : M \to N$ را اساسی گوئیم ، اگر برای هر زیر مدول غیر صفر A از N ، $f^{\leftarrow}(A)$ زیر مدول غیر صفر از M باشد . اگر M زیر مدول N باشد ، آنگاه N را توسیع اساسی M گوئیم ، اگر شمول کانونی $i : M \to N$ اساسی باشد . ثابت کنید به عنوان Z - مدول

a) Q یک توسیع اساسی Z است ؛

b) R یک توسیع اساسی Q نیست .

اگر M زیر مدول N باشد ، با استفاده از اصل زرن ثابت کنید زیر مدول A از N وجود دارد که نسبت به خاصیت $M \cap A = 0$ ماکسیمال است . برای زیر مدول A ثابت کنید که ریختار ترکیبی

$$M \xrightarrow{i} N \xrightarrow{\varphi} N/A$$

یک تکریختی اساسی است .

۹-٤- دنباله

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

از R- مدولها و R- ریختی ها داده شده است . ثابت کنید که

(a) $\operatorname{Im}(f) \cap Ker g = f^{\rightarrow}(Ker(g \circ f))$ ؛

(b) $\operatorname{Im} f + Ker g = g^{\leftarrow}(\operatorname{Im}(g \circ f))$.

۱۰-٤- نمودار

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "f"'] & C \\ B & \end{tikzcd}$$

از R- مدولها و R- ریختی ها را که در آن f یک بروریختی است در نظر بگیرید . ثابت کنید گزاره های زیر معادلند ،

(a) R- ریختی $h : B \to C$ وجود دارد به طوری که $h \circ f = g$ ؛

(b) $Ker f \subseteq Ker g$.

به علاوه ثابت کنید که چنین R- ریختی ، h ، در صورت وجود یکتا بوده و تکریختی است اگر و تنها اگر Kerf=Kerg.

اگر R- ریختی $v : M \to N$ را بتوان با ترکیب ریختارهای

$$M \xrightarrow{\alpha} A \xrightarrow{\beta} B \xrightarrow{\gamma} N$$

که در آن α یک بروریختی ، β یک یکریختی و γ یک تکریختی است نمایش داد ، ثابت کنید که $A \simeq \dfrac{M}{Ker v}$ و $B \simeq \operatorname{Im} v$.

۱۱-٤- تحقیق کنید که گزاره های زیر به عنوان Z- مدولهای مختلف برقرار است ،

(a) Q متناهی- مولد نیست ؛

(b) $\dfrac{Q}{Z}$ نامتناهی است ؛

(c) $\varnothing$ تنها زیر مجموعه مستقل $\dfrac{Q}{Z}$ است ؛

(d) $Mor_Z\left(\frac{Z}{2Z}, Q\right)=0$ ؛

(e) $Mor_Z(Q,Z)=0$.

۱۲-٤- R- مدول M را دوری گوئیم ، اگر توسط یک زیر مجموعه یک عضوی تولید شود . فرض کنید $M=Rx$ یک R- مدول دوری و $Ann_R(x)=\{\lambda\in R \mid \lambda x=0\}$ باشد . ثابت کنید که $Ann_R(x)$ یک زیر مدول R است و $M\simeq\frac{R}{Ann_R(x)}$.

فرض کنید m و n اعداد صحیح بزرگتر از یک باشند . نشان دهید که $v(x+mZ)=nx+nmZ$ یک Z- ریختی ، $v:\frac{Z}{mZ}\to\frac{Z}{nmZ}$ را توصیف می کند . ثابت کنید که Z- مدول $Mor_Z\left(\frac{Z}{mZ},\frac{Z}{nmZ}\right)$ توسط $\{v\}$ تولید می شود و نتیجه بگیرید که

$$Mor_Z\left(Z/mZ, Z/nmZ\right)\simeq Z/mZ .$$

۱۳-٤- اگر A و B زیر مدولهای R- مدول M باشند ، تحقیق کنید که دنباله

$$0\longrightarrow A\cap B\longrightarrow A\times B\longrightarrow A+B\longrightarrow 0$$

یک دنباله دقیق کوتاه است .

۱٤-٤- نمودار تعویض پذیر از R- مدولها و R- ریختی ها به صورت

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & & A_2' \arrow[d, "i_2"] \arrow[dr, "\alpha"] & & \\
0 \arrow[r] & A_1' \arrow[ur, "f"] \arrow[r, "i_1"] \arrow[dr, "\beta"'] & A \arrow[r, "\pi_1"] \arrow[d, "\pi_2"] & A_1'' \arrow[r] & 0 \\
 & & A_2'' \arrow[ur, "g"'] \arrow[d] & & \\
 & & 0 & &
\end{tikzcd}$$

با سطر و ستون کامل داده شده است . ثابت کنید که

(a α و β ریختار صفر هستند ؛

(b f و g یکریختی هستند .

۱۵-٤- فرض کنید M و N ، R- مدول و $f: M \to N$ یک R- ریختی است . اگر A یک زیر مدول M باشد ثابت کنید که گزاره های زیر هم ارزند ،

(a یک R- ریختی منحصر به فرد $f_*: \dfrac{M}{A} \to N$ وجود دارد به طوری که $f_* \circ g_A = f$ ؛

(b $A \subseteq Kerf$.

به علاوه نشان دهید R- ریختی f یک تکریختی است ، اگر و تنها اگر $A = Kerf$.

اگر A و B زیر مدولهای R- مدول M باشند ، تحقیق کنید که یک دنباله دقیق به صورت

$$0 \longrightarrow \frac{M}{(A \cap B)} \longrightarrow \frac{M}{A} \times \frac{M}{B} \longrightarrow \frac{M}{A+B} \longrightarrow 0$$

وجود دارد و بنابراین نتیجه بگیرید که

$$\frac{(A+B)}{A \cap B} \simeq \frac{(A+B)}{A} \times \frac{(A+B)}{B}$$

۱٦-٤- فرض کنید نمودار

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[d, "\gamma"] \\
A' \arrow[r, "f'"'] & B' \arrow[r, "g'"'] & C'
\end{tikzcd}$$

از R- مدولها و R- ریختی‌های تعویض پذی بوده و α وβ وγ یکریختی باشند . ثابت کنید اگر سطر بالایی دقیق باشد ، آنگاه سطر پایینی نیز دقیق خواهد بود .

۱۷-٤- [لم 3×3] فرض کنید نمودار

$$\begin{tikzcd}
& 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & A' \arrow[r, "\alpha'"] \arrow[d, "f'"] & A \arrow[r, "\beta'"] \arrow[d, "f"] & A'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & B' \arrow[r, "\alpha"] \arrow[d, "g'"] & B \arrow[r, "\beta"] \arrow[d, "g"] & B'' \arrow[r] \arrow[d, "g''"] & 0 \\
0 \arrow[r] & C' \arrow[d] & C \arrow[d] & C'' \arrow[r] \arrow[d] & 0 \\
& 0 & 0 & 0 &
\end{tikzcd}$$

از R- مدولها و R- ریختی ها ، یک نمودار تعویض پذیر بوده به طوری که هر سه ستون دقیق بوده و دو سطر بالایی نیز دقیق می باشند . ثابت کنید که R- ریختی های یکتا $\alpha'':C'\to C$ و $\beta'':C\to C''$ وجود دارند به طوری که سطر پایین دقیق و کل نمودار تعویض پذیر است .

۱۸-٤- فرض کنید R یک حوزه صحیح باشد . $0\neq x\in R$ داده شده است . نشان دهید که زنجیر نزولی

$$R\supseteq Rx\supseteq Rx^{2}\supseteq\ldots\supseteq Rx^{n}\supseteq Rx^{n+1}\supseteq\ldots$$

از زیر مدولهای R- مدول R وجود دارد به طوری که برای هر n ،

$$\frac{Rx^{n}}{Rx^{n+1}}\simeq\frac{R}{Rx}.$$

۱۹-٤- تعیین کنید کدامیک از شرطهای زنجیر در هر یک از مدولهای زیر صدق می کند ،

a) Z به عنوان یک Z- مدول ؛

b) Z_m به عنوان یک Z- مدول ؛

c) Z_m به عنوان یک Z_m- مدول ؛

d) Q به عنوان یک Q- مدول ؛

e) Q به عنوان یک Z- مدول ؛

f) $Q[X]$ به عنوان یک Q- مدول ؛

g) $Q[X]$ به عنوان یک $Q[X]$- مدول ؛

h) $\frac{Q[X]}{M}$ به عنوان $Q[X]$- مدول ، که در آن M زیر مدول شامل کلیه چند جمله ایهایی است که بر X^5 قابل تقسیم هستند ؛

i) $\frac{Q[X]}{M}$ به عنوان $Q[X]$- مدول ، جائیکه M زیر مدول شامل چند جمله ایهایی است که بر X^2+1 تقسیم پذیر هستند .

۴-۲۰- فرض کنید M یک R- مدول از ارتفاع متناهی باشد . اگر N یک زیر مدول M باشد ، ثابت کنید که یک سری ژردن- هولدر از زیر مدول ها به صورت

$$M = M_{\circ} \supset M_1 \supset \ldots \supset M_{r-1} \supset M_r = 0$$

وجود دارد به طوری که برای اندیس k ای ، $M_k=N$.

۴-۲۱- اگر M یک R- مدول از ارتفاع متناهی بوده و N یک زیر مدول M باشد ، ثابت کنید که

$$h(M) = h(N) + h\left(\frac{M}{N}\right)$$

و نتیجه بگیرید که N=M ، اگر و فقط اگر $h(N) = h(M)$.

۴-۲۲- اگر M و N ، R- مدول هایی از ارتفاع متناهی و اگر $f : M \to N$ یک R- ریختی باشد ، ثابت کنید که $\operatorname{Im} f$ و $Kerf$ از ارتفاع متناهی هستند و

$$h(\operatorname{Im} f) + h(Kerf) = h(M).$$

۴-۲۳- فرض کنید M_1 ، M_2 ،...، M_n ، R-مدول هایی از ارتفاع متناهی باشند . اگر

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \ldots \xrightarrow{f_{n-1}} M_n \longrightarrow 0$$

یک دنباله دقیق باشد ، ثابت کنید که

$$.\sum_{k=1}^{n}(-1)^{k} h(M_k)=0$$

۲۴-٤- Z - مدول های M و N با شرایط $h(M)=h(N)=2$ و $Mor_Z(M,N)=0$ را پیدا کنید .

۲۵-٤- فرض کنید F یک میدان و M_n حلقه ماتریسهای $n \times n$ روی F باشد . برای $i=1,2,\ldots,n$، فرض کنید $E_i \in M_n$ ماتریسی باشد که درایه (i,i)ام آن یک و سایر درایه های آن صفر است . برای $i=1,2,\ldots,n$ ، قرار دهید

$$B_i = M_n(E_1+E_2+\ldots+E_i).$$

ثابت کنید که

$$M_n = B_n \supset B_{n-1} \supset \ldots \supset B_1 \supset B_\circ = 0$$

یک سری ژردان- هولدر برای M_n- مدول ، M_n می باشد .

۲۶-٤- فرض کنید M_1 ، M_2 ،...، M_n زیر مدول های یک R- مدول M باشند ، به طوری که $\oplus_{i=1}^{n} M_i = M$. برای $k=1,\ldots,n$ ، N_k را زیر مدول M_k بگیرید . اگر $N=\sum_{i=1}^{n} N_i$ ، ثابت کنید که $N=\oplus_{i=1}^{n} N_i$ و $\frac{M}{N}=\oplus_{i=1}^{n}\frac{M_i}{N}$.

۲۷-٤- اگر A_1،...، A_n ، زیر مدول های R- مدول M باشند ، ثابت کنید که $M=\oplus_{i=1}^{n} A_i$ اگر و فقط اگر برای $i=1,\ldots,n$ ، R- ریختی های $f_i : A_i \to M$ و $g_i : M \to A_i$ موجود باشند به طوری که

$$(۱) \quad g_i \circ f_j = \begin{cases} id_{A_i} & i=j \\ 0 & i \neq j \end{cases} ،$$

$$(۲) \quad \sum_{i=1}^{n} f_i \circ g_i = id_M .$$

نتیجه بگیرید که M یک مجموع مستقیم از زیر مدول های M_1 و M_2 است اگر و فقط اگر یک دنباله دقیق ، کوتاه و شکافنده

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$$

موجود باشد .

۲۸-٤- فرض کنید A یک R- مدول باشد . با استفاده از اینکه R دارای عنصر همانی است ، ثابت کنید که هر دنباله دقیق از R- مدول ها و R- ریختی ها به صورت

$$0 \longrightarrow X \longrightarrow A \longrightarrow R \longrightarrow 0$$

شکافنده است . در مقابل دنباله

$$0 \longrightarrow Z \longrightarrow A \longrightarrow Y \longrightarrow 0$$

از Z - مدول ها و Z - ریختی ها شکافنده نیست

۲۹-٤- R- ریختی $f : M \to N$ را منظم گوئیم ، اگر R- ریختی $g : M \to N$ موجود باشد به طوری که $f \circ g \circ f = f$.

$$Kerf \xrightarrow{i_1} M \xrightarrow{g_1} \frac{M}{Kerf} \simeq \operatorname{Im} f \xrightarrow{i_2} N \xrightarrow{g_2} \frac{N}{\operatorname{Im} f}$$

تحقیق اینکه چه موقع آنها شکافنده هستند ، ثابت کنید که $f : M \to N$ منظم است اگر و فقط اگر $\operatorname{Ker} f$ یک جمعوند مستقیم M و $\operatorname{Im} f$ یک جمعوند مستقیم N باشد .

۳۰-٤- در نمودار داده شده

$$\begin{tikzcd}
 & M_0 \arrow[dl, "\ell_1"'] \arrow[dr, "\ell'_1"] \arrow[dd, "i_0"] & \\
M'_1 & & M'_2 \\
 & M \arrow[ul, "j_1"] \arrow[ur, "j_2"'] \arrow[dd, "j_0"] & \\
M_2 \arrow[uu, "k_1"] \arrow[ur, "i_2"'] \arrow[dr, "h_1"'] & & M_1 \arrow[uu, "k_2"'] \arrow[ul, "i_1"] \arrow[dl, "h_2"] \\
 & M'_0 &
\end{tikzcd}$$

با در نظر گرفتن ترکیب دنباله های کانونی

از R- مدول ها و R- ریختی ها ، خواص زیر برقرار است

(۱) نمودار تعویض پذیر است ؛

(۲) هر دنباله $M_t \xrightarrow{i_t} M \xrightarrow{j_t} M_t'$ دقیق است ؛

(۳) k_1 و k_2 یکریختی هستند .

ثابت کنید که $Kerj_1 \cap Kerj_2 = 0$. اگر برای هر $x \in M$ عنصر $\bar{x}$ به صورت

$$\bar{x} = \left(i_1 \circ k_2^{-1} \circ j_2\right)(x) + \left(i_2 \circ k_1^{-1} \circ j_1\right)(x)$$

تعریف شود ، نتیجه بگیرید که $\bar{x} = x$. بنابراین نشان دهید که $M = \operatorname{Im} i_1 \oplus \operatorname{Im} i_2$

$$h_1 \circ k_1^{-1} \circ \ell_1 + h_2 \circ k_2^{-1} \circ \ell_2 = 0$$

۴-۳۱- فرض کنید $(M_i)_{i\in I}$ و $(N_i)_{i\in I}$ خانواده ای از R- مدول ها باشد . اگر برای هر $i \in I$، $f_i : M_i \to N_i$ یک R- ریختی باشد ، مجموع مستقیم از خانواده $(f_i)_{i\in I}$ را به صورت R- ریختی $f : \oplus_{i\in I} M_i \to \oplus_{i\in I} N_i$ با ضابطه $f\left((m_i)_{i\in I}\right) = \left(f_i(m_i)\right)_{i\in I}$ تعریف می شود. $\operatorname{Im} f$ و $Kerf$ را تعیین کنید .

همچنین اگر $(L_i)_{i\in I}$ خانواده ای از R- مدول ها باشد و اگر برای هر $i \in I$ ، $g_i : L_i \to M_i$ یک R- ریختی و g مجموع مستقیم از خانواده $(g_i)_{i\in I}$ باشد ، ثابت کنید که

$$\bigoplus_{i\in I} L_i \xrightarrow{g} \bigoplus_{i\in I} M_i \xrightarrow{f} \bigoplus_{i\in I} N_i$$

دقیق است ، اگر و فقط اگر برای هر $i \in I$ ،

$$L_i \xrightarrow{g_i} M_i \xrightarrow{f_i} N_i$$

دقیق باشد .

۴-۳۲- حلقه تعویض پذیر و یکدار R را در نظر بگیرید . فرض کنید M یک R- مدول و $A_1, \ldots, A_n$ ، زیر مدول هایی از M باشند که $M = \oplus_{i=1}^n A_i$. برای $j = 1, \ldots, n$ ، L_j را مجموعه R- ریختی‌های $f : M \to N$ بگیرید که $\oplus_{i\neq j} A_i \subseteq Kerf$. ثابت کنید که L_j یک R- مدول است و $L_j \simeq Mor_R\left(A_j, N\right)$.

۴-۳۳- نمودار تعویض پذیر

$$\begin{tikzcd}
\cdots \arrow[r] & A \arrow[r, "f_i"] \arrow[d, "\alpha_i"] & B \arrow[r, "g_i"] \arrow[d, "\beta_i"] & C_i \arrow[r, "h_i"] \arrow[d, "\gamma_i"] & A_{i+} \arrow[r, "f_{i+1}"] \arrow[d, "\alpha_{i+1}"] & B_{i+1} \arrow[r, "g_{i+1}"] \arrow[d, "\beta_{i+1}"] & C_{i+1} \arrow[r] \arrow[d, "\gamma_{i+1}"] & \cdots \\
\cdots \arrow[r] & A'_i \arrow[r, "f'_i"] & B'_i \arrow[r, "g'_i"] & C'_i \arrow[r, "h'_i"] & A'_{i+1} \arrow[r, "f'_{i+1}"] & B'_{i+1} \arrow[r, "g'_{i+1}"] & C'_{i+1} \arrow[r] & \cdots
\end{tikzcd}$$

از R- مدول ها و R- ریختی ها با سطرهای دقیق داده شده است . اگر هر γ_i یک یکریختی باشد، تحقیق کنید که دنباله

$$\cdots \longrightarrow A_i \xrightarrow{\varphi_i} A'_i \oplus B_i \xrightarrow{v_i} B'_i \xrightarrow{h_i \gamma_i^{-1} g'_i} A_{i+1} \longrightarrow \cdots$$

که در آن φ_i و v_i توسط

$$v_i : (a'_i, b'_i) \mapsto f'_i(a'_i) - \beta_i(b_i) \quad ، \quad \varphi_i : a_i \mapsto (\alpha_i(a_i), f_i(a_i))$$

توصیف می شود دقیق است .

۴-۳۴- مثالی ارائه دهید که نشان دهد زیر مدول یک مدول آزاد لزوماً مدول آزاد نمی باشد .

۴-۳۵- فرض کنید $f : M \to M$ یک R- ریختی باشد . ثابت کنید که اگر f یک تکریختی باشد ، آنگاه f نمی تواند یک مقسوم علیه صفر چپ در حلقه $End_R(M)$ باشد . اگر M آزاد باشد ، عکس آن را تحقیق کنید .

۴-۳۶- فرض کنید $f : M \to M$ یک R- ریختی باشد . ثابت کنید که اگر f یک بروریختی باشد ، آنگاه f نمی تواند یک مقسوم علیه صفر راست در حلقه $End_R(M)$ باشد . مثالی از یک Z- مدول آزاد M و $f \in End_Z(M)$ ارائه دهید ، به طوری که f نه یک مقسوم علیه صفر راست و نه یک بروریختی است .

۴-۳۷- اگر $(P_i)_{i\in I}$ یک خانواده از مدول های تصویری باشد ، ثابت کنید که $\bigoplus_{i\in I} P_i$ یک مدول تصویری است .

۴-۳۸- برای R- مدول های M و N مجموعه $P(M,N)$ را متشکل از کلیه R-ریختی های $f:M\to N$ بگیرید که دارای این خاصیت می باشند که یک نمودار تعویض پذیر

$$\begin{tikzcd} & P \arrow[dr, "h"] & \\ M \arrow[ur, "k"] \arrow[rr, "f"'] & & N \end{tikzcd}$$

که در آن P تصویری است موجود باشد (به چنین fهایی ، عامل های گذرا از تصویرها می گوئیم). ثابت کنید $P(M,N)$ یک زیر گروه از گروه $Mor_R(M,N)$ می باشد .

۴-۳۹- نشان دهید هر نمودار از R- مدول ها و R- ریختی ها به صورت

$$\begin{tikzcd} & P' \arrow[d, "\alpha"'] & & P'' \arrow[d, "\beta"'] & \\ 0 \arrow[r] & E' \arrow[r, "f"'] & E \arrow[r, "g"'] & E'' \arrow[r] & 0 \end{tikzcd}$$

که دارای سطر دقیق بوده ، و P' و P'' تصویری می باشند را می توان به نمودار تعویض پذیر

$$\begin{tikzcd} 0 \arrow[r] & P' \arrow[r, "i"] \arrow[d, "\alpha"'] & P \arrow[r, "\pi"] \arrow[d, "\gamma"'] & P'' \arrow[r] \arrow[d, "\beta"'] & 0 \\ 0 \arrow[r] & E' \arrow[r, "f"'] & E \arrow[r, "g"'] & E'' \arrow[r] & 0 \end{tikzcd}$$

توسیع داد ، به طوری که سطر بالا کامل است و P نیز تصویری باشد .

۴-۴۰- فرض کنید n عدد صحیح بزرگتر از یک باشد . برای هر مقسوم علیه r از n ، ایده ال $r\left(\frac{Z}{nZ}\right)$ را از حلقه $\frac{Z}{nZ}$ در نظر بگیرید . نشان دهید که دنباله

$$0 \longrightarrow \frac{n}{r}\left(\frac{Z}{nZ}\right) \longrightarrow \frac{Z}{nZ} \longrightarrow r\left(\frac{Z}{nZ}\right) \longrightarrow 0$$

دقیق است . ثابت کنید که گزاره های زیر هم ارزند ،

(۱) دنباله بالا شکافنده است ؛

(۲) $h.c.f.\left\{r, \frac{n}{r}\right\} = 1$ ؛

(۳) $\frac{Z}{nZ}$ - مدول ، $r\left(\frac{Z}{nZ}\right)$ تصویری است .

از این رو یک مثال از یک مدول تصویری که آزاد نیست مهیا می شود .

۴۱-۴- فرض کنید R یک حلقه تعویض پذیر یکدار و X و Y ، R- مدول هایی می باشند که X تصویری است . اگر A و B به ترتیب زیر مدول های X و Y باشند ، ثابت کنید که

$$\Delta_{A,B} = \left\{f \in Mor_R(X,Y) \;\middle|\; f^{\rightarrow}(A) \subseteq B\right\}$$

زیر مدولی از R- مدول $Mor_R(X,Y)$ می باشد .

ثابت کنید که

$$Mor_R\left(\frac{X}{A}, \frac{Y}{B}\right) \simeq \frac{\Delta_{A,B}}{\Delta_{X,B}}$$

۴۲-۴- فرض کنید P یک R- مدول تصویری و نمودار به صورت

$$\begin{tikzcd} & P \arrow[d, "v"] & \\ X \arrow[r, "\alpha"] & Y \arrow[r, "\beta"] & Z \end{tikzcd}$$

از R- مدول ها و R- ریختی ها با سطر دقیق موجود باشد و $\beta \circ v = 0$. ثابت کنید R- ریختی $\zeta : P \to X$ وجود دارد ، به طوری که $\alpha \circ \zeta = v$.

نمودار

$$\begin{tikzcd}
\cdots \arrow[r] & P_3 \arrow[r, "g_3"] & P_2 \arrow[r, "g_2"] & P_1 \arrow[r, "g_1"] & A \arrow[d, "k_\circ"] & \\
\cdots \arrow[r] & Q_3 \arrow[r, "h_3"] & Q_2 \arrow[r, "h_2"] & Q_1 \arrow[r, "h_1"] & B \arrow[r] & 0
\end{tikzcd}$$

از R- مدول ها و R- ریختی ها با سطرهای دقیق که هر P_i تصویری است را در نظر بگیرید . به روش استقرا نشان دهید که برای هر عدد صحیح مثبت n ، یک R- ریختی $K_n : P_n \to Q_n$ وجود دارد ، به طوری که $h_n \circ k_n = k_{n-1} \circ g_n$.

۴۳-٤- نمودار

$$\begin{tikzcd}
0 \arrow[r] & Ker g \arrow[r, "j"] & A \arrow[r, "g"] \arrow[d, "i"'] & B \arrow[r] & 0 \\
& & P \arrow[r, "h"'] & \dfrac{P}{\mathrm{Im}(i \circ j)} &
\end{tikzcd}$$

از R- مدول ها و R- ریختی ها به طوری که در آن سطر بالایی دقیق ، j نگاشت یک به یک ، i تکریختی و h برو ریختی کانونی می باشد را در نظر بگیرید . ثابت کنید که R- ریختی منحصر به فرد $v : B \to \dfrac{P}{\mathrm{Im}(i \circ j)}$ وجود دارد ، به طوری که $v \circ g = h \circ i$. همچنین نشان دهید که v یک تکریختی است .

R- مدول P را شبه تصویری گوئیم ، هرگاه برای هر نمودار

$$\begin{tikzcd}
& P \arrow[d, "k"] & \\
A \arrow[r, "g"'] & B \arrow[r] & 0
\end{tikzcd}$$

با سطر دقیق که A زیر مدول P است ، یک R- ریختی منحصر به فرد $\zeta : P \to A$ وجود دارد به طوری که $g \circ \zeta = h$. ثابت کنید که P شبه تصویر است اگر و فقط اگر برای هر نمودار

$$\begin{tikzcd}
& P \arrow[d, "k"] & \\
P \arrow[r, "h"'] & \frac{P}{Q} \arrow[r] & 0
\end{tikzcd}$$

که Q زیر مدول P است ، R- ریختی منحصر به فرد $\pi : P \to P$ موجود باشد به طوری که

$$h \circ \pi = k .$$

حل مسائل فصل اول

۱-۱- (a) بیان اینکه $\frac{R}{I}$ یک حوزه صحیح است هم ارز این است که بگوییم مقسوم علیه صفر ندارد ، که این هم ارز این است که بگوییم برای هر $x, y \in R$ ، اگر $(x+I)(y+I)=0+I$ ، آنگاه $x+I=0+I$ یا $y+I=0+I$ ، و این معادل با این است که بگوییم شرط $xy \in I$ ایجاب می‌کند که $x \in I$ یا $y \in I$ ، یعنی اینکه I اول است .

(b) فرض کنید I ماکسیمال است و $x+I$ یک عنصر غیر صفر $\frac{R}{I}$ باشد . در این صورت $x \notin I$ و بنابراین ایده ال $I+(x)$ از R به طور محض شامل I می‌باشد . بنابراین $I+(x)=R$ و در نتیجه به ازای $i \in I$ ای و $r \in R$ای داریم $i+rx=1$. با استفاده از خارج قسمتها (یعنی با بکار بردن ریختار طبیعی وابسته به I در این معادله) ، تساوی $(r+I)(x+I)=1+I$ بدست می‌آید که نشان می‌دهد $r+I$ وارون $x+I$ است . بنابراین $\frac{R}{I}$ میدان است . به عکس ، فرض کنید $\frac{R}{I}$ میدان باشد و J ایده ال R با $I \subset J$ باشد . فرض کنید $b \in J \setminus I$. از آنجا که $b+I \neq 0+I$ نتیجه می‌دهد که برای هر $r \in R$ ، $x \in R$ای وجود دارد به‌طوری‌که $(b+I)(x+I)=r+I$. در نتیجه $bx-r=i \in I$ و بنابراین $r=bx-i \in J$ و نتیجتاً $J=R$.

از آنجائیکه هر میدان یک حوزه صحیح است ، از قسمت قبل نتیجه می‌شود که هر ایده ال ماکسیمال ، ایده آل اول است . واضح است که ایده ال (o) از Z اول است ولی ماکسیمال نیست.

اگر هر عنصر غیر صفر $\frac{R}{M}$ وارون پذیر باشند ، آنگاه $\frac{R}{M}$ شامل هیچ ایده ال محض غیر صفر نمی باشد ، زیرا اگر A ایده ال محض باشد که شامل عنصر $0 \neq a \in A$ باشد ، آنگاه a^{-1} موجود و $a^{-1}a \in A$ می‌باشد و تناقض $A = \frac{R}{M}$ حاصل می‌شود . بنابراین R هیچ ایده ال محضی که به طور سره شامل M باشد ندارد.

حال داریم

$$\frac{Mat_{2\times2}(Z)}{M} \simeq Mat_{2\times2}(Z_2)$$

و بنابراین از آنجائیکه $Mat_{2\times2}(Z_2)$ شامل هیچ ایده ال محض نیست ، M در $Mat_{2\times2}(Z)$ ماکسیمال است . به هر حال $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + M$ در $\frac{Mat_{2\times2}(Z)}{M}$ وارون پذیر نیست زیرا

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1+2x & 2y \\ 2z & 1+2t \end{bmatrix}$$

که این وارون پذیری آن را غیر ممکن می‌سازد .

۲-۱- فرض کنید $4Z \subseteq I \subseteq (8)$. اگر $I \neq (8)$ ، آنگاه $t = 4n \in I$ وجود دارد که n فرد است، مثلاً $n = 2m+1$. بنابراین $t = 8m+4$ ، که نتیجه می‌دهد در $\frac{Z}{(8)}$، $t+(8) = 4+(8)$.

بنابراین $I = 4Z$ و $\frac{4Z}{(8)}$ ایده ال غیر بدیهی ندارد . واضح است که $\frac{4Z}{(8)}$ میدان نیست زیرا اگر $x = 4+(8)$، آنگاه در $\frac{Z}{(8)}$ داریم $x^2=0$.

به این دلیل که $4Z$ دارای عنصرهمانی نیست نتیجه می گیریم که $4Z$ میدان نمی باشد .

۳-۱- (**a**) از آنجائیکه که هر عنصر خود توان است داریم

$$x + x = (x+x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x$$

بنابراین $x + x = 0$ و مشخصه 2 است .

(**b**) داریم $(x+y) = (x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$.

بنابراین $xy + yx = 0$. با استفاده از اینکه $y + y = 0$ نتیجه می‌گیریم که $y = -y$ و بنابراین

$$xy = -yx = (-y)x = yx .$$

$(2) \Rightarrow (1)$: اگر I اول باشد ، آنگاه $\frac{A}{I}$ حوزه صحیح است و بنابراین مقسوم علیه صفر ندارد . حال در A داریم

$$xy(x+y) = xyx + xy^2 = x^2y + xy^2 = xy + xy = 0$$

این برابری برای خارج قسمتهای به هنگ I نیز درست است ، یعنی $\overline{xy}(\bar{x} + \bar{y}) = \bar{0}$. بنابراین اگر $\bar{x} \neq \bar{0}$ و $\bar{y} \neq \bar{0}$ ، آنگاه باید داشته باشیم $\bar{x} + \bar{y} = \bar{0}$ ، که از آنجا $\bar{x} = -\bar{y} = \bar{y}$. در نتیجه $\frac{A}{I}$ شامل دو عنصر است و بنابراین $\frac{A}{I} \simeq \frac{Z}{2Z}$.

$(3) \Rightarrow (2)$ از سوال ۱-۱ نتیجه می‌شود .

$(1) \Rightarrow (3)$ از سوال ۱-۱ نتیجه می‌شود .

۱-۴- $J = XF[X,Y]$ ، بنابراین J اصلی است . داریم $\frac{F[X,Y]}{J} \simeq F[Y]$ که یک حوزه صحیح است . بنابراین J یک ایده ال اول $F[X,Y]$ است . با این وجود ، از آنجائیکه $F[Y]$ میدان نیست ، J یک ایده ال ماکسیمال $F[X,Y]$ نخواهد شد . در حقیقت

$$J \subset (J, Y^2) \subset F[X,Y]$$

۱-۵- (a) از آنجائیکه $A \subseteq r(A)$ ، برای هر A داریم

$$I + J \subseteq r(I) + r(J) \subseteq r[r(I) + r(J)].$$

حال $x \in r[r(I) + r(J)]$ را در نظر بگیرید . بنابراین به ازای $n \in \mathbb{N}$ ای ، $x^n \in r(I) + r(J)$ و در نتیجه $x^n = y + z$ جائیکه به ازای $m_1, m_2 \in \mathbb{N}$ ، $z^{m_2} \in J$ و $y^{m_1} \in I$. از این رو $x^{n(m_1+m_2)} = \sum y^{\mu} z^{\nu}$ جائیکه $\mu + \nu = m_1 + m_2$ و یا $\mu \geq m_1$ یا $\nu \geq m_2$. اما اگر $\mu \geq m_1$ ، داریم $y^{\mu} z^{\nu} \in I$ در صورتی که اگر $\nu \geq m_2$ ، داریم $y^{\mu} z^{\nu} \in J$. بنابراین $x^{n(m_1+m_2)} \in I + J$ ، پس $x \in r(I+J)$.

(**b**) اگر $I^n \subseteq J$ ، قرار دهید $x \in r(I)$. بنابراین به ازای m ای ، $x^m \in I$. اما از آنجائیکه $I^n \subseteq J$ ، آنگاه $\left(x^m\right)^n \in J$ و در نتیجه $x \in r(J)$. مجموعه عنصرهای پوچتوان $\frac{R}{I}$ مجموعه $r\left(\frac{I}{I}\right)=\frac{r(I)}{I}$ است . بنابراین $\frac{R}{I}$ عنصر پوچتوان غیر صفر ندارد اگر و تنها اگر $I=r(I)$.

اگر P اول و $x^n \in P$ ، آنگاه $x \in P$. بنابراین اگر $x \in r(P)$ داریم $x \in P$ و در نتیجه $r(P)=P$.

۶-۱- (**a**) اگر $x \in I:K$ ، آنگاه برای هر $k \in K$ ، $xk \in I$ و همچنین برای هر $k \in K$ ، $xk \in J$ ، که از آنجا $x \in J:K$. حال اگر $x \in (K:J)$ ، آنگاه برای هر $a \in J$ ، $xa \in K$ و همچنین برای هر $a \in I$ ، $xa \in K$. بنابراین $x \in (K:I)$.

(**b**) ابتدا نتیجه کلی

$$((I:J):K)=(I:JK)$$

را مشاهده کنید .

درحقیقت $JK[((I:J)):K] \subseteq J(I:J) \subseteq I$ وبنابراین‌نتیجه می‌شود که $((I:J):K) \subseteq (I:JK)$.

همچنین $JK(I:JK) \subseteq I$ نتیجه می‌دهد که $K(I:JK) \subseteq (I:J)$ و بنابراین $(I:JK) \subseteq ((I:J):K)$. حال با قرار دادن $K=J^n$ ، (b) حاصل می‌شود .

(**c**) اگر $J \subseteq I$ و $a \in R$ ، آنگاه $aJ \subseteq J \subseteq I$ و بنابراین نتیجه می‌دهد که $a \in (I:J)$.

بر عکس ، اگر $(I:J)=R$ ، آنگاه مخصوصا داریم $1 \in (I:J)$ که از آنجا $J=1J \subseteq I$.

(**d**)

$$(I:(I+J))=(I:I)\bigcap(I:J)=R\bigcap(I:J)=(I:J)$$

۷-۱- به وضوح وقتی p عدد اول باشد $\left(p^n\right)$ ایده ال اولیه Z است . بر عکس ، فرض کنید $m=pq$ و p و q نسبت به هم اول باشند . دراین صورت $pq \in (m)$ و $p \notin (m)$ ، در حالی که برای هر $n \geq 1$ ، $q^n \notin (m)$. بنابراین (m) اولیه نیست .

مستقیماً می‌توان بررسی کرد که $(4,X)$ یک ایده ال اولیه است . برای این منظور اگر $fg \in (4,X)$ و $f \notin (4,X)$ ، آنگاه هر جمله g که به 4 یا X تقسیم پذیر نیست ، باید به 2 تقسیم پذیر باشد . بنابراین $g^2 \in (4,X)$. پس $(4,X)$ اولیه است .

اگر $(4,X)$ توانی از یک ایده ال اول P باشد ، آنگاه P باید شامل $(4,X)$ باشد . اما $\frac{Z[X]}{(4,X)} \simeq Z_4$ و بنابراین تنها حالت ممکن $P=(2,X)$ است که متناظر با $2Z_4$ بوده که تنها ایده ال غیر صفر محض Z_4 است . با این وجود به ازای هر $n \geq 1$ ، $(2,X)^n \neq (4,X)$.

حال $\frac{R}{P} \simeq Z$ بنابراین P ایده ال اول R است (زیرا Z یک حوزه صحیح است) . با این وجود چون $X^2 \in P$ و $3X^2 \in P^2$ داریم $3X^3 \in P^2$. اما $X^3 \notin P$ و بنابراین اگر P^2 اولیه باشد ، به ازای $n \geq 1$ ای داریم $3^n \in P^2$. از آنجائیکه هر عنصر P^2 دارای جمله ثابت صفر است این یک تناقض است .

۸-۱- به وضوح $(Y^2Z^2, XYZ) \subseteq (Y) \cap (Z) \cap (X,Y)^2 \cap (X,Z)^2$. برای بدست آوردن طرف دیگر شمول ، فرض کنید $f(X,Y,Z)$ واقع درطرف راست باشد . بنابراین از آنجا که $f \in (Y) \cap (Z)$ داریم $f(X,Y,Z) = YZg(X,Y,Z)$. اما همچنین داریم $f \in (X,Y)^2$ و بنابراین $g(X,Y,Z) = Ya(X,Y,Z) + Xb(X,Y,Z)$

حال $YZXb(X,Y,Z) \in (X,Z)^2$ پس نیاز داریم $Y^2Za(X,Y,Z) \in (X,Z)^2$ یعنی

$$a(X,Y,Z) = Zh(X,Y,Z) + Xk(X,Y,Z).$$

پس $f \in (Y^2Z^2, XYZ)$ و این همان نتیجه است .

تساوی $(Y^2Z^2, XYZ) = (Y)(Z)(X,Y)^2(X,Z)^2$ درست نیست . برای اینکه هر چند جمله ای طرف راست حداقل درجه شش دارد و بنابراین در حالت خاص XYZ نمی تواند متعلق به طرف راست باشد .

۹-۱- از آنجائیکه $I \in F_I$ واضح است که $F_I \neq \phi$. فرض کنید $\{J_\beta | \beta \in B\}$ یک زیر مجموعه کلاً مرتب از F_I باشد . بنابراین $\bigcup_{\beta \in B} J_\beta \neq A$ در غیر این صورت به ازای β ای داریم $1 \in J_\beta$ ، که از آنجا تناقض

$$A = A1 \subseteq AJ_\beta \subseteq J_\beta \subset A$$

بدست می‌آید . حال فرض کنید x ، $y \in \bigcup_{\beta \in B} J_\beta$. بنابراین $\alpha, \gamma \in B$ وجود دارد به طوری که $x \in J_\alpha$ و $y \in J_\gamma$. اما یا $J_\alpha \subseteq J_\gamma$ و یا $J_\gamma \subseteq J_\alpha$. بدون اینکه از کلیت مسئله کم شود

فرض کنید $J_\alpha \subseteq J_\gamma$. پس $x-y \in J_\gamma \subseteq \bigcup_{\beta\in B} J_\beta$: به‌طور مشابه برای هر $a \in A$، $xa, ax \in J_\gamma$. بنابراین مشاهده می‌کنیم که $\bigcup_{\beta\in B} J_\beta$ ایده الی از A است که با A متفاوت است. بنابراین F_I به طور استقرایی مرتب شده است.

با بکار بردن اصل زرن عنصر ماکسیمال M از F_I را بدست می‌آوریم. واضح است که M یک ایده ال ماکسیمال A است به طوری که $I \subseteq M$.

فرض کنید $I \in I(A)$ و $I \neq A$. پس I عنصر وارون پذیر ندارد، زیرا فرض کنید $x \in I$ وارون پذیر باشد. پس $1 = x^{-1}x \in I$ نتیجه می‌دهد A=I، که یک تناقض است. بر عکس اگر $a \in A$ به هیچ ایده ال ماکسیمالی تعلق نداشته باشد، آنگاه بنا به قسمت اول سئوال، a به هیچ ایده ال محض تعلق ندارد. حال Aa=Aa یک ایده ال (با توجه به تعویض پذیری) A است که $a = 1a \in Aa$. در نتیجه Aa=A، که از آنجا $x \in A$ای وجود دارد به طوری که xa=1. بنابراین a وارونپذیر است.

۱۰-۱- $Mat_{n\times n}(F)$ یک فضای برداری با بعد متناهی روی F است. یک ایده ال چپ یا راست این فضا یک زیر فضا می‌باشد. بنابراین اگر L_1 و L_2 ایده ال‌های چپ باشند که $L_1 \subset L_2$، آنگاه $\dim L_1 < \dim L_2$. این نتیجه می‌دهد که هر زنجیر از ایده ال‌های چپ متناهی است. بنابراین هر دو شرطهای زنجیر صدق می‌کند. نتیجه مشابه برای ایده ال‌های راست، درست است.

I را یک ایده ال راست محض غیر صفر R بگیرید. فرض کنید I شامل عنصرهای غیر صفر

$$\begin{bmatrix} c_1 & 0 \\ c_2 & 0 \end{bmatrix}, \begin{bmatrix} d_1 & 0 \\ d_2 & 0 \end{bmatrix}$$

باشد. فرض کنید که $c_1 \neq 0$ و $d_1 \neq 0$. پس

$$\begin{bmatrix} c_1 & 0 \\ c_2 & 0 \end{bmatrix}\begin{bmatrix} c_1^{-1} & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ c_1^{-1}c_2 & 0 \end{bmatrix} \in I،$$

و به طور مشابه

$$\begin{bmatrix} 1 & 0 \\ d_1^{-1}d_2 & 0 \end{bmatrix} \in I.$$

اما I شامل $\begin{bmatrix} 0 & 0 \\ d & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ d_1^{-1}d_2 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ c_1^{-1}c_2 & 0 \end{bmatrix}$ می‌باشد که در آن $d = c_1^{-1}c_2 - d_1^{-1}d_2$

حال اگر $d \neq 0$ ، آنگاه داریم

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ d & 0 \end{bmatrix}\begin{bmatrix} d^{-1} & 0 \\ 0 & 0 \end{bmatrix}$$

که از آنجا

$$\begin{bmatrix} 0 & 0 \\ c_2 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} c_2 & 0 \\ c_1 & 0 \end{bmatrix} \in I$$

و بنابراین همچنین

$$\begin{bmatrix} c_1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} c_1 & 0 \\ c_2 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ c_2 & 0 \end{bmatrix} \in I .$$

در نتیجه

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} c_1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} c_1^{-1} & 0 \\ 0 & 0 \end{bmatrix} \in I .$$

حال بسادگی نتیجه می‌شود I=R ، که یک تناقض است . بنابراین باید d=0 و در نتیجه $d_1c_2=c_1d_2$ که نتیجه می‌دهد به ازای $\alpha \in F$ ای ،

$$\begin{bmatrix} c_1 & 0 \\ c_2 & 0 \end{bmatrix} = \alpha\begin{bmatrix} d_1 & 0 \\ d_2 & 0 \end{bmatrix}.$$

اگر $c_1 = 0$ ، آنگاه $d_1 = 0$ در غیر این صورت I=R . بنابراین نتیجه حاصل شد .

دو ایده ال راست محض غیر صفر که یکی مشمول در دیگری باشد وجود ندارد . بنابراین R در هر دو شرط زنجیر ایده الهای راست صدق می‌کند . اگر S زیر گروه جمعی R باشد ، آنگاه $S\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ ایده ال چپ R است .

پس

$$2Z\begin{bmatrix}0&0\\1&0\end{bmatrix}\supset 4Z\begin{bmatrix}0&0\\1&0\end{bmatrix}\supset 8Z\begin{bmatrix}0&0\\1&0\end{bmatrix}\supset\dots$$

یک زنجیر نزولی نامتناهی از ایده الهای چپ است . با در نظر گرفتن $S_i=\left\{\frac{t}{in}\middle|t,n\in Z\right\}$ ، زنجیر صعودی نامتناهی از ایده الهای چپ

$$S_2\begin{bmatrix}0&0\\1&0\end{bmatrix}\subset S_4\begin{bmatrix}0&0\\1&0\end{bmatrix}\subset S_8\begin{bmatrix}0&0\\1&0\end{bmatrix}\subset\dots$$

بدست می‌آید .

۱۱-۱- فرض کنید $R=\{r+xr|r\in R\}$. پس برای یک $r\in R$ ، $x=r+xr$ و بنابراین $x+(-r)+x(-r)=0$ ، که نشان می‌دهد x شبه منظم راست است . بر عکس ، اگر به ازای $y\in R$ای ، $x+y+xy=0$ ، آنگاه $x=-y+x(-y)\in\{r+xr|r\in R\}$.
چون این یک ایده ال راست R است ، بنابراین شامل xr و در نتیجه شامل عنصر $r+xr-xr=r$ می‌باشد و بنابراین برابر با R است .

حال فرض کنید که x متعلق به هر ایده ال راست ماکسیمال R باشد . اگر x شبه منظم راست نباشد ، آنگاه $A=\{r+xr|r\in R\}\neq R$. فرض کنید M ایده ال راست ماکسیمال R باشد که شامل مجموعه A بوده و $x\notin M$. بنابراین M یک ایده ال راست ماکسیمال R است و در نتیجه $x\in M$ ، که تناقض است . پس x شبه منظم راست است . بنابراین هر عنصر در اشتراک ایده ال‌های راست ماکسیمال R شبه منظم راست است که نشان می‌دهد برای هر $r\in R$ ، xr شبه منظم راست است .

اگر M ایده ال راست ماکسیمال R باشد و $x\notin M$ ، آنگاه $\{M+xr|r\in R\}$ یک ایده ال راست R است به طوری که $M\subset\{M+xr|r\in R\}$ و بنابراین $\{M+xr|r\in R\}=R$. در نتیجه به ازای $m\in M$ای و $r\in R$ای داریم $-1=m+xr$.

حال فرض کنید برای هر $r\in R$ ، xr شبه منظم راست بوده و به ازای یک ایده ال راست ماکسیمال M ، $x\notin M$. پس $m+xr=-1$ و xr شبه منظم راست است . بنابراین $z\in R$ وجود دارد به طوری که $xr+z+xrz=0$. اما تساوی $mz+xrz=-z$ نتیجه می‌دهد که

$mz = xr$. بنابراین $xr \in M$ و در نتیجه $-1 = m + xr \in M$ و این نشان می‌دهد M=R، که یک تناقض است . از این رو نتیجه حاصل می‌شود .

۱-۱۲- نتیجه برای $i = j$ (بنا به فرض) درست است . فرض کنید $j > i$ و $R^{j-1} = S^{j-1} + R^j$.

پس

$$R^j = R^{j-1}R = \left(S^{j-1} + R^j\right)R \subseteq SR^{j-1} + R^{j+1} = S\left(S^{j-1} + R^j\right) + R^{j+1} \subseteq S^j + R^{j+1}.$$

به وضوح ، $\left(S^j + R^{j+1}\right) \subseteq R^j$ و بنابراین $R^j = S^j + R^{j+1}$.

با استفاده از استقرا و بحث فوق داریم

$$R^j = S^j + R^{j+k-1} = S^j + S^{j+k-1} + R^{j+k} = S^j + R^{j+k}.$$

حال فرض کنید R پوچتوان است ، مثلاً $R^m = \{0\}$ ،

(**a**) برای $j \geq i$ و برای هر k، $R^i = S^i + R^{i+1}$ ایجاب می کند که $R^j = S^j + R^{j+k}$.
بنابراین برای هر $j \geq i$ ، $R^j = S^j + R^{j+m} = S^j$.

(**b**) فرض کنید $R = \langle a \rangle + R^2$. بنابراین بنا به (a) ، برای همه $j \geq 1$ داریم $R^j = \langle a \rangle^j$.
قرار دهید $j = 1$ تا $R = \langle a \rangle$ حاصل می‌شود .

(**c**) اگر $R^2 \not\subset M$ ، آنگاه از آنجا که M ماکسیمال است ، $R = M + R^2$. بنابراین مجدداً بنا به (a) ، R=M که غیر ممکن است . بنابراین $R^2 \subseteq M$.

(**d**) از آنجا که $R^2 \subseteq M$ ، خارج قسمت $\frac{R}{M}$ دارای عمل ضرب صفر است . بنابراین هر زیر گروه از گروه جمعی M یک ایده ال R است . پس تعداد عناصر $\frac{R}{M}$ یک عدد اول است .

۱-۱۳- فرض کنید که A زیر حلقه ای از حلقه پوچ R باشد . اگر $a \in A$ ، آنگاه $a \in R$ و بنابراین A پوچتوان است . از این رو A یک حلقه پوچ است . همچنین اگر $b \in \frac{R}{I}$ ، آنگاه به ازای $x \in R$ ای ، $b = x + I$ و از آنجا که به ازای $n \geq 1$ ، $x^n = 0$، داریم $b^n = I$. بنابراین $\frac{R}{I}$ حلقه پوچ است .

حال فرض کنید A و $\frac{B}{A}$ پوچ باشند . فرض کنید $x \in B$. ازآنجا که به ازای $n \geq 1$ای $(x+A)^n = A$ داریم $x^n \in A$ و چون A پوچ است داریم $(x^n)^m = 0$. بنابراین x پوچتوان و B پوچ است .

اگر B پوچ باشد ، آنگاه $\frac{B}{(A \cap B)} \simeq \frac{A+B}{A}$. اما A پوچ است ، بنابراین A+B نیز پوچ است .

در R_p داریم $(a_1, a_2, a_3, \ldots)^n = 0$ اگر و فقط اگر برای هر $i \geq 1$ ، $a_i^n = 0$ و این برقرار است اگر و فقط اگر هر a_i تقسیم پذیر بر p باشد . بنابراین از آنجا که فقط تعداد متناهی a_i غیر صفر است آنگاه

$$(a_1, a_2, a_3, \ldots)^n = 0 \Leftrightarrow a_i \in pZ_{p^i} .$$

حال به سادگی می‌بینید که مجموعه N متشکل از عنصرهای پوچتوان ، یک ایده ال دو طرفه R_p است . با این وجود N پوچتوان نیست . برای اینکه اگر N پوچتوان باشد ، آنگاه به ازای mای باید داشته باشیم $N^m = \{0\}$ ، که نتیجه می‌دهد برای کلیه $(a_1, a_2, \ldots) \in N$ داریم $(a_1, a_2, \ldots)^m = 0$. با این وجود

$$\left(\underbrace{0,0,\ldots,p}_{m+1},0,\ldots\right)^m \neq (0,0,\ldots).$$

۱۴-۱- (**a**) از آنجا که J کوچکترین ایده ال A_2 است که شامل I می‌باشد داریم $J \subseteq A_1$. بنابراین $JI \subseteq I$ و $IJ \subseteq I$. در نتیجه

$$\begin{aligned} J^3 &= J(I + A_2 I + IA_2 + A_2 I A_2)J \\ &\subseteq I + JI + IJ + JIJ \subseteq I. \end{aligned}$$

(**b**) I را یک زیر ایده ال n - پله ای نامند ، اگر $I = A_0 \subset A_1 \subset \ldots \subset A_n = R$. فرض کنید $\bar{I}$ کوچکترین ایده ال R شامل I باشد . با استقرا روی n نشان داده می شود که $\bar{I}^{3^n} \subseteq I$.

اگر J کوچکترین ایده ال A_2 شامل J باشد ، آنگاه

$$J \subset A_2 \subset A_3 \ldots \subset A_n = R$$

و J یک زیر ایده ال (n-1) پایه ای است . با فرض استقرا $J \subseteq \bar{J}^{3n}$ ، جائیکه $\bar{J}$ کوچکترین ایده ال R شامل J است . اما از آنجائیکه $I \subseteq A_1 \subseteq A_2$ و J کوچکترین ایده ال A_2 شامل I است داریم $J^3 \subseteq I$ (بنا به (a)) . در نتیجه $\bar{J}^{3n} \subseteq J.J^3 \subseteq JI \subseteq I$. با این وجود $I \subseteq J \subseteq \bar{I}$ ، بنابراین $\bar{J} = \bar{I}$ و در نتیجه $\bar{I}^{3n} \subseteq I$.

(c) اگر $I^m = \{0\}$ ، داریم $\left(\bar{I}^{3n}\right)^m = \{0\}$ و $\bar{I}$ پوچتوان است .

۱۵-۱- فرض کنید Q نیم اول بوده و $A^n \subseteq Q$. نشان می‌دهیم $A \subseteq Q$. درستی نتیجه برای n=2 واضح است . با بکارگیری استقرا فرض کنید که اگر $A^m \subseteq Q$ و $m<n$ ، آنگاه $A \subseteq Q$. اگر n زوج باشد ، آنگاه $A^{\frac{1}{2}n} A^{\frac{1}{2}n} \subseteq Q$ ایجاب می کند $A^{\frac{1}{2}n} \subseteq Q$ و بنابراین بنا به فرض استقرا ، $A \subseteq Q$.

اگر n فرد باشد ، آنگاه $A^{n+1} \subseteq Q$ و n+1 زوج است که از آنجا دوباره $A \subseteq Q$.

فرض کنید $\varphi : R \to \frac{R}{Q}$ ریختار طبیعی است . فرض کنید Q شبه اول بوده و X در $\frac{R}{Q}$ پوچتوان باشد ، مثلاً $X^n = 0$. نقش معکوس زیر مجموعه T از $\frac{R}{Q}$ تحت φ را با $\overline{T}$ نشان می‌دهیم . داریم $\overline{X}^n \subseteq \overline{X^n} = Q$. از آنجا که Q نیم اول است نتیجه می‌شود که $\overline{X} \subseteq Q$ و بنابراین $X = 0$. بر عکس ، فرض کنید $\frac{R}{Q}$ شامل ایده الهای پوچتوان غیر صفر نباشد . فرض کنید A یک ایده ال باشد و $A^2 \subseteq Q$. بنابراین $[\varphi(A)]^2 = \varphi(A^2) = 0$ که از آنجا $\varphi(A) = 0$ و $A \subseteq Q$.

حل مسائل فصل دوم

۱-۲- (**a**) $x|y \Leftrightarrow y=xr \Leftrightarrow y\in(x) \Leftrightarrow (y)\subseteq(x)$.

(b) اگر x و y شریک باشند ، آنگاه (a) نتیجه می‌دهد که $(x)=(y)$ ، برعکس اگر $(x)=(y)$ ، آنگاه $r,s\in R$ وجود دارد به طوری که $x=ry$ ، $y=sx$. از آنجا $x=rsx$ که نتیجه می‌دهد $rs=1$. بنابراین r و s یکه هستند و x و y شریک هستند .

(**c**) با بکار بردن (b) داریم

u یکه است $\Leftrightarrow u\sim 1 \Leftrightarrow (u)=(1)=R$.

(d) فرض کنید $x=yr$ ، جائیکه y و r یکه نیستند . بنابراین یقیناً $(x)\subseteq(y)\subseteq R$. حال $(x)\neq(y)$ زیرا در غیر این صورت x و y شریک هستند (بنا به (b)) ، و آنگاه r باید یکه باشد ، $(y)\neq R$ زیرا در غیر این صورت y باید یکه باشد (بنا به (c)) . عکس آن واضح است .

(e) اگر (x) در میان ایده ال‌های اصلی ماکسیمال نباشد ، آنگاه به ازای y ای داریم $(x)\subset(y)\subset R$. بنا به (d) ، y عامل سره از x است و بنابراین x تحویل ناپذیر نیست . برعکس اگر x تحویل ناپذیر نباشد ، آنگاه دارای یک عامل سره y است و نتیجه از (d) حاصل می‌شود .

۲-۲- (a) صحیح است . اگر $a|b$ ایجاب کند $b|a$ ، آنگاه هر زوج از عنصرهای غیر صفر شریک هستند (برای اینکه $x\sim xy\sim y$) . بنابراین به ازای هر $x\in R^*$ ، $x\sim 1$ و بنابراین R میدان است .

(b) صحیح است . اثبات (a) را مشاهده کنید .

(c) $a = bu$ و $c = dv$ نتیجه می‌دهد که $ac = bd.uv$ و بنابراین $ac \sim bd$.

(d) نادرست است . در $Z[i]$ داریم $1 \sim 1$ و $1+2i \sim -2+I$ ، اما $1+(1+2i)$ شریک $1+(-2+i)$ نیست .

(e) صحیح است . اگر هر عنصر R^* یکه یا اول باشد ، آنگاه هر عنصر R^* باید یکه باشد . زیرا فرض کنید $p \in R^*$ اول باشد و p^2 را در نظر بگیرید . واضح است که p^2 اول نیست و از آنجا که $p^2 \in (p) \neq R$ ، p^2 نمی تواند یکه باشد . بنابراین هر عنصر R^* یکه است و در نتیجه R میدان است .

۳-۲- در Z ، 5 تحویل ناپذیر است زیرا اول است .

در $Z[X]$، 5 تحویل ناپذیر است زیرا $5 = f(X)g(X)$ ایجاب می‌کند که $\deg g(X) = \deg f(X) = 0$. بنابراین $f(X)$ و $g(X)$ چند جمله ای ثابت هستند. پس یکی از چند جمله‌های f و g، ± 1 است .

در $Z[i]$ داریم $5 = (2+i)(2-i)$ که در آن نه $2+i$ و نه $2\text{-}i$ یکه است (زیرا $\ell(2+i) = \ell(2-i) = 5$)، بنابراین 5 تحویل ناپذیر است .

در $Z[\sqrt{-2}]$ ، 5 تحویل ناپذیر است . در حقیقت ، اگر $5 = \alpha\beta$ ، آنگاه $25 = \ell(5) = \ell(\alpha)\ell(\beta)$. اما اگر $\alpha = a + b\sqrt{-2}$ ، آنگاه $\ell(\alpha) = a^2 + 2b^2 \neq \pm 5$.

۴-۲- داریم که $\ell(43i-19) = 2210 = 2.5.13.17$. حال $\alpha = a + ib$ را در نظر بگیرید .
بنابراین طول α برابر است با

(۱) 2 اگر و فقط اگر $a^2 + b^2 = 2$ و این برقرار است اگر و فقط اگر α شریک 1+i باشد ؛

(۲) 5 اگر و فقط اگر $a^2 + b^2 = 5$ که این برقرار است اگر و فقط اگر α شریک 2+i یا 1+2i باشد ؛

(۳) 13 اگر و فقط اگر $a^2 + b^2 = 13$ و این برقرار است اگر و فقط اگر α شریک 3+2i یا 2+3i باشد ؛

(٤) 17 اگر و فقط اگر $a^2 + b^2 = 17$ که این برقرار است اگر و فقط اگر α شریک 4+ i یا 1+4i باشد .

حال بررسی کردن این موضوع ساده است که

$$43i-19=(2+3i)(1+i)(2+i)(4-i).$$

۲-۵- (**a**) 11+7i دارای اندازه 170=2.5.17 است . حال $1+i$ دارای اندازه 2 است و

$$(11+7i)\frac{1-i}{5}=\frac{1}{2}(11-11i+7i+7)=9-2i$$

(که دارای طول 5.17 است) و بنابراین $11+7i=(1+i)(9-2i)$. حال $1+2i$ دارای اندازه 5 بوده و

$$(9-2i)\frac{1-2i}{5}=\frac{1}{5}(9-2i-18i-4)=1-4i$$

(که دارای اندازه 17 است) و بنابراین $9-2i=(1+2i)(1-4i)$. بنابراین

$$11+7i=(1+i)(1+2i)(1-4i).$$

(**b**) $4+7\sqrt{2}=\sqrt{2}(7+2\sqrt{2})$.

(**c**) $4-\sqrt{-3}$ دارای اندازه 19 است که اول است ، بنابراین $4-\sqrt{-3}$ در $Z[\sqrt{-3}]$ تحویل ناپذیر است .

۲-۶- یکتایی تجزیه برقرار نمی باشد زیرا

$$6=2.3=\left[(-2+\sqrt{6})\ (2+\sqrt{6})\right]\ \left[(3-\sqrt{6})\ (3+\sqrt{6})\right]$$

$$=\left[(-2+\sqrt{6})\ (3+\sqrt{6})\right]\ \left[(2+\sqrt{6})\ (3-\sqrt{6})\right]$$

$$=\sqrt{6}\cdot\sqrt{6}$$

در $Z[\sqrt{10}]$ داریم

$$6=2.3=(4+\sqrt{10})\ (4-\sqrt{10})$$

که دو تجزیه متمایز 6 به تحویل ناپذیرها می‌باشد .

۲-۷- تنها یکه‌ها در $Z[\sqrt{-6}]$ ، ±1 هستند ، زیرا $a+b\sqrt{-6}$ یکه است اگر و فقط اگر $\ell(a+b\sqrt{-6})=a^2+6b^2=\pm1$ که نتیجه می‌دهد $b=0$ و $a=\pm1$. حال تجزیه های

$$10=2.5=(2+\sqrt{-6})(2-\sqrt{-6})$$

را در نظر بگیرید . $Z[\sqrt{-6}]$ دارای عنصری با اندازه 5 نمی باشد ، زیرا تساوی $a^2+6b^2=5$ به وضوح غیر ممکن است . بنابراین $2+\sqrt{-6}$ و $2-\sqrt{-6}$ تحویل ناپذیر هستند زیرا اندازه هر

یک از آنها 10 است و هر تجزیه آن شامل عنصری از مرتبه 5 است . مشابهاً 5 دارای اندازه 25 است و تحویل ناپذیر نمی باشد . همچنین چون تساوی $a^2 + 6b^2 = 2$ غیر ممکن است، عنصری با اندازه 2 نداریم . بنابراین 2 (از اندازه 4) تحویل ناپذیر است . بنابراین دو تجزیه متفاوت از 10 به حاصلضرب تحویل ناپذیرها داریم و بنابراین $Z[\sqrt{-6}]$ حوزه تجزیه یکتا نمی‌باشد .

(**a**) $2+\sqrt{-6}$ تحویل ناپذیر است اما اول نیست برای اینکه 10 را عاد می کند اما 2 و 5 را عاد نمی کند .

(*b*) بزرگترین مقسوم علیه مشترک 10 و $2(2+\sqrt{-6})$ وجود ندارد . در حقیقت 2 و $2+\sqrt{-6}$ ، 10 را عاد می‌کنند اما $2(2+\sqrt{-6})$ ، 10 را عاد نمی کند . زیرا $\ell[2(2+\sqrt{-6})] = 40$ که $\ell(10) = 100$ را عاد نمی کند .

(*c*) از آنجا که 5 و $2+\sqrt{-6}$ تحویل ناپذیر می‌باشند ، بزرگترین مقسوم علیه مشترک آنها وجود دارد و برابر با 1 است . فرض کنید $5\alpha + (2+\sqrt{-6})\beta = 1$. پس $10\alpha + 2(2+\sqrt{-6})\beta = 2$ که غیر ممکن است ، زیرا $2+\sqrt{-6}$ طرف چپ را عاد می کند ولی طرف راست را عاد نمی کند .

۸-۲- داریم

$$8 = 2.2.2 = (1+\sqrt{-7})(1-\sqrt{-7}) .$$

حال هر یک از عناصر 2 ، $1+\sqrt{-7}$ و $1-\sqrt{-7}$ تحویل ناپذیر است ، زیرا این عنصرها به ترتیب دارای طولهای 4 ، 8 ، 8 می‌باشند . بنابراین اگر یکی از آنها تحویل پذیر باشد ، آنگاه باید $a + b\sqrt{-7}$ موجود باشد به طوری که $a^2 + 7b^2 = 2$ ، که این به وضوح غیر ممکن است .

حال $8^k \in Z[\sqrt{-7}]$ را می‌توان به صورت‌های زیر نوشت :

$8^k = (1-\sqrt{-7})^k (1+\sqrt{-7})^k$	$2k$ عنصر تحویل ناپذیر
$= (1-\sqrt{-7})^{k-1} (1+\sqrt{-7})^{k-1} 2^3$	$2k+1$ عنصر تحویل ناپذیر
$= \dots$	
$= (1-\sqrt{-7})^{k-i} (1+\sqrt{-7})^{k-i} 2^{3i}$	$2k+i$ عنصر تحویل ناپذیر
$= \dots$	
$= 2^{3k}$	$3k$ عنصر تحویل ناپذیر

بنابراین با در نظر گرفتن t=2k ، نتیجه حاصل می‌شود .

یک عنصر تحویل ناپذیر که اول نیست عنصر 2 است . زیرا عنصر 2 ، عنصر $8 = \left(1+\sqrt{-7}\right)\left(1-\sqrt{-7}\right)$ را عاد می‌کند اما هیچکدام از عامل‌ها را عاد نمی کند .

از آنجا که 2 و $1+\sqrt{-7}$ تحویل ناپذیر هستند ، دارای بزرگترین مقسوم علیه مشترک 1 می‌باشند . فرض کنید که $1=\gamma 2+\delta\left(1+\sqrt{-7}\right)$. بنابراین با ضرب کردن طرفین در $1-\sqrt{-7}$ داریم

$$\gamma 2\left(1-\sqrt{-7}\right)+\delta 8=1-\sqrt{-7}.$$

اما 2 طرف چپ را عاد می‌کند ولی طرف راست را عاد نمی کند ، که یک تناقض است .

۲-۹- فرض کنید $I=(r)$. بنابراین برای $\alpha\in Z[i]$ای داریم $\alpha=\beta r+\gamma$ که در آن $N(\gamma)<N(r)$. چون $\frac{\gamma}{I}=\frac{\alpha}{I}$ و تعداد متناهی γ وجود دارد که $N(\gamma)<N(r)$، نتیجه می گیریم که $\frac{Z[i]}{I}$ متناهی است .

۲-۱۰- $\alpha=a+ib$ را یک عنصر اول در $Z[i]$ بگیرید . ابتدا فرض کنید که $\ell(\alpha)$ زوج است. بنابراین a^2+b^2 زوج است . از آنجا که a و b هر دو نمی توانند زوج باشند (در غیر این صورت می‌توانیم یک عامل 2 را استخراج کنیم و α نمی تواند اول باشد) ، در نتیجه هر دو باید فرد باشند . اما بنابراین

$$a+ib=\left[\frac{1}{2}(a+b)+\frac{1}{2}(b-a)i\right](1+i)،$$

که از آنجا $\alpha\sim 1+i$ ، زیرا $\frac{1}{2}(a+b)+\frac{1}{2}(b-a)i$ باید یکه باشد (در غیر این صورت $a+ib$ نباید اول باشد) .

حال فرض کنید $\ell(\alpha)$ فرد باشد . پس اگر a و b هر دو غیر صفر باشند ، آنگاه $\ell(\alpha)=a^2+b^2$ در Z اول است . زیرا در غیر این صورت $(a+ib)(a-ib)=a^2+b^2$ و یک تجزیه a^2+b^2 به اول‌ها در Z یک تناقض با اول بودن $a+ib$ دارد . حال $a+ib$ یک عامل $p=a^2+b^2$ که (هنگ 4) $p\equiv 1$ دارد و بنابراین (c) حاصل می‌شود .

اگر $b=0$، آنگاه $\alpha = a \in Z$ و باید اول باشد. اگر $a \equiv 1$ (هنگ 4)، آنگاه به ازای $d \in Z$ و c، $a = c^2 + d^2$ و بنابراین دوباره حالت (c) اتفاق می‌افتد. اگر $a \equiv 3$ (هنگ 4)، آنگاه حالت (b) رخ می‌دهد. اگر $a=0$، آنگاه α یک شریک $b \in Z$ است و یک بحث مشابه کارایی دارد.

۱۱-۲- (a) اگر $n < -1$، مثلاً $n = -p$، آنگاه معادله پل به صورت $a^2 + bp^2 = 1$ است. تنها جوابهای آن $a = \pm 1$ و $b=0$ است. بنابراین گروه یکه‌ها { 1 و -1 } است.

(b) اگر $n > 1$، آنگاه معادله پل به صورت $a^2 - nb^2 = \pm 1$ است. اگر قرار دهیم $\alpha = a + b\sqrt{n} \in R$ و $\overline{\alpha} = a - b\sqrt{n} \in R$، آنگاه $\alpha\overline{\alpha} = \pm 1$. این نتیجه می‌دهد که اگر α یکه باشد، آنگاه به ازای هر عدد صحیح $k \geq 1$، α^k یکه است، زیرا $\alpha^k \alpha^{-k} = \pm 1$.

(c) با استفاده از (b) مشاهده می‌کنیم که گروه یکه‌های $Z[\sqrt{2}]$ شامل مجموعه $\left\{ \pm\left(1+\sqrt{2}\right)^k \middle| k \geq 1 \right\}$ می‌باشد. حال فرض کنید که u یک یکه مثبت از $Z[\sqrt{2}]$ باشد، آنگاه به ازای $k \geq 1$ای داریم

$$\left(1+\sqrt{2}\right)^k \leq u < \left(1+\sqrt{2}\right)^{k+1}$$

که از آنجا نتیجه می‌شود که

$$1 \leq u\left(1+\sqrt{2}\right)^{-k} < 1+\sqrt{2}\,.$$

قرار دهید $u\left(1+\sqrt{2}\right)^{-k} = a + b\sqrt{2}$. بنابراین

$$1 \leq a + b\sqrt{2} < 1 + \sqrt{2}.$$

از آنجا که $b \in Z$ و a، خواهیم داشت که $a=1$ و $b=0$. بنابراین داریم $u\left(1+\sqrt{2}\right)^{-k} = 1$ و در نتیجه $u = \left(1+\sqrt{2}\right)^k$. پس مشاهده می‌کنیم که گروه یکه‌ها برابر با مجموعه $\left\{ \pm\left(1+\sqrt{2}\right)^k \middle| k \geq 1 \right\}$ است.

۱۲-۲- فرض کنید A یک ایده ال R باشد. بنابراین مجموعه

$$M = \{ m \in Z \mid \ \frac{m}{n} \in R \text{ برای بعضی از } \frac{m}{n} \in A \ \}$$

تشکیل یک ایده ال Z می‌دهد . زیرا اگر m_1 و $m_2 \in M$ ، آنگاه $\frac{m_2}{n_2} \in A$ و $\frac{m_1}{n_1}$ که از آنجا چون A ایده ال است ، داریم m_1 و $m_2 \in A$. در نتیجه $\frac{m_1 - m_2}{1} \in A$ که نشان می‌دهد $m_1 - m_2 \in M$. همچنین اگر $a \in Z$ ، آنگاه $\frac{a}{1}\frac{m_1}{n_1} \in A$ که نشان می‌دهد $am_1 \in M$.

حال هر ایده ال Z اصلی است . بنابراین $M = (m)$. پس اگر $m = p^k t$ جائیکه t و p نسبت به هم اول هستند ، آنگاه باید داشته باشیم $A = \left(\frac{p^k}{1}\right)$ ، که نشان می‌دهد A نیز اصلی است . با این وجود $\left(\frac{p}{1}\right)$ ایده ال ماکسیمال R شامل A است و بنابراین $\left(\frac{p}{1}\right)$ ایده ال ماکسیمال منحصر بفرد است که شامل هر ایده ال محض R است .

۲-۱۳- (a) اگر x و $y_1 \dots y_n$ نسبت به هم اول نباشند ، آنگاه عنصر تحویل ناپذیر $d \in D$ وجود دارد به طوری که $d|x$ و $d|y_1 \dots y_n$. از آنجا که در حوزه ایده الهای اصلی تحویل ناپذیری و اول بودن یکی هستند ، به ازای iای داریم $d|y_i$ و $d|x$ ، و این تناقض با این حقیقت است که x و y_i نسبت به هم اولند .

(b) اگر $p_i^{r_i}$ و $p_j^{r_j}$ نسبت به هم اول نباشند ، عنصر تحویل ناپذیر (=اول) $p \in D$ وجود دارد به طوری که $p|p_i^{r_i}$ و $p|p_j^{r_j}$ که از آنجا تناقض $p_i \sim p \sim p_j$ به دست می‌آید .

فرض کنید $b = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n}$ تجزیه یکتای b به حاصلضرب عوامل تحویل ناپذیر باشد . بنا به (c) عنصرهای $p_1^{r_1}, \dots, p_n^{r_n}$ دو به دو نسبت به هم اولند . از این رو بنا به (a) به ازای هر i عنصرهای $p_i^{r_i}$ و $\prod_{j \neq i} p_j^{r_j}$ نسبت به هم اولند . در نتیجه عنصرهای

$$\prod_{i \neq 1} p_i^{r_i}, \prod_{i \neq 2} p_i^{r_i}, \dots, \prod_{i \neq n} p_i^{r_i}$$

نسبت به هم اولند . بنابراین $\alpha_1, \alpha_2, \dots, \alpha_n$ وجود دارد به طوری که

$$1 = \alpha_1 \prod_{i \neq 1} p_i^{r_i} + \dots + \alpha_n \prod_{i \neq n} p_i^{r_i}$$

با ضرب کردن در a و تقسیم کردن به $b=\prod_{i=1}^{r} p_i^{r_i}$ بدست می‌آوریم

$$x=\frac{a}{b}=\frac{a\alpha_1}{p_1^{r_1}}+\ldots+\frac{a\alpha_n}{p_n^{r_n}}$$

۱۴-۲- $(1)\Longrightarrow(2)$: فرض کنید F یک خانواده از ایده الهای A باشد . $I_\circ \in F$ را انتخاب کنید . یا $I_\circ$ در F ماکسیمال است یا $I_1 \in F$ وجود دارد به طوری که $I_\circ \subset I_1$. یا I_1 در F ماکسیمال است و یا I_2 در F وجود دارد به طوری که $I_\circ \subset I_1 \subset I_2$. از آنجا که A نوتری است ، این روند در جائی متوقف می‌شود . ایده ال پایانی این روند یک ایده ال ماکسیمال در F است .

$(2)\Rightarrow(3)$: فرض کنید I ایده ال A و C را گردایه همه ایده الهای A مشمول در I بگیرید که متناهی - مولد می‌باشند . از آنجا که $(0)\in C$ ، به وضوح داریم $C\neq\phi$. بنا به (2)، C دارای عنصر ماکسیمال J است . برای $x\in I$ ایده ال $J+(x)$ را در نظر بگیرید . این ایده ال متناهی - مولد است (زیرا J متناهی- مولد است) و ایده‌الی از A است که مشمول در I است. بنابراین به C تعلق دارد . ماکسیمال بودن J ایجاب می کند $J=J+(x)$ و از آنجا $x\in J$ چون x عنصر دلخواه I بوده است ، نتیجه خواهیم گرفت که $I=J\in C$ و بنابراین I متناهی - مولد است .

$(3)\Rightarrow(1)$: فرض کنید $I_1\subseteq I_2\subseteq I_3\subseteq\ldots$ یک زنجیر صعودی از ایده الهای A باشد . بنا به فرض (3) هر ایده ال A متناهی مولد می‌شود . قرار دهید $I=\bigcup_{j\geq 1} I_j$. در این صورت I یک ایده ال است ، پس متناهی - مولد است . برای مثال توسط $\{x_1,x_2,\ldots,x_n\}$ تولید می‌شود . حالا هر x_i متعلق به بعضی از I_jها است ، فرض کنید k بزرگترین j باشد . در این صورت هر $x_i\in I_k$ و در نتیجه

$$I=(x_1,x_2,\ldots,x_n)\subseteq I_k$$

که از آنجا $I=I_k$. بنابراین $I_k=I_{k+1}=\ldots=I_{k+2}=\ldots$ و زنجیر ایستا می‌باشد .

$(\alpha)\Rightarrow(\beta)$: اگر A حوزه ایده ال اصلی باشد ، آنگاه هر ایده ال آن اصلی است . بنابراین متناهی - مولد است (در حقیقت توسط یک عنصر تولید می‌شود) . بنابراین از استلزام $(3)\Rightarrow(1)$ ، A نوتری است . همچنین مجموع دو ایده ال اصلی ، ایده ال اصلی است (زیرا هر ایده ال ، ایده ال اصلی است) .

$(\beta)\Rightarrow(\alpha)$: حال فرض کنید (β) درست بوده و I یک ایده ال A باشد . بنا به $(3)\Rightarrow(1)$ ، I متناهی – مولد است . مثلاً

$$I=(x_1,\dots,x_n)=(x_1)+\dots+(x_n)$$

با یک بحث ساده استقرایی نشان دهید (بنا به (β)) که هر مجموع متناهی از ایده الهای اصلی ، اصلی است بنابراین I اصلی است .

۲-۱۵- (**a**) $a|b$ ایجاب می کند که $b\in I=(a)$. اما a به گونه ای است که $N(a)$ برای کلیه عنصرهای I مینیمال است . بنابراین از آنجا که $N(b)=N(a)$ و $b\in I$ داریم $(a)=I=(b)$ و بنابراین a و b شریک هستند .

(**b**) فرض کنید $a,b\in R$ و هیچکدام دیگری را عاد نکنند . ایده ال $I=(a,b)$ که بوسیله a و b تولید می‌شود را در نظر بگیرید از آنجا که $b\notin(a)$ و $a\notin(b)$ ، مشاهده می‌کنیم که $I\neq(a)$ و $I\neq(b)$. حال $d\in I$ را که $N(d)$ مینیمال است انتخاب کنید . بنابراین $I=(d)$ و $N(d)<N(b), N(d)<N(a)$. از $d=(a,b)$ نتیجه می گیریم که $d\in(a,b)$ ، بنابراین $\alpha,\beta\in R$ وجود دارد که $d=\alpha a+\beta b$ ، که این همان مطلوب ما می‌باشد .

۲-۱۶- فرض کنید $a,b\in R\setminus\{0\}$ وجود دارد به طوری که

$$\delta(a+b)>\max(\delta(a),\delta(b)) .$$

بنابراین از

$$b=0(a+b)+b \text{ ، } b=1(a+b)-a$$

با $\delta(-a)=\delta(a)<\delta(a+b)$ و $\delta(b)<\delta(a+b)$ ، مشاهده می‌کنیم که خارج قسمت و باقیمانده منحصر به فرد نیست .

بر عکس ، فرض کنید $\delta(a+b)\le\max(\delta(a),\delta(b))$ و $a\in R$ دارای دو نمایش باشد مثلاً

$$a=qb+r \ (\ r=0 \text{ یا } \delta(r)<\delta(b)\ ) ؛$$

$$a=q'b+r' \ (\ r'=0 \text{ یا } \delta(r')<\delta(b)\ ) ؛$$

و $r\neq r'$ و $q\neq q'$. بنابراین تناقض زیر حاصل می‌شود ،

$$\delta(b)\le\delta[(q-q')b]=\delta(r'-r)<\max(\delta(r'),\delta(-r))<\delta(b).$$

بنابراین $r=r'$ و $q=q'$. از آنجا که هر یک دیگری را ایجاب می کند منحصر بفردی نتیجه می‌شود .

$a=1+4i$ و $b=5+3i$ را در $Z[i]$ بگیرید. پس داریم

$$\begin{aligned}1+4i &= (5+3i)(1+i)+(-1-4i)\\ &= (5+3i)i+(4-i).\end{aligned}$$

۲-۱۷- (**a**) داریم $-1+3i=(1+i)(1+2i)$. از آنجا که $\ell(1+i)=2$ و $\ell(1+2i)=5$ مشاهده می‌کنیم که $1+i$ و $1+2i$ تحویل ناپذیر می‌باشند.

(**b**) از آنجا که $g.c.d.(a_0,...,a_n)=1$ ، نمی توان برای یک عنصر تحویل ناپذیر a نوشت $f(X)=af_1(X)$. بنابراین اگر $f(X)$ تحویل پذیر باشد، می‌توان فرض کرد که $f(X)=g(X)h(X)$ جائیکه

$$\begin{aligned}g(X)&=b_0+b_1X+...+b_rX^r\\ h(X)&=c_0+c_1X+...+c_sX^s\end{aligned}$$

با $r,s<n$. حال $a_0=b_0c_0$ و بنابراین از آنجا که $p|a_0$ داریم $p|b_0$ یا $p|c_0$. همچنین از آنجا که p^2 ، b_0c_0 را عاد نمی کند می‌توان فرض کرد که $p|b_0$ و p عنصر c_0 را عاد نمی کند. اگر برای هر i ، $p|b_i$ ، آنگاه $p|a_n$ که تناقض است. بنابراین اولین ضریب مانند b_t وجود دارد که p ، b_t را عاد نمی کند. اما

$$a_t=(b_0c_t+...+b_{t-1}c_1)+b_tc_0$$

و از آنجا که $p|b_i$ برای $0\le i<t$ ، p عبارت داخل پرانتز را عاد می‌کند. بنابراین p ، a_t را عاد نمی کند زیرا p ، b_tc_0 را عاد نمی کند. از آنجا که $t<n$ این تناقض به دست می‌آید.

(**c**) از آنجا که $-1+3i=(1+i)(1+2i)$ ، قرار دهید $p=1+i$ و توجه کنیم که $p|(-1+3i)$ اما p^2 ، $-1+3i$ را عاد نمی کند. همچنین به دلیل اینکه $(1+i)(1-i)=2$ ، مشاهده می‌کنیم که $p|6$ و $p|8i$ اما p ، 1 را عاد نمی کند. بنابراین، بنا به (b)، چند جمله ای $X^3+8iX^2-6X-1+3i$ در $Z[i][X]$ تحویل ناپذیر است.

۲-۱۸- $Z[\sqrt{3}]$ حوزه اقلیدسی است، بنابراین هر دو عنصر غیر صفر آن دارای بزرگترین مقسوم علیه مشترک است. به عنوان حاصلضربهایی از تحویل ناپذیرها داریم

$$13=(4-\sqrt{3})(4+\sqrt{3}),$$
$$7+5\sqrt{3}=(1+\sqrt{3})(4+\sqrt{3}).$$

بنابراین بزرگترین مقسوم علیه مشترک آنها $4+\sqrt{3}$ است .

۱۹-۲- (**a**) $a^2+5b^2=\pm 1$ اگر و تنها اگر $a=\pm 1$ و $b=0$. بنابراین اگر $\left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)=1$ ، آنگاه

$$\left(a^2+5b^2\right)\left(c^2+5d^2\right)=\ell\left(a+b\sqrt{-5}\right)\ell\left(c+d\sqrt{-5}\right)=\ell(1)=1$$

در نتیجه $a^2+5b^2=1=c^2+5d^2$ و نتیجه حاصل می‌شود .

(**b**) $\ell(3)=\ell\left(2+\sqrt{-5}\right)=\ell\left(2-\sqrt{-5}\right)=9$ ، بنابراین اگر z یکی از عاملهای 3 ، $2+\sqrt{-5}$ ، $2-\sqrt{-5}$ باشد ، آنگاه باید داشته باشیم $\ell(z)\in\{1,3,9\}$. حال اگر $\ell(z)=3$ ، داریم $z=a+b\sqrt{-5}$ که در آن $a,b\in Z$ بوده و $a^2+5b^2=3$. که بوضوح جواب ندارد .

بنابراین اگر z یک عامل باشد ، آنگاه باید داشته باشیم $\ell(z)=1$ یا $\ell(z)=9$. در هر دو حالت یکی از عاملها از اندازه یک می‌باشد که نشان می‌دهد آن یکه است .

(**c**) داریم $9=3.3=\left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right)$. برای آنکه نشان دهیم اینها دو تجزیه متفاوت هستند کافی است مشاهده کنیم که برای هر یکه z ، $3z\neq 2+\sqrt{-5}$، زیرا تنها یکه‌ها ± 1 هستند .

(**d**) برای آنکه نشان دهیم $P_1=\left(3,2+\sqrt{-5}\right)$ اول است ، $P_1\bigcap Z$ را در نظر می‌گیریم . داریم $3\in P_1\bigcap Z$ و اگر عدد صحیحی که توسط 3 عاد نشود در $P_1\bigcap Z$ باشد بنا به الگوریتم اقلیدسی ، $1\in P_1\bigcap Z$ و تناقض $P_1=Z[\sqrt{-5}]$ را داریم . بنابراین مشاهده می‌کنیم که $P_1\bigcap Z=3Z$. برای $x,y\in Z[\sqrt{-5}]$ ، اعداد صحیح u و v را بگونه ای انتخاب کنید که

$$x-u\in P_1, y-v\in P_1 .$$

فرض کنید $xy\in P_1$. بنابراین $uv\in P_1$ و از آنجا که $uv\in Z$ ، داریم $uv\in P_1\bigcap Z=3Z$. پس $u\in 3Z$ یا $v\in 3Z$ ، بنابراین یا $x\in P_1$ یا $y\in P_1$. از این رو P_1 اول است . به طور مشابه ، $P_2=\left(3,2-\sqrt{-5}\right)$ اول است .

(**e**) با نمادهای فوق ، از آنجا که

$$1=-3+\left(2+\sqrt{-5}\right)+\left(2-\sqrt{-5}\right)\in\left(3,2+\sqrt{-5},2-\sqrt{-5}\right)$$

داریم

$$P_1P_2 = \left(3,2+\sqrt{-5}\right)\left(3,2-\sqrt{-5}\right) = (3)\left(3,2+\sqrt{-5},2-\sqrt{-5}\right) = (3)$$

۲۰-۲- ابتدا توجه کنید که

$$m+n\sqrt{10} \in P_1 \Leftrightarrow 2 | m$$

$$m+n\sqrt{10} \in P_2 \Leftrightarrow m-n \equiv 0 \ (\text{هنگ } 3)$$

$$m+n\sqrt{10} \in P_3 \Leftrightarrow m+n \equiv 0 \ (\text{هنگ } 3)$$

با استفاده از این می‌توان نشان داد که هر یک از P_1 ، P_2 و P_3 اول هستند. برای مثال اگر

$$\left(m_1+n_1\sqrt{10}\right)\left(m_2+n_2\sqrt{10}\right) \in P_2$$

آنگاه داریم

$$3 \,\Big|\, \left[(m_1-n_1)(m_2-n_2)+9n_1n_2\right].$$

بنابراین $3|(m_2-n_2)$ یا $3|(m_1-n_1)$.

حال $(6)=(2)(3)=\left(4+\sqrt{10}\right)\left(4-\sqrt{10}\right)$ و

$$(2)=P_1^2, (3)=P_2P_3 \text{ ، } \left(4+\sqrt{10}\right)=P_1P_2 \text{ ، } \left(4-\sqrt{10}\right)=P_1P_3$$

پس هر دو تجزیه عنصر 6 ما را به تجزیه ایده آل (6) به حاصلضرب ایده آل‌های اول به صورت

$$(6)=P_1^2P_2P_3$$

هدایت می کند .

حل مسائل فصل سوم

۱-۳- قضیه دو جمله ای (که در هر حلقه تعویض پذیر یکدار درست است) نتیجه می دهد که

$$(a+b)^p = \sum_{r=0}^{p} \binom{p}{r} a^{p-r} b^r, \qquad (a-b)^p = \sum_{r=0}^{p} \binom{p}{r} (-1)^r a^{p-r} b^r .$$

برای $0 < r < p$ ضریب $\binom{p}{r} = \frac{p!}{r!(p-r)!}$ عدد صحیح است . چون $p|p!$ و $r!$ و $(p-r)!$ توسط p عاد نمی‌شود که مشاهده می کنیم $\binom{p}{r}$ عدد صحیحی است که توسط p عاد می شود . بنابراین داریم

$$(a+b)^p = a^p + b^p$$

و اگر p فرد باشد ،

$$(a-b)^p = a^p + (-1)^p b^p = a^p - b^p$$

اگر p زوج باشد ، آنگاه باید p=2 که در این حالت

$$(a-b)^2 = a^2 + b^2 = a^2 - b^2 + 2b^2 = a^2 - b^2$$

برای قسمت دوم از استقراء استفاده می کنیم . نتیجه برای $n = 1$ برقرار است . برای گام استقراء فرض کنید که

$$(a \pm b)^{pk} = a^{pk} \pm b^{pk}$$

که در آن $k>1$. در این صورت داریم

$$(a \pm b)^{p^{k+1}} = [(a \pm b)^{p^k}]^p = (a^{p^k} \pm b^{p^k})^p$$
$$= (a^{p^k})^p \pm (b^{p^k})^p = a^{p^{k+1}} \pm b^{p^{k+1}}$$

۲-۳- اگر F از مشخصه صفر باشد ، آنگاه واضح است که

$$Df = 0 \Leftrightarrow a_1 = a_2 = \ldots = a_n = 0 \Leftrightarrow f = a_0 \ .$$

حال اگر F از مشخصه p باشد ، آنگاه

(۱) اگر $p|k$ ، داریم

$$ka_k = (k1)a_k = 0a_k = 0 \ ؛$$

(۲) اگر p ، k را عاد نکند داریم

$$ka_k = 0 \Rightarrow (k1)a_k = 0 \Rightarrow a_k = 0 \ .$$

بنابراین $Df = 0$ اگر و تنها اگر f به صورت

$$a_0 + a_p X^p + a_{2p} X^{2p} + \ldots + a_{rp} X^{rp}$$

باشد .

۳-۳- به وضوح هر چند جمله ای ثابت غیر صفر در $F[X]$ یکه است . که اینها کلیه یکه ها هستند زیرا اگر f و g چند جمله ای های غیر ثابت باشند ، آنگاه $\deg fg \geq \deg f \geq 1$. پس fg غیر ثابت است . بنابراین چند جمله ای از درجه بزرگتر از صفر یکه نمی باشد .

اگر $\varphi : F[X] \to F[X]$ یک خود ریختی باشد ، آنگاه φ یکه ها را به یکه ها می برد (زیرا یکه ها عنصرهای وارون پذیر هستند) . بنابراین تصویر چند جمله ایهای ثابت غیر صفر تحت φ ، چند جمله ای ثابت غیر صفر می باشد .

$v : F \to F$ را بدین صورت تعریف می کنیم که $v(0) = 0$ و به ازای هر $v(a), a \neq 0$ را چند جمله ای ثابت $\varphi(a)$ بگیرید . بنابراین واضح است که v یک خود ریختی روی F است و نمودار

$$\begin{tikzcd} F \arrow[r, "i"] \arrow[d, "v"'] & F[X] \arrow[d, "\varphi"] \\ F \arrow[r, "i"'] & F[X] \end{tikzcd}$$

تعویض پذیر است . برای تک جمله ای $X \in F[X]$ ، $\varphi(X) \in F[X]$ را در نظر بگیرید . اگر $\deg \varphi(X) < 1$ ، آنگاه φ چند جمله ای ثابت است . بنابراین

$$\varphi(a_0 + a_1X + ... + a_nX^n) = \nu(a_0) + \nu(a_1)\varphi(X) + ... + \nu(a_n)(\varphi(X))^n$$

نیز یک چند جمله ای ثابت است . این غیر ممکن است زیرا φ یک خود ریختی است. حال اگر $\deg\varphi = k > 1$ ، آنگاه تصویر $\varphi(f)$ از یک چند جمله ای درجه n باید دارای درجه nk باشد . بنابراین تنها چند جمله ای های از درجه k , 2k , 3k , ... می توانند در تصویر φ ظاهر شوند . مجدداً از آنجا که φ خود ریختی است این امر غیر ممکن است . بنابراین باید $1 = \deg\varphi(X)$ ، پس به ازای $a \neq 0$ ای ، $\varphi(X) = aX + b$.

۴-۳- f ، g هم ارزند اگر و فقط اگر

$$(f-g)(\alpha) = 0 \qquad (\forall \alpha \in F)$$

که این اتفاق می افتد اگر و فقط اگر به ازای هر $\alpha \in F$ ، $X-\alpha$ چند جمله ای $f-g$ را عاد کند. فرض کنید $\deg(f-g) = n$.

اگر F نا متناهی بوده و f و g هم ارز باشند ،آنگاه برای $n+1$ عنصر متمایز $\alpha_0, \alpha_1, ..., \alpha_n$ در F ، $f-g$ تقسیم پذیر به چند جمله ای از درجه $n+1$ ،

$$(X-\alpha_0)(X-\alpha_1)...(X-\alpha_n)$$

می باشد . از آنجا که هر چند جمله ای غیر صفر از درجه n دارای حداکثر n ریشه متمایز است ، نتیجه می گیریم که $f-g=0$ و بنابراین $f = g$.

اگر F متناهی باشد ، مثلاً $F = \{a_1, a_2, ..., a_n\}$ ، آنگاه بحث فوق نشان می دهد که $f-g$ بر

$$m(X) = (X-a_1)(X-a_2)...(X-a_n)$$

تقسیم پذیر می باشد .

بر عکس ، اگر $f-g$ تقسیم پذیر بر $m(X)$ باشد ، آنگاه واضح است که f و g هم ارزند.

در حالت $F = GF(p) = Z/_{PZ}$ ، داریم

$$m(X) = X(X-\overline{1})(X-\overline{2})...(X-\overline{p-1}) .$$

از آنجا که برای $\alpha = \overline{0}, \overline{1}, ..., \overline{p-1}$ داریم $\alpha^p = \alpha$ [قضیه فرما را بخاطر آورید که می گوید $\alpha^{p-1} \equiv 1 \bmod P$]، پس $X-\alpha$ چندجمله ای $X^p - X$ را عاد می کند بنابراین $m(X)$ چند جمله ای $X^p - X$ را عاد می کند ، مثلاً $X^p - X = m(X)h(X)$. محاسبه درجات

نتیجه می دهد که $p= p + \deg h$ و بنابراین $h(X)$ یک چند جمله ای ثابت غیر صفر است . محاسبه ضرایب پیشرو نتیجه می دهد که $h(X) =1$ و بنابراین $m(X) = X^p - X$.

۳-۵- $X^2 + Y^2 -1$ را به عنوان یک عنصر $F[Y][X]=F[X,Y]$ در نظر بگیرید : یعنی به عنوان یک چندجمله ای در X با ضرایب در $F[Y]$. حال $Y+1$ یک عنصر تحویل ناپذیر در $F[Y]$ است و $Y+1$ عبارت $Y^2 -1$ را عاد می کند .

همچنین $(Y+1)^2$ عبارت Y^2-1 را عاد نمی کند ، زیرا در غیر این صورت چون هر دو تکین هستند ، داریم $(Y+1)^2 = Y^2 - 1$ که از آنجا $2Y + 2\times 1 = 0$ و این ممکن است فقط اگر F از مشخصه 2 باشد . بنابراین می توانیم نتیجه سئوال (d) ۱۷-۲ را بکار ببریم و ببینیم که $X^2 + Y^2 - 1$ در $F[X,Y]$ تحویل ناپذیر است .

۳-٦- ریختار $Z[X] \to Z_n[X]$ از توسیع ریختار طبیعی $Z \to Z_n$ ، به سادگی از تحدید ضرایب به هنگ n بدست می آید .

برای $f \in Z[X]$ ، عدد طبیعی n را طوری انتخاب کنید که n ضریب پیشرو f را عاد نکند . اگر f روی Z تجزیه شود، آنگاه تصویر f تحت ریختار روی Z_n تجزیه می شود . بنابراین اگر تصویر f روی Z_n تحویل ناپذیر باشد ، آنگاه f باید روی Z تحویل ناپذیر باشد . تمامی نکات قبلی برای آزمون تحویل ناپذیری مفید است ، زیرا Z_n متناهی است و بنابراین فقط تعداد متناهی حالت برای بررسی کردن وجود دارد.

در $Z_5[X]$ داریم $X^4 + 15X^3 + 7 = X^4 + 2$. این چند جمله ای عامل خطی ندارد ، زیرا $t \in Z_5$ ای وجود ندارد که در معادله $t^4 + 2 = 0$ صدق کند . فرض کنید که

$$X^4 + 2 = (X^2+ aX + b)(X^2 + cX + d)$$

بنابراین

$$a + c =0 , ac + b+ d =0 , ad + bc =0 , bd = 2$$

از $a = -c$ داریم $a(b-d) = 0$. اگر $a = 0$ ، آنگاه $b = -d$ و بنابراین $b^2 = -2 = 3$ ، در حالی که اگر $b = d$ ، آنگاه $b^2 = 2$. با این وجود $0 , 1 , 4$ تنها مربعات در Z_5 می باشند . بنابراین نه $b^2 = 3$ و نه $b^2=2$ ممکن است . بنابراین مشاهده می کنیم که $X^4 + 2$ روی Z_5 تحویل نا پذیر است . بنا به بحث فوق این چند جمله ای روی Z تحویل نا پذیر است . اما اگر روی Q تحویل پذیر بود ، آنگاه باید روی Z نیز تحویل پذیر باشد .

۳-۷- $\{1,\sqrt{2}\}$ یک پایه برای $Q(\sqrt{2})$ روی Q است و $\{1,\sqrt[3]{2},\sqrt[3]{2^2}\}$ یک پایه برای $(\sqrt[3]{2})$ $Q(\sqrt{2})$ روی $Q(\sqrt{2})$ است . بنابراین

$$\{1,\sqrt{2},\sqrt[3]{2},2^{5/6},2^{2/3},2^{7/6}\}$$

یک پایه برای $Q(\sqrt{2},\sqrt[3]{2})$ روی Q است .

حال داریم $2^{7/6}=2.2^{1/6}$. بنابراین $2^{1/6}\in Q(\sqrt{2},\sqrt[3]{2})$ و بنابراین

$$Q\subseteq Q(\sqrt[6]{2})\subseteq Q(\sqrt{2},\sqrt[3]{2})$$

$\sqrt[6]{2}$ یک ریشه X^6-2 است (که با توجه به محک ایزنشتین روی Q تحول ناپذیر است) . بنابراین چند جمله ای مینیمال $\sqrt[6]{2}$ روی Q است . بنابراین داریم ،

$$6=\left[Q\left(\sqrt{2},\sqrt[3]{2}\right):Q\right]=\left[Q\left(\sqrt{2},\sqrt[3]{2}\right):Q\left(\sqrt[6]{2}\right)\right]\ \left[Q\left(\sqrt[6]{2}\right):Q\right]$$
$$=\left[Q((\sqrt{2},\sqrt[3]{2}):Q(\sqrt[6]{2})\right]\times 6$$

بنابراین $[Q(\sqrt{2},\sqrt[3]{2}):Q(\sqrt[6]{2})]=1$ و از این رو $Q(\sqrt{2},\sqrt[3]{2})=Q(\sqrt[6]{2})$ یک توسیع ساده است .

۳-۸- فرض کنید Z روی F جبری باشد ، بنابراین باید یک چند جمله ای

$$f(X)=a_0+a_1X+\ldots+a_nX^n,\quad (a_n\neq 0)$$

روی F موجود باشد که $f(Z)=0$. یعنی

$$a_0+a_1(\frac{X^3}{X+1})+a_2(\frac{X^3}{X+1})^2+\ldots+a_n(\frac{X^3}{X+1})^n=0 ،$$

که نتیجه می دهد

$$a_nX^{3n}+a_{n-1}X^{3n-3}(X+1)+\ldots+a_0(X+1)^n=0 .$$

از آنجا که طرف چپ یک چند جمله ای غیر صفر از درجه $3n$ می باشد ، یک تناقض بدست می آید . بنابراین Z باید روی F غیر جبری باشد .

حال در $(F(Z))[Y]$ ، عنصر X در $Y^3-ZY-Z=0$ صدق می کند . اما Y^3-ZY-Z در $(F(Z))[Y]$ تحویل ناپذیر است ، زیرا اگر چنین نباشد دارای یک عامل خطی $Y-\alpha$ است که $\alpha\in F(Z)$ بوده و $\alpha^3-Z\alpha-Z=0$ و این نتیجه می دهد که چند جمله ای غیر صفر f وجود دارد که $f\ (Z)=0$ و همان طور که قبلاً دیدیم این غیر ممکن است . پس مشاهده می کنیم

که $Y^3 - ZY - Z$ چند جمله ای مینیمال X روی $F(Z)$ است. بنابراین $F(X)$ توسیع ساده جبری از $F(Z)$ است.

۹-۳- بنا به محک ایزنشتین هر دو تحول نا پذیرند. داریم

$$X^2 - 3 = (X - \sqrt{3})(X + \sqrt{3})$$
$$X^2 - 2X - 2 = (X - 1 - \sqrt{3})(X - 1 + \sqrt{3})$$

و میدان شکافنده هر کدام $Q(\sqrt{3})$ است.

۱۰-۳- روی $\mathbb{C}$ داریم

$$.(X^2 - 2X - 2)(X^2 + 1) = (X - 1 + \sqrt{3})(X - 1 - \sqrt{3})(X - i)(X + i)$$

بنابراین $Q(\sqrt{3}, i)$ یک میدان شکافنده است.

پس

$$X^5 - 3X^3 + X^2 - 3 = (X^2 - 3)(X^3 + 1)$$
$$= (X - \sqrt{3})(X + \sqrt{3})(X + 1)(X - \frac{1}{2}(-1 + i\sqrt{3}))(X - \frac{1}{2}(-1 - i\sqrt{3}))$$

و میدان شکافنده آن $Q(\sqrt{3}, \frac{1}{2}(-1 + i\sqrt{3})) = Q(\sqrt{3}, i)$ می باشد.

قرار دهید $K = Q(\sqrt{3}, i)$. حال $\sqrt{3}$ دارای چند جمله ای مینیمال $X^2 - 3$ روی Q است، بنابراین $[Q(\sqrt{3}) : Q] = 2$. از آنجا که $i \notin Q(\sqrt{3})$ و i دارای چند جمله ای مینیمال $X^2 + 1$ روی $Q(\sqrt{3})$ است، داریم $[Q(\sqrt{3}, i) : Q(\sqrt{3})] = 2$. بنابراین

$$[K : Q] = [K : Q(\sqrt{3})]\ [Q(\sqrt{3}) : Q] = 2.2 = 4 .$$

۱۱-۳- به سادگی دیده می شود که

$$X^3 - 3abX + a^3 + b^3 = (X + a + b)(X^2 + (a + b)X + (a + b)^2 - 3ab) .$$

چون $X^6 - 6X^3 + 8 = (X^3 - 2)(X^3 - 4)$، بنابراین یک میدان شکافنده آن روی Q میدان $Q(\sqrt[3]{2}, \sqrt[3]{4}, i\sqrt{3})$ است. اما $(\sqrt[3]{2})^2 = \sqrt[3]{4}$، بنابراین $Q(\sqrt[3]{2}, \sqrt[3]{4}, i\sqrt{3}) = Q(\sqrt[3]{2}, i\sqrt{3})$. از این رو $S = Q(\sqrt[3]{2}, i\sqrt{3})$ و

$$[S : Q] = [Q(\sqrt[3]{2}, i\sqrt{3}) : Q(\sqrt[3]{2})]\ [Q(\sqrt[3]{2}) : Q] = 2.3 = 6 .$$

از آنجا که S شامل $\sqrt[3]{2}$ و $\sqrt[3]{4}$ می باشد ، داریم $\sqrt[3]{2}+\sqrt[3]{4}\in S$. حال با قراردادن $b=-\sqrt[3]{2}$، و $a=-\sqrt[3]{4}$ در قسمت اول سئوال مشاهده می‌کنیم که $X-(\sqrt[3]{4}+\sqrt[3]{2})$ عبارت X^3-6X-6 را عاد می کند . به دلیل آنکه $\sqrt[3]{4}+\sqrt[3]{2}\in S$ دارای درجه 3 روی Q است و $\sqrt[3]{4}+\sqrt[3]{2}\notin Q$ ، مشاهده می کنیم که چند جمله ای مینیمال $\sqrt[3]{4}+\sqrt[3]{2}$ روی Q درجه سه است . بنابراین با توجه به مشاهدات بالا چند جمله ای مینیمال آن باید X^3-6X-6 باشد .

از آنجا که $\sqrt[3]{4}+\sqrt[3]{2}\in S$ داریم $Q(\sqrt[3]{4}+\sqrt[3]{2})\subseteq S$. اما $Q(\sqrt[3]{4}+\sqrt[3]{2})$ دارای درجه 3 روی Q است . در صورتی که S دارای درجه 6 است . بنابراین نتیجه می گیریم که $S\neq Q(\sqrt[3]{4}+\sqrt[3]{2})$.

۳-۱۲- در $Q[X]$ داریم

$$f(X)=(X^2+4X+1)(X^2-2X-1)$$

و در $R[X]$ داریم

$$f(X)=(X+2-\sqrt{3})(X+2+\sqrt{3})(X-1-\sqrt{2})(X-1+\sqrt{2}).$$

بنابراین $K=Q(\sqrt{2},\sqrt{3})$ یک میدان شکافنده برای f است . حال اگر $\sqrt{3}\in Q(\sqrt{2})$ ، آنگاه $a,b\in Q$ وجود دارد به طوری که $\sqrt{3}=a+b\sqrt{2}$ ، که از آنجا داریم

$$3=a^2+2b^2-2ab\sqrt{2}.$$

اگر $a,b\neq 0$ ، آنگاه تناقض $\sqrt{2}\in Q$ را داریم . اگر $a=0$ ، آنگاه $\sqrt{3}=b\sqrt{2}$ و بنابراین $\sqrt{6}=2b\in Q$. که تناقض دیگری است . اگر $b=0$ ، آنگاه $\sqrt{3}=a\in Q$ که مجدداً یک تناقض است . بنابراین مشاهده می کنیم که $\sqrt{3}\notin Q(\sqrt{2})$ و بنابراین

$$[Q(\sqrt{2},\sqrt{3}):Q]=[Q(\sqrt{2},\sqrt{3}):Q(\sqrt{2})]\ [Q(\sqrt{2}):Q]=2.2=4$$

مجموعه $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ یک پایه برای $Q(\sqrt{2},\sqrt{3})$ روی Q است . حال چند جمله‌ای مینیمال $\sqrt{3}-\sqrt{2}$ دارای درجه 2 یا 4 است . اگر درجه 2 باشد ، آنگاه برای بعضی از $a,b\in Q$ داریم

$$(\sqrt{3}-\sqrt{2})^2+a(\sqrt{3}-\sqrt{2})+b=0$$

که نتیجه می دهد

$$b+5+a\sqrt{3}-a\sqrt{2}-2\sqrt{6}=0$$

که یک تناقض با پایه بودن $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ است .

بنابراین مشاهده می کنیم که درجه چند جمله ای مینیمال 4 است و $Q(\sqrt{2},\sqrt{3}) = Q(\sqrt{3}-\sqrt{2})$.

چند جمله ای مینیمال $\sqrt{3}-\sqrt{2}$ روی Q، X^4-10X^2+1 است، در حالی که روی $Q(\sqrt{3})$، چند جمله ای مینیمال $X^2-2\sqrt{3}+1$ است.

۱۳-۳- داریم که

$$X^4 - X^2 - 2 = (X^2-2)(X^2+1)$$

به طوری که X^2+1 و X^2+2 تحویل ناپذیر روی Q هستند. حال در $(\mathbb{C})$ داریم

$$X^4 - X^2 - 2 = (X-\sqrt{2})(X+\sqrt{2})(X-i)(X+i).$$

بنابراین f کاملاً روی $Q(\sqrt{2},i)$ تجزیه می شود. از آنجا که به وضوح f نمی تواند در هر زیر میدان کوچکتر $\mathbb{C}$ شکافنده باشد، $K = Q(\sqrt{2},i)$ یک میدان شکافنده است. حال $\sqrt{2}$ دارای چند جمله ای مینیمال X^2-2 روی Q است. بنابراین $[Q(\sqrt{2}):Q]=2$. به دلیل آنکه $i \notin Q(\sqrt{2})$ و i دارای چند جمله ای مینیمال X^2+1 روی $Q(\sqrt{2})$ است، داریم $[Q(\sqrt{2},i):Q(\sqrt{2})]=2$. بنابراین

$$[K:Q] = [K:Q(\sqrt{2})]\ [Q(\sqrt{2}):Q] = 2.2 = 4.$$

$\{1,\sqrt{2},i,i\sqrt{2}\}$ یک پایه برای K روی Q است. چون $Q(i+\sqrt{2}) \subseteq Q(i,\sqrt{2})$، آنگاه $[Q(i+\sqrt{2}):Q]$ برابر با 2 یا 4 است. حال $(i+\sqrt{2})^2 = 1+2i\sqrt{2}$ و اگر چند جمله ای مینیمال $i+\sqrt{2}$ از درجه 2 باشد، می توان $a,b \in Q$ را به گونه ای پیدا کرد که

$$0 = (i+\sqrt{2})^2 + a(i+\sqrt{2}) + b = b+1+a\sqrt{2}+ai+2i\sqrt{2}$$

که متناقض با پایه بودن $\{1,\sqrt{2},i,i\sqrt{2}\}$ است. بنابراین چند جمله ای مینیمال $i+\sqrt{2}$ از درجه 4 است و بنابراین $[Q(i+\sqrt{2}):Q]=4$، و در نتیجه $Q(i+\sqrt{2}) = Q(i,\sqrt{2})$.

به وضوح چون $(i+\sqrt{2})^2 = 1+2i\sqrt{2}$ داریم

$$(i+\sqrt{2})^4 = (1+2i\sqrt{2})^2 = -7+4i\sqrt{2},$$

و بنابراین

$$(i+\sqrt{2})^4 - 2(i+\sqrt{2})^2 + 9 = 0$$

که در نتیجه چند جمله ای مینیمال $i+\sqrt{2}$، چند جمله ای X^4-2X^2+9 است.

a) چون $(i+\sqrt{2})^2 = 1+2i\sqrt{2} = 1+2i(i+\sqrt{2})+2$ ، پس چند جمله ای مینیمال $i+\sqrt{2}$ روی $\mathrm{Q(i)}$ ، $X^2-2iX-3$ است .

b) از آنجا که $(i+\sqrt{2})^2 = 1+2i\sqrt{2} = 1+2\sqrt{2}(i+\sqrt{2})-4$ ، بنابراین چند جمله ای مینیمال $i+\sqrt{2}$ روی $Q(\sqrt{2})$ ، $X^2-2\sqrt{2}X+3$ است .

c) چون $(i+\sqrt{2})^2 = 1+2i\sqrt{2}$ پس چند جمله ای مینیمال $i+\sqrt{2}$ روی $Q(i\sqrt{2})$ ، $X^2-1-2i\sqrt{2}$ است .

۱۴-۳- $(1) \Rightarrow (2)$: اگر f تحویل پذیر باشد ، آنگاه آن دارای یک عامل خطی یا یک عامل درجه دوم است . اگر دارای عامل خطی $X-\alpha$ باشد ، آنگاه α یک ریشه است، که از آنجا همچنین $-\alpha$ نیز یک ریشه است . بنابراین f دارای عامل $X+\alpha$ نیز می‌باشد . پس f دارای عامل درجه دوم $(X+\alpha)(X-\alpha)$ است .

$(2) \Rightarrow (3)$: اگر $X^4+r = (X^2+\alpha X+\beta)(X^2+\alpha' X+\beta')$ ، آنگاه

$$\alpha+\alpha'=0,\ \ \beta+\beta'+\alpha\alpha'=0,\ \ \alpha\beta'+\alpha'\beta=0,\ \ \beta\beta'=r\,.$$

اگر $\alpha \neq 0$ ، آنگاه $\alpha'=-\alpha$. بنابراین $\alpha(\beta'-\beta)=0$ ، پس $\beta'=\beta$ ، که نتیجه می دهد $r=\beta^2$ با $2\beta=-\alpha\alpha'=\alpha^2$ یعنی $r=\frac{1}{4}\alpha^4$.

اگر $\alpha=0$ ، آنگاه $\alpha'=0$ ، $\beta'=-\beta$ ، و $r=-\beta^2$.

$(3) \Rightarrow (1)$: اگر $r=-p^2$ ، آنگاه $X^4+r = X^4-p^2 = (X^2+p)(X^2-p)$ و اگر $r=\frac{1}{4}q^4$ ، آنگاه

$$X^4+r = X^4+\frac{1}{4}q^4 = (X^2+qX+\frac{1}{2}q^2)(X^2-qX+\frac{1}{2}q^2)\,.$$

هر عنصر از $K=Q(\xi)$ به صورت

$$\eta = a+b\xi+c\xi^2+d\xi^3$$

می‌باشد که در آن $a,b,c,d \in Q$ و $\xi^4=-r\in Q$. حال $[Q(\xi):Q]=4$. بنابراین اگر $Q\subset L\subset Q(\xi)$ باید داشته باشیم $[L:Q]=2$. پس L لزوماً به صورت $Q(\eta)$ بوده که در آن $\eta^2\in Q$ و $\eta\notin Q$. حال

$$\eta^2 = a^2 + b^2\xi^2 + c^2\xi^4 + d^2\xi^6 + 2ab\xi + 2ac\xi^2 + 2ad\xi^3 + 2bc\xi^3 + 2bd\xi^4 + 2cd\xi^5$$
$$= a^2 + b^2\xi^2 - rc^2 - rd^2\xi^2 + 2ab\xi + 2ac\xi^2 + 2ad\xi^3 + 2bc\xi^3 - 2bdr - 2cdr\xi$$
$$= (a^2 - rc^2 - 2rbd) + 2(ab - rcd)\xi + (b^2 - rd^2 + 2ac)\xi^2 + 2(ad + bc)\xi^3,$$

بنابراین $\eta^2 \in Q$ و $\eta \notin Q$ هم ارز است با

$$ad + bc = 0 \text{ ،}$$
$$ab - rdc = 0 \text{ ،}$$
$$b^2 - rd^2 + 2ac = 0 \text{ ،}$$

که b,c,d با هم صفر نیستند .

حال اگر $c \neq 0$ آنگاه چون $r \neq \frac{-b^2}{d^2}$ ، داریم a=b=d=0 که در این حالت $\eta = c\xi^2$ و $Q(\xi) = Q(c\xi^2) = Q(\xi^2)$. از طرف دیگر اگر c=0 ، آنگاه

$$ab = 0 \text{ ،}$$
$$ad = 0 \text{ ،}$$
$$b^2 = rd^2 .$$

که d و b هیچکدام صفر نیستند .

بنابراین اگر $\sqrt{r} \notin Q$ ، جواب دیگری وجود ندارد . به هر حال اگر $\sqrt{r} \in Q$ ، آنگاه این شرط ها نتیجه می دهد که $a = 0$ ، $\frac{a}{b} = \pm r$

در این حالت می توان فرض کرد که $b = \pm\sqrt{r}, d = 1$ ، بنابراین دو جواب دیگر $\eta = \sqrt{r}\xi + \xi^3$ و $\eta = -\sqrt{r}\xi + \xi^3$ وجود دارد .

۱۵-۳-(a) گروه گالوای مرتبه چهار دارد ، زیرا $X^4 + X^3 + X^2 + X + 1$ چند جمله ای مینیمال $\omega = e^{\frac{2\pi i}{5}}$ است .

(b) گروه گالوا از مرتبه *1* است (یعنی هر Q – خود ریختی از $Q(\omega)$ همانی است) . زیرا فرض کنید α یک Q خود ریختی باشد . در این صورت و از آنجا که $\omega = \sqrt[3]{2}$ داریم

$$[\alpha(\omega)]^3 = \alpha(\omega^3) = \alpha(2) = 2.$$

اما به دلیل آنکه $Q(\omega) \subseteq R$ داریم $\alpha(\omega) \in R$ و بنابراین $\omega = \alpha(\omega)$. از این رو α نگاشت همانی است .

۳-۱۶- در $\mathbb{C}[X]$ داریم

$$X^4 - 2 = (X + r)\,(X - r)\,(X + ir)\,(X - ir)$$

جائیکه $r = \sqrt[4]{2}$. بنابراین یک میدان شکافنده برای $X^4 - 2$ ، $Q\left(\sqrt[4]{2}, i\right)$ است . همچنین

$$[Q(\sqrt[4]{2}, i) : Q\sqrt[4]{2}]\ \ [Q(\sqrt[4]{2}) : Q] = 2.4 = 8\,.$$

یک Q – خود ریختی از $Q(\sqrt[4]{2}, i)$ کاملاً بوسیله اثر آن روی $\sqrt[4]{2}$ و i تعیین می‌شود . مزدوج‌های i عبارتند از i ,-i ، زیرا چند جمله ای مینیمال آن ها $X^2 + 1$ است . همچنین مزدوج‌های $\sqrt[4]{2}$ عبارتند از

$$\sqrt[4]{2}, \quad -\sqrt[4]{2}, \quad i\sqrt[4]{2}, \quad -i\sqrt[4]{2}$$

زیرا چند جمله ای مینیمال آن ها $X^4 - 2$ است . بنابراین در گروه گالوای $Gal(Q(\sqrt[4]{2}, i) : Q)$ هشت عنصر وجود دارد . عنصر های β, α فرض شده با $\alpha(r) = -r$ ، $\alpha(i) = -i$ و $\beta(r) = ir$, $\beta(i) = i$ تعویض پذیر نیستند ، بنابراین گروه گالوا آبلی نیست .

۳-۱۷- فرض کنید $\alpha = \sqrt[3]{2}$. بنابراین

$$X^3 - 2 = (X - \alpha)(X^2 + \alpha X + \alpha^4)$$

$$= (X - \alpha)(X - \alpha(-\frac{1}{2} + \frac{i\sqrt{3})}{2}))(X - \alpha(-\frac{1}{2} - \frac{i\sqrt{3}}{2}))$$

بنا به قضیه یکتایی ، هر میدان شکافنده $X^2 - 2$ یکریخت با زیر میدان $\mathbb{C}$ تولید شده روی Q توسط $\{\alpha, (-\frac{1}{2} + \frac{i\sqrt{3}}{2})\alpha, (-\frac{1}{2} - \frac{i\sqrt{3}}{2})\alpha\}$ می باشد . همه این عنصر ها متعلق به $Q(\alpha, i\sqrt{3})$ هستند و از آنجا که

$$i\sqrt{3} = \alpha^{-1}\left[(-\frac{1}{2} + i\frac{\sqrt{3}}{2})\alpha - (-\frac{1}{2} - \frac{i\sqrt{3}}{2})\alpha\right]$$

نتیجه می گیریم که یک میدان شکافنده آن $Q(\sqrt[3]{2}, i\sqrt{3})$ است .

حال $[Q(\sqrt[3]{2},i\sqrt{3}):Q]$ حاصلضرب $[Q(i\sqrt{3}):Q],[Q(\sqrt[3]{3}):Q]$ است ، بنابراین مضربی از 6 است. اما X^3-2 از درجه 3 است ، بنابراین میدان شکافنده دارای حداکثر $6=3!$ است . بنابراین $[Q(\sqrt[3]{2},i\sqrt{3}):Q]=6$. بنابراین گروه گالوای X^3-2 روی Q از مرتبه 6 است .

حال فرض کنید که $K=Q(\sqrt[3]{2},i\sqrt{3})$. یک Q- خود ریختی روی K کاملاً بوسیله عمل آن روی $\sqrt[3]{2}$ و $i\sqrt{3}$ تعیین می شود . مزدوج های $\alpha=\sqrt[3]{2}$ عبارتند از

$$\alpha \text{ ، } (-\frac{1}{2}+i\frac{\sqrt{3}}{2})\alpha \text{ ، } (-\frac{1}{2}-\frac{i\sqrt{3}}{2})\alpha \text{ ، }$$

و $-i\sqrt{3},i\sqrt{3}$ مزدوج های $i\sqrt{3}$ هستند . بنابراین شش عضو Gal (K ، Q) دارای نمایش های به فرم زیر هستند ،

$$e=\begin{pmatrix}\alpha & i\sqrt{3}\\ \alpha & i\sqrt{3}\end{pmatrix}, \quad a=\begin{pmatrix}\alpha & i\sqrt{3}\\ (\frac{-1}{2}+\frac{i\sqrt{3}}{2})\alpha & i\sqrt{3}\end{pmatrix}, \quad b=\begin{pmatrix}\alpha & i\sqrt{3}\\ (\frac{-1}{2}-\frac{i\sqrt{3}}{2})\alpha & i\sqrt{3}\end{pmatrix}$$

$$g=\begin{pmatrix}\alpha & i\sqrt{3}\\ \alpha & -i\sqrt{3}\end{pmatrix}, \quad h=\begin{pmatrix}\alpha & i\sqrt{3}\\ (\frac{-1}{2}+\frac{i\sqrt{3}}{2})\alpha & -i\sqrt{3}\end{pmatrix}, \quad k=\begin{pmatrix}\alpha & i\sqrt{3}\\ (\frac{-1}{2}-\frac{i\sqrt{3}}{2})\alpha & -i\sqrt{3}\end{pmatrix}.$$

جدول گروه به صورت زیر است

o	e	a	b	g	h	k
e	e	a	b	g	h	k
a	a	b	e	h	k	g
b	b	e	a	k	g	h
g	g	k	h	e	b	a
h	h	g	k	a	e	b
k	k	h	g	b	a	e

و زیر گروهها عبارتند از

$$\{e\}\ ,\ \{e,a,b\}\ ,\ \{e,g\}\ ,\ \{e,h\}\ ,\ \{e,k\}$$

و نمودار هس مربوطه به صورت

$$\begin{tikzcd}[arrows=dash]
 & \mathrm{Gal}\,(K,Q) \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
\{e,a,b\} \arrow[dr] & \{e,g\} \arrow[d] & \{e,h\} \arrow[dl] & \{e,k\} \arrow[dll] \\
 & \{e\} & &
\end{tikzcd}$$

می باشد .

بنا به قضیه اصلی تئوری گالوا ، زیر میدان های میدان شکافنده دارای یک نمودار مشبکه است که دوگان نمودار مشبکه فوق از زیر گروه های بالا است . به عنوان مثال $K = Q(\sqrt[3]{2}, i\sqrt{3})$ باید چهار زیر میدان (غیر از K , Q) داشته باشد . اینها عبارتند از

$Q(\sqrt[3]{2})$ از درجه 3 – میدان ثابت $\{e , g\}$ ؛

$Q(i\sqrt{3})$ از درجه 2 – میدان ثابت $\{e , a , b\}$ ؛

$Q((-\frac{1}{2} - \frac{i\sqrt{3}}{2})\alpha)$ از درجه 3 – میدان ثابت $\{e , h\}$ ؛

$Q((-\frac{1}{2} - \frac{i\sqrt{3}}{2})\alpha)$ از درجه 3 – میدان ثابت $\{e , k\}$.

۱۸-۳– ابتدا توجه کنید که به دلیل آنکه α یک صفر f است ، داریم $\alpha^3 = 3\alpha - 1$. حال

$$\begin{aligned}
&(X-\alpha)(X-\alpha^2+2)(X+\alpha^2+\alpha-2)\\
&=(X^2+(-\alpha^2-\alpha+2)X+\alpha^3-2\alpha)(X+\alpha^2+\alpha-2)\\
&=(X^2+(-\alpha^2-\alpha+2)X+\alpha-1)(X+\alpha^2+\alpha-2)\\
&=X^3+(-\alpha^2-\alpha+2+\alpha^2+\alpha-2)X^2\\
&+[(-\alpha^2-\alpha+2)(\alpha^2+\alpha-2)+\alpha-1]X+(\alpha-1)(\alpha^2+\alpha-2)\ .
\end{aligned}$$

اما ضریب X^2 به وضوح صفر است ، در حالی که ضریب X عبارت است از

$$\begin{aligned}
&-\alpha^4-\alpha^3+2\alpha^2-\alpha^3-\alpha^2+2\alpha+2\alpha^2+2\alpha-4+\alpha-1\\
&=-\alpha(3\alpha-1)-2(3\alpha-1)+3\alpha^2+5\alpha-5\\
&=-3
\end{aligned}$$

و جمله ثابت برابر است با

$$\alpha^3+\alpha^2-2\alpha-\alpha^2-\alpha+2=1.$$

چون

$$f(X)=(X-\alpha)(X-\alpha^2+2)(X+\alpha^2+\alpha-2)$$

مشاهده می کنیم که $Q(\alpha)$ میدان شکافنده f روی Q است و $\{1,\alpha,\alpha^2\}$ یک پایه است، بنابراین $[(Q(\alpha):Q)]=3$. از آنجا که $v(\alpha)=\alpha^2-2$ باید داشته باشیم

$$v(\alpha^2)=[v(\alpha)]^2=\alpha^4-4\alpha^2+4=-\alpha^2-\alpha+4،$$

زیرا $\alpha^3=3\alpha-1$. بنابراین v به یک Q – خود ریختی منحصر به فرد تعریف شده توسط

$$v(a+b\alpha+c\alpha^2)=a+b(\alpha^2-2)+c(-\alpha^2-\alpha+4)$$

$$=(a-2b+4c)+(-c)\alpha+(b-c)\alpha^2$$

توسیع می یابد. بنابراین $Gal(Q(\alpha),Q)=\{1,v,v^2\}$ گروه دوری از مرتبه 3 است.

توجه کنید که هر Q – خود ریختی که α را به α^2-2 تصویر کند، α^2-2 را به

$$(-\alpha^2-\alpha+4)-2=-\alpha^2-\alpha+2$$

تصویر می کند. بنابراین Q – خود ریختی وجود ندارد که α و α^2-2 را با هم عوض کند.

۱۹-۳- تنها (a) نرمال و یک میدان شکافنده برای X^2-2 است. بقیه جملگی دارای چند جمله ای مینیمال با ریشه های مختلط است.

۲۰-۳-(a) داریم $f(X)=(X-X_1)(X-X_2)\ \dots\ (X-X_n)$ و f در هیچ زیر میدان محض K شکافته نمی شود.

(b) یک F – خود ریختی از K، نگاشتی است که مزدوج ها را به مزدوج ها می برد. بنابراین جایگشتی از X_i است. به عکس، اگر $\varphi\in S_n$ (S_n گروه متقارن از درجه n)، آنگاه نگاشت $\varphi^*:K\to K$ به طوری که

$$\begin{aligned}\varphi^*(a)&=a && (a\in E)\\ \varphi(X_i)&=X_{\varphi(i)} && (i=1,2,\dots,n)\end{aligned}$$

یک F – خود ریختی از K است، زیرا چند جمله ای های متقارن تغییر نا پذیرند. بنابراین مشاهده می کنیم که $\varphi\to\varphi^*$ یک یکریختی از S_n بر روی $Gal(x,F)$ توصیف می کند.

(c) $[K:F]=|Gal(K,F)|=|S_n|=n!$.

حل مسائل فصل چهارم

۱-٤- این مطلب با یک تحقیق ساده از اصول بدست می آید ، مثلاً

$$(f+g)m=(f+g)(m)=f(m)+g(m)=fm+gm.$$

۲-٤- $\Rightarrow$: تابع $\mu_r : M \to M$ با ضابطه $\mu_r(m)=rm$ را تعریف کنید . در این صورت $r \to \mu_r$ یک 1- حافظ ریختار حلقه‌ای $\mu : R \to EndM$ را به دست می دهد .

$\Leftarrow$:یک قاعده بیرونی به وسیله $(r,m) \mapsto r_m = [\mu(r)]m$ را تعریف کنید . چون μ ریختار حلقه ای است ، داریم

$$r(m_1+m_2)=rm_1+r(m_2)،$$

$$(r+s)m=rm+sm،$$

$$(rs)m=r(sm)،$$

$$1m=m،$$

و بنابراین M یک R- مدول است .

۳-٤- درسوال (۲-٤) قراردهید $R=M=Z$. اگر $f \in EndZ$ ، چون برای $m \in Z$ ، $f(m)=f(m1)=mf(1)$ ، آنگاه f کاملاً توسط $f(1)$ مشخص می شود . حال مشاهده می کنید که $\mu_{f(1)}=f$. بنابراین μ پوشا است :

$$(\forall m \in Z) \quad \mu_{f(1)}(m)=f(1)m=f(m).$$

حال اگر $r \in Ker\mu$ ، آنگاه $\mu(r) = 0$ ایجاب می کند که برای هر $m \in Z$ ، $rm = 0$ بنابراین $r = 0$. در این صورت μ یک یکریختی حلقه ای است .

نتیجه برای Q مشابهاً حاصل می شود . در اینجا از این حقیقت استفاده می کنیم که اگر $q = \dfrac{n}{m} \in Q$، آنگاه $mq = n$. بنابراین $mf(q) = f(mq) = f(n) = nf(1)$ ، و در نتیجه $f(q) = \dfrac{n}{m} f(1) = qf(1)$.

۴-۴- اگر $\alpha, \beta \in R$ موجود باشد به گونه ای که برای هر $y \in R$ ، x داریم $f(x, y) = \alpha x + \beta y$ ، آنگاه به وضوح f یک R-ریختی است .

بر عکس ، اگر $f : R \times R \to R$ یک R -ریختی باشد ، آنگاه برای کلیه عناصر $x, y \in R$ ، داریم

$$f(x,y) = f[x\,(1\,,0) + y\,(0\,,1)] = xf(1,0) + yf(0,1)$$

بنابراین چون R جابجایی است ، و با در نظر گرفتن $\alpha = f(1,0)$ و $\beta = f(0,1)$ نتیجه حاصل می شود .

۴-۵- (a) یک ریختار حلقه ای نمی باشد ، زیرا به عنوان مثال

$$f(\sqrt{2}.\sqrt{2}) = f(2) = 2 \text{ و } f(\sqrt{2})f(\sqrt{2}) = 1 \times 1 = 1 .$$

(b) یک $Z(\sqrt{2})$ - ریختی نمی باشد ، زیرا به عنوان مثال

$$\sqrt{2}f(1) = \sqrt{2} \text{ و } f(\sqrt{2} \times 1) = f(\sqrt{2}) = 1$$

(c) f یک Z -ریختی است زیرا

$$f[(a + b\sqrt{2}) + (c + d\sqrt{2}] = a + b + c + d = f(a + b\sqrt{2}) + f(c + d\sqrt{2})،$$

$$f[n(a + b\sqrt{2})] = na + nb = n(a + b) = nf(a + b\sqrt{2}).$$

۴-۶- به وضوح $\lambda f \in Mor_R(R,M)$ و $Mor_R(R,M)$ یک R -مدول است. اینکه $\upsilon : Mor_R(R,M) \to M$ با ضابطه $\upsilon(f) = f(1_R)$ یک R -ریختی است ، از این حقیقت بدست می آید که

$$\upsilon(f + g) = (f + g)(1_R) = f(1_R) + g(1_R) = \upsilon(f) + \upsilon(g) ،$$

$$\upsilon(\lambda f) = (\lambda f)(1_R) = f(1_R \lambda) = f(\lambda) = \lambda f(1_R) = \lambda \upsilon(f) .$$

یـک بـه یـک بودن υ از مشاهده اینکه اگر $\upsilon(f)=\upsilon(g)$ ، آنگاه $f(1_R)=g(1_R)$ و همچنین fو g روی پایـه $\{1_R\}$ از R - مـدول R برابـرند بدسـت مـی آیـد . نهایـتاً بـرای $m\in M$ ، $f_m:R\to M$ را بـا ضـابطه f_m(rm)در نظـر بگـیرید . بـه وضـوح $f_m\in Mor_R(R,M)$ و $m=1_R m=f_m(1_R)=\upsilon(f_m)$ ، و نتیجه می گیریم که υ پوشا است .

۷-٤- ابتدا مشاهده می کنیم که $f^{\rightarrow}$ و $f^{\leftarrow}$ ، حافظ شمول هستند . چون $Kerf=f^{\leftarrow}(0)$ و $\operatorname{Im} f=f^{\leftarrow}(M)$ ، بنابراین واضح است که

$$A+Kerf\subseteq f^{\leftarrow}[f^{\rightarrow}(A)]،$$

$$f^{\rightarrow}[f^{\leftarrow}(B)]\subseteq B\bigcap \operatorname{Im} f .$$

(a) اگـر $x\in f^{\leftarrow}\left[f^{\rightarrow}(A)\right]$ ، آنگاه برای $a\in A$ ای ، داریـم $f(x)=f(a)$ و در نـتیجـه $x-a\in Kerf$ و $x\in Kerf+A$. این اولین تساوی را به اثبات می رساند .

(b) اگـــر $x\in B\bigcap \operatorname{Im} f$ ، آنگـــاه بـــرای $y\in M$ ای داریـــم $f(y)=x\in B$. پـــس $y\in f^{\leftarrow}(B)$ و بنابراین $x=f(y)\in f^{\rightarrow}(f^{\leftarrow}(B))$ ، که تساوی دوم را به دست می دهد .

(c) چـــون $f^{\rightarrow}$ حـــافظ شـــمول اســـت ، پـــس $f^{\rightarrow}(A\bigcap f^{\leftarrow}(B))\subseteq f^{\rightarrow}(A)$ و $f^{\rightarrow}(A\bigcap f^{\leftarrow}(B))\subseteq f^{\rightarrow}\left[f^{\leftarrow}(B)\right]\subseteq B$. بنابرایـن کافـی اسـت ثابـت کنـیم کـه اگـر $x\in f^{\rightarrow}(A)\bigcap B$، آنگاه برای بعضی از مقادیر $a\in A\bigcap f^{\leftarrow}(B)$, $x=f(a)$ ، و این فوراً از $x=f(a)\in B$ نتیجه می شود .

۸-٤-**(a)** فـرض کنـید $i:Z\to Q$ شمول کانونی و M یک زیر مدول غیر صفر Q باشد . در ایـن صـورت عـدد گویـای نـا صفر $\frac{m}{n}\in M$ وجود دارد . بنابراین $m=n.\frac{m}{n}\in M$ و در نتیجه $M\bigcap Z\neq\{0\}$. در این صورت $i^{\leftarrow}(M)\neq\{0\}$ و i اساسی است .

(b) فـرض کنـید $j:Q\to R$ شـمول کانونی و $\alpha\in R$ اصم باشد . در این صورت αZ یک زیرمدول غیرصفر R است. به‌وضوح $\alpha Z\bigcap Q=\{0\}$،بنابراین $j^{\leftarrow}(\alpha Z)=\{0\}$ و j اساسی نمی‌باشد.

فـرض کنـید A گـردایه ای از زیـر مـدول های T از N باشد به طوری که $M\bigcap F=\{0\}$. بنابرایـن $A\neq\phi$ چـون $\{0\}\in A$. حـال A بـه طـور اسـتقرایی مرتـب شـده اسـت زیرافرض کنید $N_1\subset N_2\subset N_3\subset\ldots$ یـک زنجیر از زیـر مـدول‌های A باشد . بنابراین $\bigcup_{i\geq1}N_i=\sum_{i\geq1}N_i$ یک زیر مدول N است و

$$M \cap \left(\bigcup_{i \geq 1} N_i \right) = \bigcup_{i\geq 1} (M \cap N_i) = \bigcup_{i \geq 1} \{0\} = \{0\}$$

بنابراین $\bigcup_{i\geq 1} N_i \in A$. با استفاده از اصل زرن زیر مدول B از N که عضو ماکسیمال A است وجود دارد.

حال ریختار مرکب

$$M \xrightarrow{i} N \xrightarrow{\varphi} N/B$$

را در نظر بگیرید . تکریختی بودن آن از این حقیقت ناشی می شود که اگر $x \in Ker\varphi \circ i$ ، آنگاه $\varphi[i(x)] = 0$ و بنابراین $x = i(x) \in Ker\varphi = B$، بنابراین $x \in M \cap B = \{0\}$ و در نتیجه $x = 0$.

برای اثبات اساسی بودن $\varphi \circ i$ ، فرض کنید G یک زیر مدول غیر صفر N/B باشد . بنابراین با توجه به قضیه تناظر داریم $G = X/B$ ، که در آن X یک زیر مدول غیر صفر N است که $B \subseteq X$. در ضمن $B \subsetneq X$ ، زیرا G غیر صفر است . حال اگر $(\varphi \circ i)^{\leftarrow}(G) = \{0\}$ ، آنگاه $X \cap M = i^{\leftarrow}[\varphi^{\leftarrow}(X/B)] = \{0\}$. بنابراین $X \in A$ که یک تناقض با ماکسیمال بودن B است . بنابراین $(\varphi \circ i)^{\leftarrow}(G) \neq \{0\}$ و در نتیجه $\varphi \circ i$ اساسی است .

۹-٤– (a) داریم

$$x \in f^{\leftarrow}(Ker \quad gof) \Leftrightarrow x = f(y) \quad (\text{به طوری که } g[f(y)]=0)$$
$$\Leftrightarrow x = f(y) \text{ و } g(x) = 0$$
$$\Leftrightarrow x \in \operatorname{Im} f \cap Krg.$$

(b) مشابهاً

$$x \in g^{\leftarrow}(\operatorname{Im} g \circ f) \Leftrightarrow (\exists y) \qquad g(x) = g[f(y)]$$
$$\Leftrightarrow (\exists y) \qquad x - f(y) \in Kerg$$
$$\Leftrightarrow x \in \operatorname{Im} f + Kerg.$$

۱۰-٤- $(a) \Rightarrow (b)$: اگر $h \circ f = g$ ، آنگاه

$$x \in Kerf \Rightarrow g(x) = h[f(x)] = h(0) = 0 \Rightarrow x \in Kerg.$$

$(b) \Rightarrow (a)$: اگر $Kerf \subseteq Kerg$ ، آنگاه برای $x, y \in A$ داریم :

$$.f(x)=f(y)\Rightarrow x-y\in Kerf\subseteq Kerg\Rightarrow g(x)=g(y)$$

چون f پوشا است ، می توان نگاشت $h:B\to C$ با ضابطه $h[f(x)]=g(x)$ را تعریف کرد . بنابراین به وضوح $h\circ f=g$ ، و h یک R – ریختی است زیرا

$$h[f(x)+f(y)]=h[f(x+y)]=g(x+y)=g(x)+g(y)=h[f(x)]+h[f(y)].$$

$$h[\lambda f(x)]=h[f(\lambda x)]=g(\lambda x)=\lambda g(x)=\lambda h[f(x)]$$

اگر چنین R – ریختی ، h ، موجود باشد و اگر همچنین $k:B\to C$ یک R –ریختی با $k\circ f=g$ باشد ، آنگاه $k\circ f=h\circ f$ ایجاب می کند $k=h$ (چون f پوشاست می توان آن را از راست حذف کرد) . بنابراین h منحصر به فرد است . همچنین

$$Kerh=\{0\}\Leftrightarrow (g(x)=0\Rightarrow f(x)=0)$$
$$\Leftrightarrow Kerg\subseteq Kerf$$
$$\Leftrightarrow Kerg=Kerf$$

حال نمودار زیر را در نظر بگیرید :

$$\begin{tikzcd}
 & M/Kerf \arrow[r, "\hat{f}"] \arrow[dd, dashed, "h"] & Imf \arrow[dr, "i"] \arrow[dd, dashed, "k"] & \\
M \arrow[ur, "\varphi"] \arrow[dr, "\alpha"'] & & & N \\
 & A \arrow[r, "\beta"'] & B \arrow[ur, "\gamma"'] &
\end{tikzcd}$$

به طوری که $i\circ f\circ\varphi$ تجزیه کانونی f ، و γ,β,α به‌ترتیب بروریختی ، یکریختی و تکریختی می باشند .

چون $f=\gamma\circ\beta\circ\alpha$ و β و γ و تکریختی هستند ، آنگاه $f(x)=0$ اگر و فقط اگر $\alpha(x)=0$. بنابراین $Ker\alpha=Kerf=Ker\varphi$. با توجه به بخش قبلی سئوال ، یک تکریختی منحصر به فرد $h:A\to M/Kerf$ به طوری که $h\circ\alpha=\varphi$ بدست خواهد آمد . چون φ پوشا است ، h نیز پوشا خواهد شد و بنابراین h یکریختی است .

با بحث مشابه، می بینیم که $\operatorname{Im}\gamma=\operatorname{Im}f$ و یک برو ریختی منحصر به فرد $k:\operatorname{Im}f\to B$ به طوری که وجود دارد $\gamma\circ k=i$. چون i یک به یک است، k نیز یک به یک خواهد شد. بنابراین k یکریختی است.

۱۱-٤ (a) فرض کنید $\left\{\frac{a_1}{a'_1},\dots,\frac{a_n}{a'_n}\right\}$ یک زیر مجموعه متناهی از Q و $b=\prod_{i=1}^n a'_i$ باشد. p را عدد اولی بگرید که b را عاد نمی کند. در این صورت $\frac{1}{p}$ در زیر مدول تولید شده توسط $\left\{\frac{a_1}{a'_1},\dots,\frac{a_n}{a'_n}\right\}$ نمی باشد. در واقع اگر $\frac{1}{p}$ متعلق به این زیر مدول باشد، آنگاه $x_1,x_2,\dots,x_n\in Z$ وجود دارد به طوری که

$$\frac{1}{p}=\sum_{i=1}^n x_i\frac{a_i}{a'_i}=\frac{z}{b}\quad (\text{برای } z\in Z \text{ ای})$$

بنابراین $b=pz$ و در نتیجه $p|b$ که تناقض است. بنابراین Q متناهی - مولد نمی باشد.

(b) اگر p □ q اعداد اول متمایز باشند، آنگاه $\frac{1}{p}+Z\neq\frac{1}{q}+Z$ ، زیرا در غیر این صورت $\frac{1}{p}-\frac{1}{q}\in Z$ و بنابراین برای بعضی از مقادیر $n\in Z$ ، $q-p=pqn$ و بنابراین $q=p(1+q^n)$ و در نتیجه $p|q$ که یک تناقض است. بنابراین اگر $p_1,p_2,p_3,\dots$ اعداد اول متمایز باشند، آنگاه عناصر

$$\frac{1}{p_1}+Z,\frac{1}{p_2}+Z,\frac{1}{p_3}+Z,\dots.$$

عناصر متمایز Q/Z بوده و در نتیجه Q/Z نا متناهی است.

(c) برای هر $x\in Q/Z$ ، $n\in Z$ وجود دارد به طوری که $n\neq 0$ و $nx=0$. در واقع اگر $x=\frac{p}{q}+Z$ ، آنگاه $q\neq 0$ و

$$.qx=q(p/q+Z)=qp/q+Z=p+Z=0+Z=0$$

بنابراین زیر مجموعه های تک عنصری Q/Z مستقل نیستند. تنها زیر مجموعه مستقل خطی مجموعه ϕ (بنا به تعریف) می باشد.

(d) اگر $v\in Mor_Z(Z/2Z,Q)$ ، قرار دهید $x=v(l+2Z)$. داریم

$$2x = 2v(1+2Z) = v(2+2Z) = v(0+2Z) = 0$$

بنابراین $x=0$ و در نتیجه $v=0$

e) فرض کنید $v \in Mor_Z(Q,Z)$ و $v(1) \neq 0$. در این صورت برای هر $0 \neq r \in Z$ ، داریم $v(1) = rv\left(\frac{1}{r}\right)$ و بنابراین $r|v(1)$ و چون $v(1)$ تعداد متناهی شمارنده دارد ، نتیجه می گیریم که $v(1) = 0$. در نتیجه برای هر $p ,q \in Z$ که $p ,q \neq 0$ ، داریم

$$0 = pv(1) = p\left(v\left(\frac{q}{q}\right)\right) = pqv\left(\frac{1}{q}\right) = q\left(v\left(\frac{p}{q}\right)\right)$$

بنابراین $v\left(\frac{p}{q}\right) = 0$ و در نتیجه v نگاشت صفر است .

۱۲-٤- نگاشت $f : R \to M = Rx$ با ضابطه $f(\lambda) = \lambda x$ را در نظر بگیرید . به وضوح f یک R - ریختی با $Kerf = Ann_R(x)$ است . با بکارگیری قضیه اول یکریختی داریم

$$M = \operatorname{Im} f \simeq R/_{Kerf} = R/_{Ann_R(x)}.$$

v خوش تعریف است زیرا

$$\begin{aligned} x+mZ = y+mZ &\Rightarrow x-y \in mZ \\ &\Rightarrow nx-ny \in nmZ \\ &\Rightarrow v(x+mZ) = v(y+mZ) \quad . \end{aligned}$$

به وضوح v یک Z - ریختی است .

فرض کنید $g \in Mor_Z(Z/_{mZ}, Z/_{nmZ})$, و $g(1+mZ) = t+nmZ$. بنابراین

$$\begin{aligned} 0+nmZ = g(0+mZ) &= g(m+mZ) \\ &= mg(1+mZ) \\ &= m(t+nmZ) = mt+nmZ \end{aligned}$$

و بنابراین $mt \in nmZ$ و در نتیجه $t \in nZ$. قرار دهید $t = nr$. بنابراین $g(1+nZ) = nr+nmZ$ و در نتیجه ، برای هر $x \in Z$ ،

$$\begin{aligned} g(x+mZ) = xg(1+mZ) &= xnr+nmZ \\ &= r(nx+nmZ) \\ &= rv(x+mZ) \end{aligned}$$

بنابراین $g = rv$. در این صورت $Mor_Z(Z/_{mZ}, Z/_{nmZ})$ توسط $\{v\}$ تولید می شود . حال

$$\lambda \in Ann_Z(v) \Leftrightarrow \lambda v = 0 \Leftrightarrow \lambda v(1+mZ) = 0 + nmZ$$
$$\Leftrightarrow \lambda n + nmZ = 0 + nmZ$$
$$\Leftrightarrow \lambda n \in nmZ$$
$$\Leftrightarrow \lambda \in mZ\text{،}$$

بنابراین $Ann_Z(v) = mZ$. با توجه بخش اول سئوال نتیجه می گیریم که

$$Mor_Z(Z/mZ, Z/nmZ) \simeq Z/Ann_Z(v) = Z/mZ.$$

۱۳-٤- نگاشت های $\vartheta = A \cap B \to A \times B$ با ضابطه $\vartheta(x) = (x,x)$ و $\pi : A \times B \to A + B$ با ضابطه $\pi(x,y) = x - y$ را تعریف کنید. به وضوح ϑ یک تکریختی و π یک برو ریختی است، زیرا $\pi\ (a,-b) = a + b$. حال داریم

$$\operatorname{Im}\vartheta = \{(x,x) | x \in A \cap B\}$$
$$.Ker\pi = \{(x,y) | x \in A, y \in B, x - y = 0\} = \{(x,x) | x \in A \cap B\}$$

و بنابراین دنباله

$$0 \longrightarrow A \cap B \xrightarrow{\vartheta} A \times B \xrightarrow{\pi} A + B \longrightarrow 0$$

دقیق است .

۱٤-٤- **(a)** با توجه به تعویض پذیری داریم

$$\alpha = \pi_1 \circ \alpha_2 = g_2 \circ \pi_2 \circ i_2 = g \circ 0 = 0$$

مشابهاً $\beta = 0$.

(b) چون $\pi_1 \circ i_2 = \alpha = 0$ داریم $\operatorname{Im} i_2 \subseteq Ker\pi_1 = \operatorname{Im} i_1$. بنابراین یک R- ریختی منحصر به فرد $k : A_2' \to A_1'$ وجود دارد به طوری که $i_1 \circ k = i_2$. این نتیجه می دهد که $i_1 okof = i_2 of = i_1$ و بنابراین i_1 یک به یک است . (و بنابراین از چپ حذف می شود)، پس $k \circ f = id_{A_1'}$.

چون $\pi_2 \circ i_1 = \beta = 0$ ، مشابهاً یک R- ریختی منحصر به فرد $k' : A_1' \to A_2'$ به طوری که $i_2 \circ k' = i_1$ وجود دارد. بنابراین $k \circ k' = id_{A_1'}$.

حال داریم $i_2 \circ k' \circ k = i_1 \circ k = i_2$. بنابراین i_2 از چپ حذف می شود و $k' \circ k = id_{A_2'}$. در نتیجه می بینیم که k یکریختی است با $k^{-1} = k'$ زیرا $k \circ f = id_{A_1'}$ ، نتیجه می گیریم که $f = k^{-1}$ ، بنابراین f یکریختی است. مشابهاً g نیز چنین است .

۱۵-٤- بخش اول حالت خاصی از سئوال ۱۰-٤ است . با این وجود جزئیات را شرح می دهیم .
$(a) \Rightarrow (b)$: اگر $f_* \circ g_A = f$ ، آنگاه چون $Ker g_A = A$ داریم :

$$(\forall a \in A) \quad f(a) = f_*[g_A(a)] = f_*(0) = 0$$

بنابراین $A \subseteq Kerf$.
$(b) \Rightarrow (a)$: اگر $A \subseteq Kerf$ ، آنگاه داریم

$$x + A = y + A \Rightarrow x - y \in A \subseteq Kerf \Rightarrow f(x) = f(y)$$

بنابراین می توان نگاشت $f_* : M/A \to N$ با ضابطه $f_*(x + A) = f(x)$ را تعریف کرد . به وضوح f_* یک R-ریختی بوده و $f_* \circ g_A = f$.
منحصر به فردی f_* از آنجا بدست می آید که g_A پوشا بوده و بنابراین از راست قابل حذف است .
حال f_* یک به یک است اگر و فقط اگر

$$f(x) = 0 \Rightarrow x + A = 0 + A = A$$

و این برقرار است اگر و فقط اگر $Kerf \subseteq A$. بنابراین نتیجه برقرار است زیرا عکس شمول بنا به فرض برقرار است .
دنباله

$$0 \longrightarrow M/A \cap B \xrightarrow{\alpha} M/A \times M/B \xrightarrow{\beta} M/A+B \longrightarrow 0$$

را در نظر بگیرید .
فرض کنید β با ضابطه $\beta(x + A, y + B) = x - y + A + B$ داده شده باشد . در این صورت β یک R-برو ریختی است ؛ برای مثال ، $\beta(z + A, 0 + B) = z + A + B$.
برای تابع α ، ابتدا نگاشت $f : M \to M/A \times M/B$ با ضابطه $f(x)=(x+A,x+B)$ را در نظر بگیرید . f یک R-ریختی با هسته $Kerf = A \cap B$ بوده و بنا به قسمت اول قضیه یک تکریختی (یکتا) $\alpha : M/A \cap B \to M/A \times M/B$ وجود دارد به طوری که $\alpha \circ g_{A \cap B} = f$.
برای اثبات دقیق بودن باید نشان دهیم که $\operatorname{Im} \alpha = Ker\beta$. داریم

$$\operatorname{Im} \alpha = \{(x + A, x + B) | x \in M\}$$

و

$$Ker\beta = \{(x + A, y + B) | x - y \in A + B\} .$$

اما داریم که

$$x - y \in A + B \Leftrightarrow (\exists \alpha \in A)\ (\exists b \in B) \quad x - y = a + b$$
$$\Leftrightarrow (\exists a \in A)\ (\exists b \in B) \quad x - a = y + b = z$$
$$\Leftrightarrow (\exists z \in M)\ \ x + A = z + A, y + B = z + B$$
بنابراین $\operatorname{Im}\alpha = Ker\beta$.

برای آخرین قسمت ، قرار دهید $M = A + B$. دنباله زیر حاصل می شود ،

$$0 \longrightarrow {}^{(A+B)}\!\big/_{A \cap B} \xrightarrow{\alpha} {}^{A+B}\!\big/_{A} \times {}^{A+B}\!\big/_{B} \longrightarrow 0 \longrightarrow 0$$
دقیق بودن دنباله فوق ، نشان می دهد که α یک یکریختی است .

۱۶-۴- فرض کنید که سطر بالایی دقیق است . بنابراین
$$g' \circ f' \circ \alpha = \gamma \circ g \circ f = \gamma \circ 0 = 0$$
بنابراین ، α از راست قابل حذف شدن است و $g' \circ f' = 0$ ، پس بنابراین $\operatorname{Im} f' \subseteq Kerg'$.

برای بدست آوردن عکس شمول فوق، قرار دهید $b' \in Kerg'$. چون β یکریختی است، پس عنصر یکتای $b \in B$ وجود دارد به طوری که $b' = \beta(b)$. بنابراین
$$0 = g'(b') = g'[\beta(b)] = \gamma[g(b)]$$
بنابراین ، γ یک یکریختی خواهد شد . $g(b) = 0$ نتیجه می دهد که $b \in Kerg = \operatorname{Im} f$. در این صورت برای $a \in A$ ای ، $b=f(a)$. بنابراین
$$b' = \beta(b) = \beta[f(a)] = f'[\alpha(a)] \in \operatorname{Im} f'$$
بنابراین سطر پایینی دقیق است .

۱۷-۴- $g \circ \alpha \circ f' = 0 \circ f \circ \alpha' = 0 \circ \alpha' = 0$ ، بنابراین $Kerg' = \operatorname{Im} f' \subseteq Ker\ \ g \circ \alpha$. چون g' پوشاست ، یک R – ریختی یکتای $\alpha'' : C' \to C$ وجود دارد که $\alpha'' \circ g' = g \circ \alpha$. مشابهاً $g'' \circ \beta \circ f = 0$ که در این صورت $Kerg = \operatorname{Im} f \subseteq Ker\ \ g'' \circ \beta$ و یک R – ریختی یکتای $\beta'' : C \to C''$ وجود دارد به طوری که $\beta'' \circ g = g'' \circ \beta$.

برای اینکه نشان دهیم سطر کامل پایینی دقیق است ، باید نشان دهیم که

(۱) α'' یک به یک است ؛

(۲) β'' پوشاست ؛

(۳) $\operatorname{Im}\alpha'' = Ker\beta''$.

هر سه مورد را با روند معمولی از این ور و آن ور رفتن روی نمودار حاصل می شود .

(۱) قرار دهید $c' \in Ker\alpha''$. چون g' پوشاست یک $b' \in B'$ وجود دارد که $g'(b') = c'$. در این صورت

$$0 = \alpha''(c') = \alpha''[g'(b')] = g[\alpha(b')]$$

بنابراین $\alpha(b') \in Kerg = \operatorname{Im} f$ و در نتیجه برای $a \in A$ ای ، $\alpha(b') = f(a)$. چون

$$0 = \beta[\alpha(b')] = \beta[f(a)] = f''[\beta'(a)]$$

بنابراین $\beta'(a) \in Kerf'' = \{0\}$. پس $a \in Ker\beta' = \operatorname{Im}\alpha'$ ، بنابراین $a = \alpha'(a')$. در نتیجه داریم

$$\alpha(b') = f(a) = f[\alpha'(a')] = \alpha[f'(a')] ،$$

پس $b' = f(a')$ ، زیرا α یک به یک است . حال داریم

$$c' = g'(b') = g'[f'(a')] = 0$$

و بنابراین $Ker\alpha'' = \{0\}$ ، که نتیجه مطلوب را به دست می دهد .

(۲) چون $\beta'' \circ g = g'' \circ \beta$ و چون g'' و β پوشا هستند ، پس $\beta'' \circ g$ پوشاست و در نتیجه β'' پوشاست .

(۳) $\beta'' \circ \alpha'' \circ g' = g'' \circ \beta \circ \alpha = g'' \circ 0 = 0$. بنابراین g' پوشاست (و در نتیجه از راست قابل حذف شدن است) ، و در نتیجه $\beta'' \circ \alpha'' = 0$. بنابراین $\operatorname{Im}\alpha'' \subseteq Ker\beta''$.

برای بدست آوردن عکس شمول فوق ، $c \in Ker\beta''$ را در نظر بگیرید. چون g پوشاست، برای $b \in B$ ای ، c =g(b). بنابراین

$$0 = \beta''(c) = \beta''[g(b)] = g''[\beta(b)] .$$

در این صورت $\beta(b) \in Kerg'' = \operatorname{Im} f''$. بنابراین برای $a'' \in A''$ ای ، $\beta(b) = f''(a'')$ و چون β' پوشاست ، برای $a \in A$ ای، $a'' = \beta'(a)$. بنابراین

$$\beta(b) = f''[\beta'(a)] = \beta[f(a)] .$$

که در نتیجه $b - f(a) \in Ker\beta = \operatorname{Im}\alpha$. در این صورت برای $b' \in B'$ ای ، $b - f(a) = \alpha(b')$ و این ، نتیجه زیر را بدست می دهد

$$\begin{aligned} c = g(b) &= g[f(a) + \alpha(b')] = g[f(a)] + g[\alpha(b')] \\ &= g(\alpha(b')] \qquad (\text{چون } g \circ f = 0) \\ &= \alpha''[g'(b') \in \operatorname{Im}\alpha'' \end{aligned}$$

بنابراین $Ker\beta'' \subseteq \operatorname{Im}\alpha''$.

۴-۱۸- به وضوح $Rx^{n+1} = Rx.x^n \subseteq Rx^n$. بنابراین زنجیر نزولی به صورت

$$R \supseteq Rx \supseteq Rx^2 \supseteq \dots \supseteq Rx^n \supseteq Rx^{n+1} \supseteq \dots$$

از زیر مدول ها داریم .

نگاشت $f : R \to {Rx^n}/{Rx^{n+1}}$ که با ضابطه $f(r) = rx^n + Rx^{n+1}$ تعریف شده است را در نظر بگیرید . به وضوح f یک R–برو ریختی است . حال داریم

$$\begin{aligned} Kerf &= \{r \in R \mid rx^n \in Rx^{n+1}\} \\ &= \{r \in R \mid (\exists t \in R) \quad rx^n = tx^{n+1}\} \\ &= \{r \in R \mid (\exists t \in R) \quad (r - tx)x^n = 0\} \\ &= \{r \in R \mid (\exists t \in R) \quad r - tx = 0\} \\ &= Rx \quad . \end{aligned}$$

تساوی ما قبل آخر ، از این حقیقت که $x \neq 0$ و R دارای مقسوم علیه صفر نمی باشد بدست می آید . حال با توجه به قضیه اول یکریختی داریم

$$Rx^n/_{Rx^{n+1}} = \operatorname{Im} f \simeq R/_{Kerf} = R/_{Rx}$$

۴-۱۹-(a) Z–مدول ، Z، در زنجیر صعودی از ایده آلها صدق می کند ، ولی در زنجیر نزولی از ایده آلها صدق نمی کند . زیرا هر زیر مدول از Z ، متناهی – مولد بوده (در واقع توسط یک عنصر تولید می شود) و یک زنجیر نزولی نا متناهی از زیر مدول ها به صورت

$$2Z \supseteq 4Z \supseteq 8Z \supseteq 16Z \supseteq \dots$$

را داریم .

(b) Z–مدول Z_m در هر دو شرط های زنجیر صدق می کند زیرا متناهی است .

(c) مشابه (b) است .

(d) Q–مدول، Q ،یک فضای برداری از بعد یک روی Q است . هر زیر مدول آن یک زیر فضاست و بنابراین $\{0\}$ یا Q است . بنابراین در هر دو شرط های زنجیر صدق می کند .

(e) Q به عنوان یک Z–مدول در هیچکدام از شرط های زنجیر صدق نمی کند . برای مشاهده این مطلب ، مدول تولید شده توسط $t \in Q$ که به صورت $(t) = \{nt \mid n \in Z\}$ تعریف می شود را در نظر بگیرید . در این صورت

$$(2) \supset (4) \supset (8) \supset (16) \supset \dots$$

یک زنجیر نزولی نامتناهی از زیر مدول ها بوده و

$$(\tfrac{1}{2}) \subset (\tfrac{1}{4}) \subset (\tfrac{1}{8}) \subset (\tfrac{1}{16}) \subset \dots$$

یک زنجیر صعودی نامتناهی از زیر مدول ها است .

(f) $Q[X]$ به عنوان Q – مدول در هیچکدام از شرط های زنجیر صدق نمی کند . برای مشاهده این مطلب ، زیر مدول تولید شده توسط $t \in Q[X]$ یعنی $(t) = tQ$ را در نظر بگیرید . بنابراین

$$(X, X^2, X^3, X^4, \dots) \supseteq (X^2, X^3, X^4, \dots) \supset (X^3, X^4, \dots) \supset \dots$$

یک زنجیر نزولی نامتناهی از زیر مدول ها ، و

$$(X) \subset (X, X^2) \subset (X, X^2, X^3) \subset \dots$$

یک زنجیر صعودی نامتناهی از زیر مدول ها است .

(g) Q[X] ، به عنوان یک Q[X] – مدول در شرط زنجیر صعودی صدق کرده ولی در شرط زنجیر نزولی صدق نمی کند . در واقع

$$(X) \supset (X^2) \supset (X^3) \supset (X^4) \supset \dots$$

یک زنجیر نامتناهی نزولی از زیر مدول ها است و هر زیر مدول متناهی – مولد است (زیرا زیر مدول Q[X] به عنوان Q[X] – مدول یک ایده آل است ، که با توجه به الگوریتم تقسیم توسط چند جمله ای تکین از کوچکترین درجه که در آن قرار دارد تولید می شود) .

(h) با بکار گیری قضیه تناظر ، زیر مدول های $Q[X]/M$ به صورت T/M می باشند که T زیر مدولی از Q[X] شامل M است . اما تنها زیر مدول های T ، به فرم $(f(X))$ می باشند که $f(X)$ یک شمارنده x^5 است ، و بنابراین تعداد متناهی از این زیر مدول ها وجود دارد . بنابراین $Q[X]/M$ ، به عنوان یک Q[X] – مدول در هر دو شرط های زنجیر صدق می کند .

(i) مشابه (h) است .

۴–۲۰– هر زنجیر از زیر مدول ها قابل تظریف شدن به یک زنجیر جردن – هولدر است . به خصوص ، زنجیر $\{0\} \subseteq N \subseteq M$ ، قابل تظریف شدن است .

۴–۲۱– با استفاده از سئوال قبل یک زنجیر جردن – هولدر گذرا از N مانند

$$M = M_0 \supset M_1 \dots \supset M_n = N \supset M_{n+1} \supset \dots \supset M_{n+t} = 0$$

از ارتفاع n +t وجود دارد . چون

$$M/N = M_0/N \supset M_1/N \supset \ldots M_n/N = N/N = 0$$

یک زنجیر جردن – هولدر (از ارتفاع n) برای M/N و

$$N = M_n \supset M_{n+1} \supset \ldots \supset M_{n+t} = 0$$

یک زنجیر جردن – هولدر (از ارتفاع t) برای N می باشد ، نتیجه می گیریم که

$$h(M) = n + t = h(M/N) + h(N) .$$

برای آخرین قسمت مشاهده می کنیم که

$$N = M \Leftrightarrow M/N = 0 \Leftrightarrow h(M/N) = 0 \Leftrightarrow h(M) = h(N) .$$

۴-۲۲- چون M از ارتفاع متناهی و $Kerf$ زیر مدول M می باشد ، نتیجه می گیریم که $Kerf$ از ارتفاع متناهی می باشد . چون $\operatorname{Im} f \simeq M/Kerf$ و همچنین $M/Kerf$ از ارتفاع متناهی می باشد (زیرا مدول های خارج قسمتی خاصیت شرط های زنجیر را به ارث می برند) نتیجه می گیریم که $\operatorname{Im} f$ از ارتفاع متناهی می باشد . با توجه به سئوال قبل داریم که

$$h(\operatorname{Im} f) + h(Kerf) = h(M/Kerf) + h(Kerf) = h(M) .$$

۴-۲۳- اثبات با استقراء است . اگر $n = 1$ ، آنگاه دنباله

$$0 \longrightarrow M_1 \longrightarrow 0 ،$$

تنها در حالتی دقیق است که $M_1 = 0$. پس در این حالت نتیجه بدیهی است . هرگاه $n = 2$ ، دقیق بودن

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \longrightarrow 0$$

به این بر می گردد که f یکریختی باشد که در این حالت $h(M_1) = h(M_2)$. فرض کنید $n > 2$ و نتیجه برای هر دنباله دقیق از هر نوع ارتفاع کمتر یا مساوی $n-1$ برقرار باشد . نمودار

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r] & M_2 \arrow[r] & \ldots \arrow[r] & M_{n-2} \arrow[rr, "f_{n-2}"] \arrow[dr, "\pi"'] & & M_{n-1} \arrow[r, "f_{n-1}"] & M_n \arrow[r] & 0 \\
& & & & & K \arrow[ur, "i"'] \arrow[dr] & & & \\
& & & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

که دارای سطر دقیق است را در نظر بگیرید به طوری که $\pi , K = Kerf_{n-1} = \operatorname{Im} f_{n-2}$ یک برو ریختی القا شده توسط f_{n-2} و i تابع شمول کانونی است .

دنباله

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \dots \longrightarrow M_{n-2} \xrightarrow{\pi} K \longrightarrow 0$$

دقیق است و بنابراین با توجه به فرض استقراء

$$\sum (-1)^k h(M_k) + (-1)^{n-1} h(k) = 0 .$$

همچنین دنباله

$$0 \longrightarrow K \longrightarrow M_{n-1} \xrightarrow{f_{n-1}} M_n \longrightarrow 0$$

دقیق است و مجدداً بنا به فرض استقراء ،

$$-h(K) + h(M_{n-1}) - h(M_n) = 0 ،$$

و مطلب فوق این نتیجه را به همراه دارد که

$$(-1)^{n-1} h(K) = (-1)^{n-1} [h(M_{n-1}) - h(M_n)] = 0$$

با جایگزینی $(-1)^{n-1} h(k)$ در تساوی قبلی ، نتیجه برای n حاصل می شود و استقرا تکمیل می گردد .

۴-۲۴- $M = Z_2 \oplus Z_2$ ، و $N = Z_3 \oplus Z_3$ را درنظر بگیرید. به‌وضوح $h(M) = h(N) = 2$. همچنین هر عنصر M از مرتبه دو است . حال اگر $\vartheta \in Mor_Z(M, N)$ ، آنگاه

$$(\forall x \in M) \qquad 0 = \vartheta(0) = \vartheta(x + x) = \vartheta(x) + \vartheta(x) .$$

چون N دارای عنصر مرتبه دو نمی باشد ، نتیجه می گیریم که برای هر $x \in M$ ، $\vartheta(x) = 0$ و بنابراین $\vartheta = 0$.

۴-۲۵- به سادگی دیده می شود که $M_n E_i$ زیر مدولی از M_n شامل ماتریس های به فرم

$$\begin{bmatrix} 0 & \dots & 0 & a_{1i} & 0 & 0 \\ 0 & & 0 & a_{2i} & 0 & 0 \\ 0 & & 0 & a_{3i} & 0 & 0 \\ . & & . & . & . & . \\ . & & . & . & . & . \\ . & & . & . & . & . \\ 0 & & 0 & a_{ni} & 0 & 0 \end{bmatrix}$$

و B_i زیر مدول از M، شامل ماتریس هایی به صورت

$$\begin{bmatrix} a_{11} & a_{12}\ldots\ldots & a_{1i} & 0\ldots\ldots & 0 \\ a_{21} & a_{22}\ldots\ldots & a_{2i} & 0\ldots\ldots & 0 \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ a_{n1} & a_{n2} & a_{ni} & 0 & 0 \end{bmatrix}$$

باشد . بنابراین زنجیر زیر را داریم :

$$M_n = B_n \supset B_{n-1} \supset \ldots \supset B_1 \supset B_0 = \{0\}.$$

حال زیر مدولی از A به‌صورت $B_{i-1} \subset A \subset B_i$ وجود ندارد و بنابراین بااستفاده ازقضیه تناظر، B_i/B_{i-1} ساده است . پس دنباله فوق یک زنجیر جردن – هولدر است .

۴-۲۶- برای قسمت اول کافی است که برای $i = 1 , \ldots , n$، ثابت کنیم

$$.N_i \bigcap \sum_{j\neq i} N_j = \{0\}$$

این مطلب از این حقیقت که برای هر i ، $N_i \subseteq M_i$ و $M = \bigoplus_{i=1}^{n} M_i$ و بنابراین

$$N_i \bigcap \sum_{j\neq i} N_j \subseteq M_i \bigcap \sum_{j\neq i} M_j = \{0\}$$

بدست می آید .

حال نگاشت

$$\vartheta : M = \bigoplus_{i=1}^{n} M_i \to \bigoplus_{i=1}^{n} M_i/N_i$$

که با ضابطه

$$\vartheta\ (m_1, \ldots, m_n) = (m_1 + N_1, \ldots, m_n + N_n)$$

داده شده است را در نظر بگیرید . به وضوح ϑ یک R- ریختی است که

$$Ker\,\vartheta = \{(m_1, \ldots, m_n) | m_i \in N_i\} = \bigoplus_{i=1}^{n} N_i = N\ .$$

بنابراین با بکارگیری قضیه اول یکریختی ،

$$\bigoplus_{i=1}^{n} M_i/N_i = \operatorname{Im}\vartheta \simeq M/Ker\,\vartheta = M/N\ .$$

۲۷-٤- فرض کنید که $M=\bigoplus_{i=1}^{n} A_i$ ، $\Pr_i : M \to M_i$ و $in_i : M_i \to M$ ، به ترتیب i-امین تصویر و انژکتیو باشند به طوری که

$$pr_i(a_1,...,a_n)=a_i \text{ ،}$$
$$in_i(a_i)=(\underbrace{0,...0,a_i}_{i},0,...0) \ .$$

بنابراین به وضوح in_i , Pr_i در (۱) و (۲) صدق می کنند .

بـر عکس ، فرض کنید $f_i : M \to A_i$ و $g_i : A_i \to M$ در (۱) و (۲) صدق کنند . X را یک R -مدول دلخواه و برای هر $i\in I$ ، $h_i : A_i \to X$ را یک R-ریختی بگیرید . نمودار

$$\begin{tikzcd} X & A_i \arrow[l, "h_i"'] \arrow[d, shift right, "f_i"'] \\ & M \arrow[u, shift right, "g_i"'] \end{tikzcd}$$

را در نظر بگیرید .

$h : M \to X$ را با ضابطه $h=\sum_{j=1}^{n} h_j \circ g_j$ تعریف کنید . برای هر i داریم

$$h\circ f_i=\sum_{j=1}^{n} h_j\circ g_j\circ f_i \overset{(1)}{=} h_i$$

اگر به علاوه $t : M \to X$ بگونه ای باشد که برای هر i ، $t\circ f_i = h_i$ ، آنگاه

$$t=t\circ id_M \overset{(2)}{=} t\circ\sum_{j=1}^{n} f_j\circ g_j=\sum_{j=1}^{n} t\circ f_j\circ g_j=\sum_{j=1}^{n} h_j\circ g_j=h \ .$$

بنابراین M جمع مستقیم A_1 ،...، A_n است .

حال $M=M_1\oplus M_2$ اگر و فقط اگر R -ریختی های

$$\begin{tikzcd} M_1 \arrow[r, shift left, "f_1"] & M \arrow[l, shift left, "g_1"] \arrow[r, shift left, "g_2"] & M_2 \arrow[l, shift left, "f_2"] \end{tikzcd}$$

موجود باشد به گونه ای که

(a) $g_1\circ f_1=id_M$ ، **(b)** $g_1\circ f_2=o$ ، **(c)** $g_2\circ f_2=id_M$ ،

(d) $g_2\circ f_1=0$ ، **(e)** $f_1\circ g_1+f_2\circ g_2=id_M$.

بنابراین اگر این شرایط برقرار باشد ، دنباله

$$0 \longrightarrow M_1 \xrightarrow{f_1} M \xrightarrow{g_2} M_2 \longrightarrow 0$$

دقیق است ، زیرا با توجه به (a) ، f_1 یک به یک است ، با توجه (c) g_2 پوشاست ، از (d) ، $\operatorname{Im} f \subseteq Ker g_2$ ، و با توجه به (e) اگر $g_2(x)=0$ ، آنگاه $x = (f_1 \circ g_1)(x)$ ، و بنابراین $Ker g_2 \subseteq \operatorname{Im} f_1$. به علاوه دنباله با توجه به (a) و (c) شکافنده است .

۴-۲۸- توجه داشته باشید که R آزاد است با پایه $\{1\}$. اگر

$$0 \to X \to A \xrightarrow{f} R \to 0$$

دقیق باشد ، آنگاه f پوشاست و بنابراین $a \in A$ ای موجود است به طوری که $f(a)=1$ ، $a \in A$ را به دلخواه انتخاب کنید . تابع $g : R \to A$ که $g(1)=a$ بوده و بنابراین می‌توان آن را به تمام R با توجه به خاصیت خطی بودن توسیع داد ، تعریف کنید . بنابراین

$$(f \circ g)_{(1)} = f(a) = 1$$

پس $f \circ g$ و id_R روی پایه $\{1\}$ مساویند. بنابراین $f \circ g = id_R$ و g یک ریختارشکافنده است.

دنباله

$$0 \to Z \xrightarrow{\times 2} Z \xrightarrow{\varphi} Z/2Z \to 0$$

دقیق است ولی نمی تواند شکافنده باشد ، زیرا با بحث مشابه با قسمت (d) از سئوال ۱۱-۴ ، داریم

$$Mor_Z(Z/2Z, Z) = 0 .$$

۴-۲۹- گفتن اینکه Ker$f$ یک جمعوند مستقیم M بوده و Imf یک جمعوند مستقیم N است ، معادل با این است که بگوییم در نمودار زیر (به طوری که $i_2 \circ b \circ g_1$ تجزیه کانونی f است) هر دو دنباله کوتاه ، دقیق و شکافنده هستند .

$$\begin{tikzcd}
0 \arrow[d] & & & 0 \arrow[d] & & \\
Kerf \arrow[r, "i_1"] & M \arrow[r, shift left, "g_1"] & M/Kerf \arrow[l, shift left, "p_1"] \arrow[r, shift left, "b"] & \operatorname{Im} f \arrow[l, shift left, "b^{-1}"] \arrow[r, shift left, "i_2"] \arrow[d] & N \arrow[l, shift left, "\pi_2"] \arrow[r, "g_2"] & N/\operatorname{Im} f \arrow[d] \\
 & & & 0 & & 0
\end{tikzcd}$$

فرض کنید $g: N \to M$ با ضابطه $g = \rho_1 \circ b^{-1} \circ \pi_2$ داده شده باشد. بنابراین

$$\begin{aligned} f \circ g \circ f &= i_2 \circ b \circ \underbrace{g_1 \circ \rho_1}_{id} \circ b^{-1} \circ \underbrace{\pi_2 \circ i_2}_{id} \circ b \circ g_1 \\ &= i_2 \circ b \circ b^{-1} \circ b \circ g_1 \\ &= i_2 \circ b \circ g_1 \\ &= f \end{aligned}$$

و بنابراین f منظم است.

بر عکس، فرض کنید f منظم باشد. در این صورت $g: N \to M$ وجود دارد به طوری که $f \circ g \circ f = f$. با استفاده از تجزیه کانونی $f = i_2 \circ b \circ g_1$ آن را به صورت زیر ترجمه می کنیم،

$$i_2 \circ b \circ g_1 \circ g \circ i_2 \circ b \circ g_1 = i_2 \circ b \circ g_1$$

با استفاده از این واقعیت که i_2 از چپ، g_1 از راست و b از هر دو طرف قابل حذف شدن می باشند، نتیجه می گیریم که

$$b \circ g_1 \circ g \circ i_2 = id_{\operatorname{Im} f} ،$$

از طرف دیگر،

$$g_1 \circ g \circ i_2 \circ b = id_{M/Kerf} \,.$$

بنابراین $\pi_2 = b \circ g_1 \circ g$ و $\rho_1 = g \circ i_2 \circ b$ ریختار های شکافنده برای دنباله های دقیق و کوتاه فوق بوده و نتیجه حاصل می شود.

۴-۳۰- اگر $x \in Kerj_1 \bigcap Kerj_2$ ، آنگاه $j_1(x) = 0 = j_2(x)$ و با توجه به دقیق بودن، $x \in \operatorname{Im} i_1 \bigcap \operatorname{Im} i_2$. بنابراین $x = i_1(m_1) = i_2(m_2)$. با کنار هم قرار دادن این روابط و ترکیب آنها به سادگی داریم

$$0 = j_1(x) = j_1 j_2(m_2) = k_1(m_2),$$

که چون k_1 یک یکریختی است، نتیجه می گیریم که $m_2 = 0$. در نتیجه

$$x = i_2(m_2) = i_2(0) = 0$$

و بنابراین $Kerj_1 \bigcap Kerj_2 = \{0\}$.

اگر $\bar{x} = i_1 k_2^{-1} j_2(x) + i_2 k_1^{-1} j_1(x)$ ، آنگاه

$$j_1(\bar{x}) = \underbrace{j_1 i_1}_{0} k_2^{-1} j_2(x) + \underbrace{j_1 i_2}_{k_1} k_1^{-1} j_1(x) = j_1(x)$$

و

$$j_2(\bar{x}) = \underbrace{j_2 i_1}_{k_2} k_2^{-1} j_2(x) + \underbrace{j_2 i_2}_{0} k_1^{-1} j_1(x) = j_2(x)$$

و بنابراین $\bar{x} - x \in Kerj_1 - Kerj_2$. حال از بخش اول ، تساوی $\bar{x} = x$ حاصل می شود .

تساوی $\bar{x} = x$ بدین معنی است که

$$i_1 k_2^{-1} j_2 + i_2 k_1^{-1} j_1 = id_M.$$

بنابراین مشاهده می کنیم که $M = \operatorname{Im} i_1 + \operatorname{Im} i_2$. همچنین چون

$$\operatorname{Im} i_1 \cap \operatorname{Im} i_2 = Kerj_1 \cap Kerj_2 = \{0\}،$$

نتیجه می گیریم که $M = \operatorname{Im} i_1 \oplus \operatorname{Im} i_2$.

برای آخرین قسمت مشاهده می کنیم که

$$\begin{aligned} h_1 k_1^{-1} l_1 + h_2 k_2^{-1} l_2 &= j_0 i_2 k_1^{-1} j_1 i_0 + j_0 i_1 k_2^{-1} j_2 i_0 \\ &= j_0 (i_2 k_1^{-1} j_1 + i_1 k_2^{-1} j_2) i_0 \\ &= j_0 \circ id_M \circ i_0 \\ &= j_0 i_0 \\ &= 0 \end{aligned}$$

۳۱-٤- داریم

$$\begin{aligned} (m_\alpha)_{\alpha \in I} \in \operatorname{Im} f &\Leftrightarrow (\forall \alpha \in I)(\exists m_\alpha \in M_\alpha) \quad f_\alpha(m_\alpha) = n_\alpha \\ &\Leftrightarrow (\forall \alpha \in I) \quad n_\alpha \in \operatorname{Im} f_\alpha \\ &\Leftrightarrow (n_\alpha)_{i \in I} \in \bigoplus_{\alpha \in I} \operatorname{Im} f_\alpha \quad ، \end{aligned}$$

$$\begin{aligned} (m_\alpha)_{\alpha \in I} \in Kerf &\Leftrightarrow (\forall \alpha \in I) \quad f_\alpha(m_\alpha) = 0 \\ &\Leftrightarrow (\forall \alpha \in I) \quad m_\alpha \in Kerf_\alpha \\ &\Leftrightarrow (m_\alpha)_{\alpha \in I} \in \bigoplus_{\alpha \in I} Kerf_a \quad ، \end{aligned}$$

بنابراین $\operatorname{Im} f = \underset{\alpha\in I}{\oplus} \operatorname{Im} f_\alpha$ ، و $Ker f = \underset{\alpha\in I}{\oplus} Ker f_\alpha$.

اگر هر دنباله $L_\alpha \xrightarrow{g_\alpha} M_\alpha \xrightarrow{f_\alpha} N_\alpha$ دقیق باشد ، آنگاه برای هر $\alpha \in I$ ، $\operatorname{Im} g_\alpha = Ker f_\alpha$ و بنابراین

$$\operatorname{Im} g = \underset{\alpha\in I}{\oplus} \operatorname{Im} g_\alpha = \underset{\alpha\in I}{\oplus} Ker f_\alpha = Ker f \ .$$

بنابراین دنباله

$$\underset{\alpha\in I}{\oplus} L_\alpha \xrightarrow{g} \underset{\alpha\in I}{\oplus} M_\alpha \xrightarrow{f} \underset{\alpha\in I}{\oplus} N_\alpha$$

دقیق است .

برعکس ، فرض کنید که دنباله جمع مستقیم ، دقیق باشد . بنابراین دیاگرام زیر جابجایی است (برای هر α) ،

$$\begin{tikzcd}
L_\alpha \arrow[r, "f_\alpha"] \arrow[d, "i_1"] & M_\alpha \arrow[r, "g_\alpha"] \arrow[d, "i_2"] & N_\alpha \arrow[d, "i_3"] \\
L_\alpha \arrow[r, "f"'] & \oplus M_\alpha \arrow[r, "g"'] & \oplus N_\alpha
\end{tikzcd}$$

که در آن سطر پایینی دقیق است و i_1 , i_2 , i_3 ، انژکتیو های کانونی هستند . حال $g \circ f = 0$ نتیجه می دهد که $g \circ f \circ i_1 = 0$ و بنابراین با توجه به تعویض پذیری ، $i_3 \circ g_\alpha \circ f_\alpha = 0$. چون i_3 یک به یک است و بنابراین از چپ قابل حذف شدن است ، نتیجه می گیریم که $g_\alpha \circ f_\alpha = 0$ و بنابراین $\operatorname{Im} f_\alpha \subseteq Ker g_\alpha$.

برای اثبات عکس شمول ، قرار دهید $m_\alpha \in M_\alpha$. $\overline{m}_\alpha$ را عنصری از $\underset{\alpha\in I}{\oplus} M_\alpha$ بگیرید که α -مؤلفه آن m_α بوده و سایر مؤلفه ها صفر است . بنابراین داریم

$$m_\alpha \in Ker g_\alpha \Rightarrow \overline{m}_\alpha \in Ker g \qquad \text{(مربع طرف راست جابجایی است)}$$
$$\Rightarrow \overline{m}_\alpha \in \operatorname{Im} f \qquad \text{(سطر پایینی دقیق است)}$$
$$\Rightarrow m_\alpha \in \operatorname{Im} f \qquad \text{(مربع طرف چپ جابجایی است)}$$

و بنابراین $Ker g_\alpha \subseteq \operatorname{Im} f_\alpha$. بنابراین مشاهده می کنیم که سطر بالایی نیز دقیق است .

۳۲-٤- ابتدا توجه کنید که چون R جابجایی است ، $Mor_R(M,N)$ یک R – مدول است . همچنین $L_j \neq \phi$ ، چون به وضوح شامل ریختار صفر از M به N است . برای آنکه نشان دهیم که L_j یک R – مدول است ، کافی است نشان دهیم که یک زیر مدول از $Mor_R(M,N)$ است . برای نشان دادن این مطلب کافی است ثابت کنیم که اگر $f,g \in L_j$ ، آنگاه $f+g \in L_j$ و اگر $f \in L_j$ و $\lambda \in R$ ، آنگاه $\lambda f \in L_j$. برای اثبات اولین بخش مشاهده می کنیم که

$$Kerf \bigcap Kerg \subseteq Ker(f+g)$$

زیرا $f(x)=0=g(x)$ نتیجه می‌دهد که $(f+g)_{(x)} = f(x)+g(x) = 0$. برای اثبات بخش دوم، داریم $Kerf \subseteq Ker\lambda f$، زیرا $f(x)=0$ نتیجه می‌دهد که $(\lambda f)(x) = \lambda f(x) = \lambda 0 = 0$.

برای شرح یکریختی ، توجه داشته باشید که با بکارگیری قضیه اول یکریختی برای $pr_j : M = \overset{n}{\underset{i=1}{\oplus}} A_i \to A_j$ خواهیم داشت که

$$A_j \simeq M \Big/ \underset{i\neq j}{\oplus} A_j \ .$$

فرض کنید $\vartheta_j : A_j \to M \Big/ \underset{i\neq j}{\oplus} A_j$ یک R – یکریختی باشد که با ضابطه $\vartheta_j(a_j) = a_j + \underset{i\neq j}{\oplus} A_i$ تعریف می شود . اگر $f \in L_j$ ، آنگاه $\underset{i\neq j}{\oplus} A_i \subset Kerf$ ، پس یک R – ریختی منحصر به فرد $f_* : M \Big/ \underset{i\neq j}{\oplus} A_i \to N$ وجود دارد به طوری که تساوی $f_* \circ g = f$ در نمودار زیر برقرار است :

$$\begin{tikzcd}
M \arrow[d, "g"'] \arrow[dr, "f"] & \\
M \Big/ \underset{i\neq j}{\oplus} A_i \arrow[r, "f_*"'] & N \\
A_j \arrow[u, "\vartheta_j"] &
\end{tikzcd}$$

بنابراین به وضوح $f_* \circ \vartheta_j \in Mor\ (A_j, N)$. نگاشتی که با ضابطه $f \to f_* \circ \vartheta_j$ تعریف می شود را در نظر بگیرید . این نگاشت یک به یک است ، چون ϑ_j یکریختی و f_* منحصر به

فرد بوده و یک R−ریختی است (زیرا منحصر به فردی f_* نتیجه می دهد که $(f+g)_* = f_* + g_*, (\lambda f)_* = \lambda f_*$). باقی می ماند که نشان دهیم که این نگاشت پوشاست .

حال فرض کنید $h \in Mor_R(A_j, N)$ دلخواه باشد ، پس $h \circ pr_j \in Mor_R(M, N)$.

چون به وضوح

$$(h \circ pr_j)^{\rightarrow}(\oplus_{i \neq j} A_i) = 0 \ .$$

داریم $h \circ pr_j \in L_j$. به علاوه برای کلیه عناصر $a_j \in A_j$ داریم

$$\begin{aligned}[(h \circ pr_j)_* \circ v_j](a_j) &= (h \circ pr_j)_*(a_j + \oplus_{i \neq j} A_i) \\ &= (h \circ pr_j)(a_j) \\ &= h(a_j)\end{aligned}$$

بنابراین مشاهده می کنیم که $h = (h \circ pr_j)_* \circ v_j$.

۴−۳۳− ابتدا نشان می دهیم که دنباله نیم دقیق است ، بدین معنی که ترکیب دو ریختار متوالی صفر است . این گواه بر این است که تصویر ریختار ورودی در هر مرحله مشمول در هسته ریختار خروجی است ، یعنی

$$f \circ g = 0 \Leftrightarrow \operatorname{Im} g \subseteq Ker f$$

ما آن را با مخلوط کردن نماد ها و کنار هم قرار دادن و ترکیب کردن آن ها بدست می آوریم .

(۱) $\varphi_i \circ h_{i-1}\gamma_{i-1}^{-1}g'_{i-1} = 0$ که توسط دقیق بودن و تعویض پذیری و رابطه های

$$\alpha_i h_{i-1}\gamma_{i-1}^{-1}g'_{i-1} = h'_{i-1}\gamma_{i-1}\gamma_{i-1}^{-1}g'_{i-1} = h'_{i-1}g'_{i-1} = 0 \text{؛}$$

$$f_i h_{i-1}\gamma_{i-1}^{-1}g'_{i-1} = 0 \text{ ،}$$

بدست می آید .

(۲) $\vartheta_i \circ \varphi_i = 0$ زیرا

$$\vartheta_i[\varphi_i(a_i)] = \vartheta_i(\alpha_i(a_i), f_i(a_i)) = f'_i[\alpha_i(a_i)] - \beta_i[f_i(a_i)] = 0$$

(۳) $h_i\gamma_i^{-1}g'_i \circ \vartheta_i = 0$ چون

$$\begin{aligned}(h_i\gamma_i^{-1}g'_i\vartheta_i)(a'_i, b_i) &= h_i\gamma_i^{-1}g'_i f'_i(a'_i) - h_i\gamma_i^{-1}g'_i\beta_i(b_i) \\ &= 0 - h_i\gamma_i^{-1}\gamma_i g_i(b_i) \\ &= 0 \ .\end{aligned}$$

برای آنکه نشان دهیم دنباله در B'_i دقیق است ، کافی است مشاهده کنیم که

$$b_i' \in Ker h_i \gamma_i^{-1} g_i' \Rightarrow h_i \gamma_i g_i'(b_i') = 0$$

$$\Rightarrow \gamma_i^{-1} g_i'(b_i') \in Ker h_i = \operatorname{Im} g$$

$$\Rightarrow \gamma_i^{-1} g_i'(b_i') = g_i(b_i)$$

$$\Rightarrow g_i'(b_i') = \gamma_i g_i(b_i) = g_i' \beta_i(b_i)$$

$$\Rightarrow b_i' - \beta_i(b_i) \in Ker g_i' = \operatorname{Im} f'$$

$$\Rightarrow b_i' = \beta_i(b_i) + f_i'(a_i') = f_i'(a_i') - \beta_i(-b_i) \in \operatorname{Im} \vartheta_i .$$

برای دقیق بودن در $A_i' \oplus B_i$ ، داریم :

$$(a_i', b_i) \in Ker \vartheta_i$$

$$\Rightarrow f_i'(a_i') = \beta_i(b_i)$$

$$\Rightarrow 0 = g_i' f_i'(a_i') = g_i' \beta_i(b_i) = \gamma_i g_i(b_i)$$

$$\Rightarrow 0 = g_i(b_i)$$

$$\Rightarrow b_i \in Ker g_i = \operatorname{Im} f_i$$

$$\Rightarrow b_i = f_i(a_i) \qquad (*)$$

$$\Rightarrow f_i(a_i') = \beta_i(b_i) = \beta_i f_i(a_i) = f_i' \alpha_i(a_i)$$

$$\Rightarrow a_i' - \alpha_i(a_i) \in Ker f_i' = \operatorname{Im} h_{i-1}'$$

$$\Rightarrow a_i' - \alpha_i(a_i) = h_{i-1}'(c_{i-1}') = h_{i-1}' \gamma_{i-1}(c_{i-1}) = \alpha_i h_{i-1}(c_{i-1})$$

$$\Rightarrow a_i' = \alpha_i(a_i + h_{i-1}(c_{i-1})) \quad .$$

با استفاده از $(*)$ و این واقعیت که $f_i h_{i-1} = 0$ ، داریم

$$b_i = f_i[a_i + h_{i-1}(c_{i-1})] .$$

بنابراین $(a_i', b_i) \in \operatorname{Im} \varphi_i$.

نهایتاً برای دقیق بودن در A_i اگر $a_i \in Ker\varphi_i$ ، آنگاه $a_i \in Ker\alpha_i$ و $a_i \in Kerf_i$. اگر $a_i \in Kerf_i = \operatorname{Im} h_{i-1}$ ، آنگاه

$$a_i = h_{i-1}(c_{i-1}) = h_{i-1}\gamma_{i-1}^{-1}(c'_{i-1}).$$

حال اگر $a_i \in Ker\alpha_i$ ، آنگاه

$$0 = \alpha_i(a_i) = \alpha_i h_{i-1}\gamma_{i-1}^{-1}(c'_{i-1}) = h'_{i-1}\gamma_{i-1}\gamma_{i-1}^{-1}(c'_{i-1}) = h'_{i-1}(c'_{i-1})$$

که بدست می دهد $\operatorname{Im} g'_{i-1}$ ، $c'_{i-1} \in Kerh'_{i-1}$ ، بنابراین $c'_{i-1} = g'_{i-1}(b'_{i-1})$. در نتیجه داریم

$$a_i \in Ker\varphi_i \Rightarrow a_i = h_{i-1}\gamma_{i-1}^{-1}g'_{i-1}(b'_{i-1}) \in \operatorname{Im} h_{i-1}\gamma_{i-1}^{-1}g'_{i-1}.$$

۴-۳۴- فرض کنید $R = Z \times Z$ و حلقه R را به عنوان یک R – مدول در نظر بگیرید . این R – مدول آزاد با پایه $\{(1,1)\}$ است . قرار دهید $M = Z \times \{0\}$. M یک زیر مدول R است . اما M آزاد نمی باشد زیرا از

$$(0,1)(x,0) = (0,0)$$

مشاهده می کنیم که هیچکدام از زیر مجموعه های غیر تهی M ، مستقل خطی نیستند .

۴-۳۵- اگر f تکریختی باشد ، آنگاه چون f از چپ حذف شدنی است ، آنگاه $f \circ g = 0$ ایجاب می کند که $g=0$. بنابراین f یک مقسوم علیه صفر چپ در $End_R(M)$ نمی باشد .

حال فرض کنید که M آزاد باشد با پایه $\{m_i | i \in I\}$. عکس مطلب را با نشان دادن اینکه $Kerf \neq \{0\}$ ایجاب می کند که f یک مقسوم علیه صفر چپ نمی باشد ، به دست می آوریم . فرض کنید $Kerf \neq \{0\}$ و $(n_i)_{i\in I}$ یک خانواده از اعضاء غیر صفر $Kerf$ باشد و $g : M \to M$ یک R ریختی (منحصر به فرد) بوده به طوری که $g(m_i)=n_i$ برای هر $i \in I$. چون $\{m_i | i \in I\}$ یک پایه M است ، به وضوح

$$\{0\} \neq \operatorname{Im} g \subseteq Kerf$$

بنابراین $f \circ g = 0$ و f یک مقسوم علیه صفر چپ نمی باشد .

۴-۳۶- اگر f یک برو ریختی باشد ، آنگاه f از راست حذف شدنی است ، بنابراین $f \circ g = 0$ نتیجه می دهد که $g=0$. پس f یک مقسوم علیه صفر راست در $End(M)$ نمی‌باشد.

Z – مدول Z آزاد است. ضرب در 2 ، (که در و بعضی در $End_Z(Z)$ می‌شود) ، نه یک برو ریختی است و نه یک مقسوم علیه صفر راست .

۴-۳۷- فرض کنید هر P_i در خانواده $(P_i)_{i\in I}$ تصویری باشد. برای اثبات آنکه $\bigoplus\limits_{i\in I} P_i$ تصویری است نمودار زیر را در نظر بگیرید:

$$\begin{tikzcd}
 & P_i \arrow[d, "in_i"] \arrow[ddl, dotted, "h_i"'] & \\
 & \oplus P_i \arrow[d, "f"] \arrow[dl, dotted, "h"] & \\
A \arrow[r, "g"'] & B \arrow[r] & 0
\end{tikzcd}$$

(دقیق است)

چون P_i تصویری است، یک R- بروریختی $h_i : P_i \to A$ وجود دارد به طوری که $g\circ h_i = f\circ in_i$. با استفاده از تعریف همضرب، یک R - ریختی منحصر به فرد $h : \bigoplus\limits_{i\in I} P_i \to A$ وجود دارد به طوری که $h\circ in_i = h_i$. نشان می دهیم $g\circ h = f$ و بنابراین $\bigoplus\limits_{i\in I} P_i$ تصویری است.

حال $g\circ h\circ in_i = g\circ h_i = f\circ in_i$ و بنابراین چون هر $x\in \bigoplus\limits_{i\in I} P_i$ را به طور منحصر به فرد به صورت

$$x = \sum_{j\in J} in_j(p_j)$$

(که J زیر مجموعه متناهی I بوده و برای $j\in J$ ، $p_j \in P_j$) می توان نوشت،

داریم:

$$\begin{aligned}
(g\circ h)(x) &= (g\circ h)(\sum_{j\in J} in_j(p_j)) \\
&= \sum_{j\in J} (g\circ h\circ in_j)(p_j) \\
&= \sum_{j\in J} (f\circ in_j)(p_j) \\
&= f(\sum_{j\in J} in_j(p_j)) \\
&= f(x)
\end{aligned}$$

بنابراین $g \circ h = f$.

۳۸-٤- اگر P_1 و P_2 تصویری باشند ، آنگاه $P_1 \oplus P_2$ تصویری است (همانطور که در سئوال قبلی دیدیم) . ابتدا مشاهده می کنیم که $P(M,N) \neq \phi$ ، چون به وضوح شامل ریختار صفر از M به N است. حال برای $f\,,g \in P(M,N)$ ، نشان می دهم که $f-g \in P(M,N)$. برای این مطلب نمودار زیر که در آن f به مدول تصویری P_1 و g به مدول تصویری P_2 تجزیه می شود را درنظربگیرید. دراین نمودار π_2,π_1 به ترتیب تصویرهای $P_1 \oplus P_2$ به P_1 , P_2 می‌باشند.

$$\begin{tikzcd}
 & P_1 \oplus P_2 \arrow[ddl, "\pi_1"'] \arrow[ddr, "\pi_2"] & \\
 & M \arrow[u, dotted, "v"'] \arrow[dl, "k_1"'] \arrow[dr, "k_2"] \arrow[dd, shift right, "f"'] \arrow[dd, shift left, "g"] & \\
P_1 \arrow[dr, "h_1"'] & & P_2 \arrow[dl, "h_2"] \\
 & N &
\end{tikzcd}$$

از تعریف همضرب نتیجه می شود که R- ریختی منحصر به فرد $v: M \to P_1 \oplus P_2$ وجود دارد به طوری که $\pi_1 \circ v = k_1$ و $\pi_2 \circ v = k_2$ و چون

$$h_1 \circ \pi_1 \circ v = h_1 \circ k_1 = f$$
$$h_2 \circ \pi_2 \circ v = h_2 \circ k_2 = g ،$$

مشاهده می کنیم که

$$f-g = (h_1\pi_1 - h_2\pi_2) \circ v .$$

یعنی $f-g$ به مدول تصویری $P_1 \oplus P_2$ تجزیه می شود . بنابراین $f-g \in P(M,N)$.

۳۹-٤- چون P' و P'' تصویری هستند ، پس $P' \oplus P''$ نیز تصویری است . بنابراین دنباله

$$0 \longrightarrow P' \xrightarrow{i} P' \oplus P'' \xrightarrow{\pi} P'' \longrightarrow 0$$

که در آن $i(p') = (p',0)$ و $\pi(p',p'') = p''$ ، پس بنابراین دقیق شکافنده است . اگر $j: P' \oplus P'' \to P'$ را ریختار شکافنده دست چپی و $\overline{\beta}$ یک تصویر القا شده از β در نظر بگیریم ، آنگاه نمودار داده شده به صورت زیر قابل توسیع است :

$$\begin{tikzcd}
0 \arrow[r] & P' \arrow[r, shift left, "i"] \arrow[d, "\alpha"'] & P' \oplus P'' \arrow[l, shift left, "j"] \arrow[r, "\pi"] & P'' \arrow[r] \arrow[d, "\beta"] \arrow[dl, "\bar{\beta}"'] & 0 \\
0 \arrow[r] & E' \arrow[r, "f"'] & E \arrow[r, "g"'] & E'' \arrow[r] & 0
\end{tikzcd}$$

نگاشت $\gamma : P' \oplus P'' \to E$ که با ضابطه $\gamma = f\alpha j + \bar{\beta}\pi$ داده شده است را در نظر بگیرید.
به وضوح γ یک R− ریختی است. با مشاهده اینکه

$$\gamma i = (f\alpha j + \bar{\beta}\pi)i = f \circ \alpha \circ \underbrace{j \circ i}_{id} + \bar{\beta} \circ \underbrace{\pi \circ i}_{o} = f\alpha \text{ ،}$$

$$g\gamma = g(f\alpha j + \bar{\beta}\pi) = \underbrace{g \circ f}_{o} \circ \alpha \circ j + \underbrace{g \circ \bar{\beta}}_{\beta} \circ \pi = \beta\pi \ .$$

نتیجه می گیریم که نمودار جابجایی است.

۴۰-۴- $(2) \Leftrightarrow (1)$: اگر $h.c.f.\{r, \frac{n}{r}\} = 1$ ، آنگاه اعداد صحیح x و y چنان موجودند که $xr + y\frac{n}{r} = 1$. با اثر گذاری روی خارج قسمتها داریم :

$$r(x + nZ) + \frac{n}{r}(y + nZ) = 1 + nZ$$

و بنابراین برای هر $t \in Z$ ،

$$t + nZ = r(xt + nZ) + \frac{n}{r}(yt + nZ).$$

همچنین داریم

$$\begin{aligned}
\frac{n}{r}(x + nZ) = r(y + nZ) &\Leftrightarrow \frac{n}{r}x - ry \in nZ \\
&\Leftrightarrow \frac{n}{r}x - ry = \alpha n \\
&\Leftrightarrow \frac{n}{r} \mid ry && \text{(زیرا } \tfrac{n}{r} \mid n \text{)} \\
&\Leftrightarrow \frac{n}{r} \mid y && \text{(چون } h.c.f.\{\tfrac{n}{r}, r\} = 1 \text{)} \\
&\Leftrightarrow ry \in nZ \\
&\Leftrightarrow r(y + nZ) = 0 + nZ \ .
\end{aligned}$$

بنابراین اگر (2) صدق کند داریم

$$Z/nZ \simeq \frac{n}{r}(Z/nZ) \oplus r(Z/nZ)$$

و دنباله شکافته می شود .

بر عکس ، اگر دنباله شکافته شود ، آنگاه یکریختی بالا را داریم و بنابراین $x, y \in Z$ وجود دارد به طوری که

$$r(x+nZ) + \frac{n}{r}(y+nZ) = 1+nZ \ .$$

این نتیجه می دهد که $rx + \frac{n}{r}y = 1+\alpha n$ برای $\alpha \in Z$ ای . این عبارت را می توان به صورت

$$rx + (y-\alpha r)\frac{n}{r} = 1$$

نوشت و این نشان می دهد که $h.c.f.\{r, \frac{n}{r}\} = 1$.

$(3) \Leftrightarrow (2)$: اگر (2) صدق کند ، آنگاه $r(Z/nZ)$ یک جمعوند مستقیم Z/nZ مدول آزاد Z/nZ است . (یک پایه برای آن $\{1+nZ\}$ است) . بنابراین (3) برقرار خواهد شد . برعکس اگر (3) برقرار باشد ، آنگاه با توجه به تعریف مدول تصویری ، دنباله شکافته می شود .

قرار دهید $n=6$ و $r=3$. در نتیجه (2) برقرار است و بنابراین $3(Z/6Z) \simeq Z/2Z$ یک $Z/6Z$ - مدول تصویری است . با این وجود ، مدول آزاد نمی باشد ، زیرا یک $Z/6Z$ - مدول آزاد جمع مستقیمی از کپی های $Z/6Z$ است و بنابراین حداقل 6 عضو دارد ، در حالیکه $Z/2Z$ تنها 2 عنصر دارد.

۴۱-٤- $\Delta_{A,B} = \{f \in Mor_R(X,Y) \mid f^{\rightarrow}(A) \subseteq B\}$ یک زیرمدول از R - مدول $Mor_R(X,Y)$ است ، به دلیل آنکه

(۱) $\Delta_{A,B} \neq \phi$ چون شامل ریختار صفر است ؛

(۲) $(f,g) \in \Delta_{A,B} \Rightarrow (f+g)^{\rightarrow}(A) \subseteq B \Rightarrow f+g \in \Delta_{A,B}$ ؛

(۳) $f \in \Delta_{A,B} \Rightarrow \lambda f \Delta_{A,B}$.

حال فرض کنید که $f \in \Delta_{A,B}$. بنابراین چون $f^{\rightarrow}(A) \subseteq B$ ، یک R - ریختی منحصر به فرد $f_* : X/A \rightarrow Y/B$ وجود دارد به طوری که نمودار

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\varphi_A"'] & Y \arrow[d, "\varphi_B"] \\ X/A \arrow[r, "f_*"'] & Y/B \end{tikzcd}$$

جابجایی است . بنابراین می توان نگاشت

$$\xi : \Delta_{A,B} \to Mor_R(X/A, Y/B)$$

را با ضابطه $\xi(f) = f_*$ تعریف کرد . به سادگی می توان مشخص کرد که ξ یک R - ریختی است ، در واقع با توجه به منحصر به فردی f_* داریم

$$(\lambda f)_* = \lambda f_* \quad ، \quad (f+g)_* = f_* + g_* \ .$$

برای آنکه نشان دهیم که ξ پوشاست ، $t \in Mor_R(X/A, Y/B)$ را اختیار کرده و نمودار زیر را در نظر بگیرید :

$$\begin{tikzcd} X \arrow[d, "g_A"'] \arrow[dr, "t \circ g_A"] & Y \arrow[d, "g_B"] \\ X/A \arrow[r, "t"] & Y/B \end{tikzcd}$$

چون X تصویری است ، یک R - ریختی $g : X \to Y$ وجود دارد به طوری که $g_B \circ g = t \circ g_A$. در واقع g یک تصویر القایی از $t \circ g_A$ است . نتیجه می گیریم که $g^{\to}(A) \subseteq B$ و $\xi(g) = t$.

حال $Ker\xi$ را محاسبه می کنیم . داریم

$$\begin{aligned} f \in Ker\xi &\Leftrightarrow f_* = 0 \\ &\Leftrightarrow (\forall x \in X) f(x) + B = 0 + B \\ &\Leftrightarrow (\forall x \in X) f(x) \in B \\ &\Leftrightarrow f^{\to}(X) \subseteq B \\ &\Leftrightarrow f \in \Delta_{X,B} \ . \end{aligned}$$

بنابراین با استفاده از قضیه اول یکریختی ،

$$Mor_R(X/A, Y/B) = \operatorname{Im}\xi \simeq \Delta_{A,B}/Ker\xi = \Delta_{A,B}/\Delta_{X,B}.$$

۴-۴۲- نمودار

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle v} & & \\ X & \xrightarrow[\alpha]{} & Y & \xrightarrow[\beta]{} & Z \end{array}$$

که سطر آن دقیق بوده و $\beta \circ v = 0$ را در نظر بگیرید . نتیجه می گیریم که
$\operatorname{Im} v \subseteq Ker\beta = \operatorname{Im}\alpha$.

فرض کنید $\alpha^+ : X \to \operatorname{Im}\alpha$ ، و $v^+ : P \to \operatorname{Im}\alpha$, R - ریختی هایی القا شده توسط v, α باشد . بنابراین α^+ یک بروریختی بوده و در نتیجه نمودار

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle v^+} & & \\ X & \xrightarrow[\alpha^+]{} & \operatorname{Im}\alpha & \longrightarrow & 0 \end{array}$$

دارای سطر دقیق است . چون P تصویری است ، نگاشتی $\xi : P \to x$ که $\alpha^+ \circ \xi = v^+$ وجود دارد . حال $i : \operatorname{Im}\alpha \to Y$ که تابع شمول کانونی است را در نظر بگیرید . در نتیجه داریم :

$$\alpha \circ \xi = i \circ \alpha^+ \circ \xi = i \circ v^+ = v.$$

در بخش دوم سئوال ، استقراء را بکار می بریم . ابتدا توجه داشته باشید که وجود $k_1 : P_1 \to Q_1$ به طوری که $h_1 \circ k_1 = k_0 \circ g_1$ از این حقیقت که h_I برو ریختی و p_I تصویری است حاصل می شود .

فرض کنید برای $t = 1, \dots, n-1$ ، ریختار های $k_t : P_t \to Q_t$ که $h_t \circ k_t = k_{t-1} \circ g_t$ وجود دارد . دیاگرام

$$\begin{tikzcd} P_n \arrow[r, "g_n"] & P_{n-1} \arrow[r, "g_{n-1}"] \arrow[d, "k_{n-1}"] & P_{n-2} \arrow[d, "k_{n-2}"] \\ Q_n \arrow[r, "h_n"'] & Q_{n-1} \arrow[r, "h_{n-1}"'] & Q_{n-2} \end{tikzcd}$$

که دارای سطر های دقیق است را در نظر بگیرید . داریم

$$\begin{aligned} h_{n-1} \circ (k_{n-1} \circ g_n) &= (h_{n-1} \circ k_{n-1}) \circ g_n \\ &= k_{n-2} \circ g_{n-1} \circ g_n \\ &= k_{n-2} \circ 0 \\ &= 0 \end{aligned}$$

و بنابراین P_n ها تصویری هستند . بخش اول سئوال ما را به وجود یک R - ریختی $K_n : P_n \to Q_n$ به طوری که $h_n \circ k_n = k_{n-1} \circ g_n$ هدایت می کند . بنابراین بحث استقراء کامل می شود .

۴-۴۳- در دیاگرام داده شده به وضوح $h \circ i \circ j = 0$ و بنابراین

$$Kerg = \operatorname{Im} j \subseteq Ker h \circ i \ .$$

چون g یک بروریختی است ، بنابراین R - ریختی یکتای $v : B \to P/\operatorname{Im} i \circ j$ وجود دارد که $h \circ i = v \circ g$. برای اثبات آنکه v یک تکریختی است ، از این واقعیت که g پوشاست استفاده می کنیم . حال

$$v[g(a)] = v[g(b)] \Rightarrow (h \circ i)_{(a)} = (h \circ i)_{(b)}$$

$$\Rightarrow i(a) - i(b) \in \operatorname{Im} i \circ j \qquad \text{برای } x \in Kerg \text{ ای}$$

$$\Rightarrow i(a-b) = i[j(x)] \qquad \text{زیرا } i \text{ یکنواست}$$

$$\Rightarrow a - b = j(x)$$

$$\Rightarrow g(a) - g(b) = g(a-b) = g[j(x)] = 0$$

و نتیجه حاصل می شود .

اگر P شبه تصویری باشد ، آنگاه بخش پایانی از بحث بالا با در نظر گرفتن A = P و $B = P/N$ و $g = h_N$ بدست می آید . برای عکس مطلب ، نمودار

$$\begin{tikzcd}
 & & & P \arrow[d, "\varphi"] \arrow[ddl, dotted, "\pi"'] & \\
0 \arrow[r] & Kerg \arrow[r, "j"] & A \arrow[r, "g"] \arrow[d, "i"'] & B \arrow[r] \arrow[d, dotted, "v"] & 0 \\
 & & P \arrow[r] & P/\operatorname{Im} i \circ j &
\end{tikzcd}$$

را در نظر بگیرید .

با توجه به بخش اول سئوال ، یک تکریختی یکتای v چنان وجود دارد که $v \circ g = h \circ i$.
با توجه به فرض یک R − ریختی یکتای π وجود دارد به طوری که $h \circ \pi = v \circ h$.
$p \in \operatorname{Im} \pi$ را در نظر بگیرید . پس $p = \pi(q)$. بنابراین با جستجو کردن بدست می آوریم :

$$h(p) = h[\pi(q)] = v[\varphi(q)] = v[g(a)] = h[i(a)]،$$

که نتیجه می دهد

$$p - i(a) \in Kerh = \operatorname{Im} i \circ j$$

پس $p \in \operatorname{Im} i$. بنابراین $\operatorname{Im} \pi \subseteq \operatorname{Im} i$. چون i یکنوا است ، یک R − ریختی یکتای $\xi : P \to A$ به طوری که $i \circ \xi = \pi$ وجود دارد . بنابراین

$$v \circ g \circ \xi = h \circ i \circ \xi = h \circ \pi = v \circ h$$

و چون v یک به یک است (با توجه به بخش اول سئوال) ، داریم $g \circ \xi = \varphi$.

امتحان شماره ۱

وقت مجاز : ۳ ساعت

برای هر سئوال ، ۲۰ امتیاز در نظر گرفته شده است .

۱- فرض کنید R یک حلقه و N کوچکترین زیر حلقه R باشد که شامل هر ایده آل دو طرفه و پوچ R است . نشان دهید که N یک ایده آل پوچ دو طرفه R است .

فرض کنید که I یک ایده آل راست باشد . ثابت کنید $I + RI$ یک ایده آل دو طرفه R است . همچنین ثابت کنید که برای هر عدد صحیح $m \geq 1$ ،

$$(I + RI)^m \subseteq I^m + RI^m .$$

نتیجه بگیرید که اگر I ایده آل راست پوچ توان باشد ، آنگاه $I \subseteq N$.

آیا N شامل هر ایده آل چپ پوچ توان R است ؟

۲- فرض کنید R یک حوزه صحیح باشد به طوری که دنباله نامتناهی (a_n) از عناصر حلقه را نمی توان یافت به طوری که a_{n+1} یک عامل محض a_n باشد . ثابت کنید R یک دامنه تجزیه یکتا است، اگر و فقط اگر هر عنصر تحویل ناپذیر R اول باشد .

عنصر $9+19i$ به صورت حاصلضرب از عناصر تحویل ناپذیر در $Z[i]$ بنویسید .

نشان دهید در دامنه مربعی $Z[\sqrt{14}]$ تساوی های

$$14 = \sqrt{14}\sqrt{14} = 2 \times 7$$

دلیلی بر عدم تجزیه یکتا بودن نمی باشد .

۳- فرض کنید F یک میدان و f چند جمله ای تحویل ناپذیر غیر خطی در $F[X]$ باشد . نشان دهید که $E = {F[X]}/{(f)}$ یک توسیع

F است و f دارای عامل $X-\alpha$ در $E[X]$ است که در آن $\alpha = X+(f) \in E$. همچنین نشان دهید که $E = F(\alpha)$.

حال فرض کنید $F = GF(3) = \mathbb{Z}/_{(3)}$ ، میدانی سه عضوی بوده و $f(X) = X^3 - X + 1$.

a) نشان دهید f روی F تحویل ناپذیر است ؛

b) تعداد عناصر $F(\alpha)$ را بیابید ؛

c) وارون α در $F(\alpha)$ مشخص کنید ؛

d) نشان دهید f کاملاً به عوامل خطی در $F(\alpha)[X]$ تجزیه می شود و این عوامل را بیابید ،

e) گروه گالوای $Gal(F(\alpha), F)$ را بیابید .

٤- فرض کنید M و N R - مدول و $f: M \to N$ یک R - ریختی باشد . اگر B, A به ترتیب زیر مدول های M و N باشند ، ثابت کنید که گزاره های زیر معادلند

(۱) $f^{\rightarrow}(A) \subseteq B$ ؛

(۲) یک R - ریختی منحصر به فرد $f_*: M/_A \to N/_B$ وجود دارد به طوری که نمودار

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle g_A}\downarrow & & \downarrow{\scriptstyle g_B} \\ M/_A & \xrightarrow[f_*]{} & N/_B \end{array}$$

جابجایی است ،

به علاوه نشان دهید که R - ریختی f_* اگر موجود باشد ، آنگاه

a) یک تکریختی است ، اگر و فقط اگر $A = f^{\leftarrow}(B)$ ؛

b) یک برو ریختی است ، اگر و فقط اگر $N = B + Im f$.

نمودار $M \xrightarrow{f} N \xrightarrow{g} P$ از R - مدول ها و R - ریختی ها داده شده است. نشان دهید که

$$0 \to Kerf \to Ker g\circ f \to Kerg \to N/_{\operatorname{Im} f} \to P/_{\operatorname{Im} g\circ f} \to P/_{\operatorname{Im} g} \to 0$$

دقیق است .

۵- R - مدول های $A_1, A_2, \ldots, A_m$ ، و $B_1, B_2, \ldots, B_n$ را در نظر بگیرید . برای هر R - ریختی $f : \overset{m}{\underset{k=1}{\oplus}} A_k \to \overset{n}{\underset{k=1}{\oplus}} B_k$ تعریف می کنیم

$$f_{ji} = pr_j^B \circ f \circ in_i^A$$

جائیکه $\Pr_j^B : \overset{n}{\underset{k=1}{\oplus}} B_k \to B_j$ یک برو ریختی کانونی و $in_i^A : A_i \to \overset{m}{\underset{k=1}{\oplus}} A_k$ یک تکریختی کانونی است . اگر M را مجموعه ماتریس های $n \times m$ ، $[v_{ji}]$ بگیرید به طوری که $v_{ji} : A_i \to B_j$ یک R - ریختی است ، نشان دهید که نگاشت

$$\xi : Mor_R(\overset{m}{\underset{i=1}{\oplus}} A_i, \overset{n}{\underset{j=1}{\oplus}} B_j) \to M$$

که با ضابطه $\xi(f) = [f_{ji}]$ تعریف می شود یک یکریختی از گروه های آبلی است ، به طوری که f منحصراً توسط ماتریس $n \times m$ ، $[f_{ij}]$ مشخص می شود .

نشان دهید که R - ریختی مرکب

$$\overset{m}{\underset{i=1}{\oplus}} A_i \xrightarrow{f} \overset{n}{\underset{j=1}{\oplus}} B_j \xrightarrow{g} \overset{p}{\underset{k=1}{\oplus}} C_k$$

توسط حاصلضرب ماتریس های $[g_{kj}][f_{ji}]$ نمایش داده می شود . بنابراین برای هر R - مدول A ، یکریختی حلقه ای

$$Mor_R(A^m, A^m) \simeq Mat_{m\times m}[Mor_R(A, A)]$$

بدست می آید .

امتحان شماره ۲

وقت مجاز : ۳ ساعت

برای هر سئوال ، ۲۰ امتیاز در نظر گرفته شده است .

۱- فرض کنید R یک حلقه جابجایی یکدار باشد و A را ایده الی بگیرید که در میان ایده آلهای R که متناهی – مولد نیستند ، ماکزیمال است . فرض کنید $xy \in A$ ، و $x, y \notin A$. نشان دهید که (A,x) و $C = \{c \in R | cx \in A\}$ ، ایده الهای متناهی –مولد R می باشند. اگر

$(A,x) = (a_1 + b_1 x, a_2 + b_2 x, \dots, a_n + b_n x)$ و $C = (c_1, c_2, \dots, c_m)$ ،

نشان دهید که

$$A = (a_1, a_2, \dots, a_n, c_1 x \dots, c_m x) .$$

نتیجه بگیرید که A یک ایده آل اول است .

بنابراین با استفاده از لم زرن ، نشان دهید که اگر هر ایده آل اول حلقه جابجایی یکدار متناهی – مولد باشد ، آنگاه هر ایده آل حلقه متناهی – مولد است .

۲- فرض کنید $\omega = \frac{1}{2}(-1 + \sqrt{-3})$ یک ریشه سوم اولیه واحد باشد . تعریف کنید

$$Z[\omega] = \{a + b\omega | a, b \in Z\} .$$

نشان دهید که $Z[\omega]$ یک دامنه اقلیدسی با تعریف تابع نرم $N(a + b\omega) = a^2 - ab + b^2$ می‌باشد .

[راهنمایی . اثبات مشابه بحثی است که $Z[\sqrt{n}]$ یک دامنه اقلیدسی برای $-2 \le n \le 3$ می باشد] .

ثابت کنید $Z[\sqrt{-3}]$ یک زیر حلقه $Z[\omega]$ است . نتیجه بگیرید که یک زیر حلقه یک دامنه تجزیه یکتا لزوماً یک دامنه تجزیه یکتا نمی باشد .

۳- فرض کنید K یک توسیع متناهی میدان F باشد . توضیح دهید که معنی اینکه K توسیع نرمال F است چیست .

آیا $Q[\sqrt{5}]$ یک توسیع نرمال Q است ؟ آیا $Q[\sqrt[3]{2}]$ یک توسیع نرمال Q است؟

گروه گالوای توسیع $Q(\sqrt{2},\sqrt{5})$ از Q را بیابید . زیرگروه های این گروه گالوا را یافته و میدان های ثابت متناظر آن ها را بیابید .

٤- اگر N یک R- مدول و $(M_i)_{i\in I}$ یک خانواده از R – مدول ها باشد ، یکریختی های زیر از گروه های آبلی را بدست آورید (منظور از $\prod$ ، حاصلضرب مستقیم است) :

$$Mor_R(\bigoplus_{i\in I} M_i, N)\simeq\prod_{i\in I} Mor_R(M_i, N) \qquad (۱)$$

$$Mor_R(N\prod_{i\in I} M_i)\simeq\prod_{i\in I} Mor_R(N, M_i) . \qquad (۲)$$

نتیجه بگیرید اگر $(M_i)_{i\in I}$ و $(N_i)_{j\in J}$ خانواده هایی از R – مدول ها باشند ، آنگاه یک یکریختی از گروه های آبلی به صورت

$$Mor_R(\bigoplus_{i\in I} M_i, \prod_{j\in J} N_j)\simeq \prod_{(i,j)\in I\times J} Mor_R(M_i, N_j)$$

وجود دارد .

یکریختی گروه های آبلی $Mor_Z(Z,Z)\simeq Z$ را بدست آورید .

اگر برای هر عدد صحیح مثبت n ، حاصلضرب دکارتی n کپی از Z را با Z^n نمایش دهیم ، نتیجه بگیرید که برای هر عدد صحیح مثبت m و n ،

$$Mor_Z(Z^n, Z^m)\simeq Z^{nm} .$$

۵- اگر P یک R – مدول تصویری بوده و اگر نمودار

$$\begin{tikzcd} & P \arrow[d, "\nu"] & \\ X \arrow[r, "\alpha"'] & Y \arrow[r, "\beta"'] & Z \end{tikzcd}$$

دارای سطر دقیق بوده و $\beta \circ \nu = 0$ ، ثابت کنید یک R – ریختی $\xi : P \to X$ وجود دارد به طوری که $\alpha \circ \xi = \nu$.

یک دنباله دقیق به صورت

$$(*) \quad \ldots \longrightarrow P_n \xrightarrow{f_n} P_{n-1} \xrightarrow{f_{n-1}} \ldots \longrightarrow P_1 \xrightarrow{f_1} P_0 \longrightarrow 0$$

را شکافنده گوییم ، اگر R – ریختی های $g_i : P_i \to P_{i+1}$ موجود باشند به طوری که

(۱) $f_1 \circ g_o = id_{p_\circ}$ ،

(۲) $g_{i-1} f_i + f_{i+1} g_i = id_{p_i} \quad (\forall i \geq 1)$.

با استقراء ثابت کنید که اگر هر $\mathrm{P_i}$ تصویری باشد ، آنگاه دنباله $(*)$ شکافنده است .

امتحان شماره ۳

وقت مجاز : ۳ ساعت

برای هر سئوال ۲۰ امتیاز در نظر گرفته شده است .

۱- یک دامنه اقلیدسی را شرح دهید و ثابت کنید هر دامنه اقلیدسی یک دامنه ایده آل اصلی است. کدامیک از حلقه های زیر دامنه اقلیدسی است ؟ یک اثبات یا یک مثال نقض برای دلیل خود ارائه دهید .

(a) $Z[X]$ ؛

(b) $Q[X]$ ؛

(c) $Z[\sqrt{3}]$ ؛

(d) $Z[i]$.

با نشان دادن اینکه ایده آل $(2,1+\sqrt{-3})$ ایده آل اصلی در $Z[\sqrt{-3}]$ نمی باشد ، ثابت کنید که $Z[\sqrt{-3}]$ اقلیدسی نمی باشد .

۲- فرض کنید $a_0 = 2$ و برای $n = 0,1,2,\ldots$ ، a_{n+1} را ریشه مثبت و مرتبه دوم a_n بگیرید . قرار دهید $K_n = Q(a_n)$.

(a) نشان دهید $K_n \subseteq K_{n+1}$.

(b) نشان دهید $K_{n+1} = K_n(a_{n+1})$ و $[K_{n+1} : K_n] \leq 2$.

(c) با استقرا ثابت کنید که $a_{n+1} \notin K_n$ ؛

(d) برای هر $n \geq 1$ ، $[K_n : Q]$ را محاسبه کنید .

۳- عاملهای تحویل ناپذیر $f(X) = X^4 - 2X^2 - 3$ در $Q[X]$ را بیابید .

نشان دهید که $Q(i,\sqrt{3})$ میدان شکافنده f روی Q است . همچنین نشان دهید که $[Q(i,\sqrt{3}) : Q] = 4$ و یک پایه برای $Q(i,\sqrt{3})$ روی Q بیابید . چند جمله ای مینیمال $i+\sqrt{3}$ روی Q را بیابید . نشان دهید که $Q(i,\sqrt{3}) = Q(i+\sqrt{3})$.

چند جمله ای مینیمال $i+\sqrt{3}$ روی حلقه های زیرا را بیابید .

(a) $Q(i)$ ؛

(b) $Q(\sqrt{3})$ ؛

(c) $Q(i\sqrt{3})$.

۴- نمودار

$$\begin{array}{ccccccc} 0 \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} D \\ & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & \\ 0 \longrightarrow & A' & \xrightarrow[f']{} & B' & \xrightarrow[g']{} & C' & \end{array}$$

از R – مدول ها و R – ریختی ها که جابجایی بوده و سطرها دقیق می باشند را در نظر بگیرید .
اگر γ یکریختی باشد ، ثابت کنید دنباله

$$0 \longrightarrow A \xrightarrow{\varphi} A' \oplus B \xrightarrow{v} B' \xrightarrow{\xi} D$$

جائیکه $\zeta = h\circ\gamma^{-1}\circ g'$ و v و φ با ضابطه زیر می باشند

$$v(a',b) = f'(a') - \beta(b) \text{ ، } \varphi(a) = (\alpha(a), f(a)) \text{ ،}$$

یک دنباله دقیق است .

۵- اگر $(M_\alpha)_{\alpha\in I}$ یک خانواده از R – مدول ها باشد ، حاصلضرب این خانواده را شرح دهید .
اگر $(P,(\varphi_\alpha)_{\alpha\in I})$ و $(Q,(q_\alpha)_{\alpha\in I})$ حاصلضربهایی از $(M_\alpha)_{\alpha\in I}$ باشند ، ثابت کنید که یک R – ریختی منحصر به فرد $v: P \to Q$ وجود دارد به طوری که برای هر $\alpha \in I$ ، $q_\alpha \circ v = p_\alpha$.

فرض کنید $\left(\prod_{\alpha\in I} M_\alpha, (pr_\alpha)_{\alpha\in I}\right)$ حاصلضرب دکارتی $(M_\alpha)_{\alpha\in I}$ باشد . یک زیر مدول M از $\prod_{\alpha\in I} M_\alpha$ را یک زیر حاصلضرب مستقیم از $(M_\alpha)_{\alpha\in I}$ گوییم ، هرگاه برای هر $\alpha \in I$ تحدید $pr_\alpha^M : M \to M_\alpha$ از تصویر کانونی pr_α یک R – بروریختی باشد .

اگر N یک R – مدول بوده و یک خانواده $(f_\alpha)_{\alpha\in I}$ از R – بروریختی های $f_\alpha : N \to M_\alpha$ موجود باشد ، به گونه ای که $\bigcap Kerf_\alpha = \{0\}$ ، آنگاه ثابت کنید که N با یک زیر حاصلضرب مستقیم از $(M_\alpha)_{\alpha\in I}$ یکریخت است .

نتیجه بگیرید که Z یکریخت با یک زیر حاصلضرب مستقیم از $(Z/nZ)_{n>1}$ است .

امتحان شماره ٤

وقت مجاز : ۳ ساعت

برای هر سئوال ۲۰ امتیاز در نظر گرفته شده است .

۱- فرض کنید $A_1, \ldots, A_n$ ایده آلهای دو طرفه حلقه R باشند . گوییم R جمع مستقیم A_1، A_2، ...، A_n است و می نویسیم $R = \bigoplus_{i=1}^{n} A_i$ ، اگر

(۱) $R = \sum_{i=1}^{n} A_i$ ؛

(۲) $A_i \cap \sum_{j \neq i} A_j = \{0\}$ $(i = 1,2,\ldots,n)$.

اگر $S_1 , \ldots , S_m$ ایده آلهای دو طرفه حلقه R باشند به طوری که

(a) $R = \sum_{i=1}^{m} S_i$ ؛

(b) هیچ زیر مجموعه محض از $\{S_1,\ldots,S_m\}$ ، R را تولید نکند ؛

(c) هر S_i حلقه ای شامل یک عنصر 1 است که شامل هیچ ایده آلی به جز $\{0\}$ و S_i نمی باشد ، نشان دهید که $R = \bigoplus_{i=1}^{m} S_i$.

حال فرض کنید که

$$R = \bigoplus_{i=1}^{m} S_i = \bigoplus_{i=1}^{n} T_i$$

دو نمایش R به صورت حاصلضرب مستقیم از ایده آل های دو طرفه باشد . برای $i= 1, 2, \ldots, m$ ، نشان دهید که $S_i R = S_i$ و نتیجه بگیرید که دقیقاً یک مقدار $j \in \{1,2,\ldots,n\}$ وجود دارد به طوری که $S_i T_j = S_i$. بنابراین نشان دهید که $S_i = T_j$ و نتیجه بگیرید که تجزیه به جمع مستقیم اساساً یکتاست .

۲- فرض کنید K یک زیر میدان $\mathbb{C}$ بوده به طوری که میدان شکافنده یک چند جمله ای $f \in Q[x]$ می باشد . با در نظر گرفتن گروه گالوای K روی Q نشان دهید که تعداد متناهی زیر میدان متمایز K شامل Q وجود دارد .

فرض کنید $D = \{[Q(\xi):Q] \;|\xi \in K\}$ ، مجموعه درجه های توسیع های ساده Q و مشمول در K باشند . شرح دهید که چرا D شامل بزرگترین عنصر d است. اگر $\alpha \in K$ بوده به طوری که $[Q(\alpha):Q] = d$، نشان دهید که $Q(\alpha) = K$.

[راهنمایی . اگر $Q(\alpha) \neq K$ ، $\beta \in K \setminus Q(\alpha)$ را انتخاب و برای $q \in Q$میدان های $Q(\alpha + q\beta)$ را در نظر بگیرید].

۳- مفهوم توسیع متناهی میدان F که نرمال می باشد را شرح دهید . نشان دهید که اگر $f \in F[x]$ و K میدان شکافنده برای fروی F باشد ، آنگاه K توسیع نرمال F است .

فرض کنید $F = GF(p) = Z_p$ و $K = GF(P^n)$ میدان شکافنده برای $X^{P^n} - X$ روی F باشد . نشان دهید که هر چند جمله ای تحویل ناپذیر از درجه n در $F[X]$ ، کاملاً در K تجزیه می شود

نشان دهید که اگر $m_\alpha, \alpha \in K$ چند جمله ای مینیمال α روی F باشد ، آنگاه $\deg m_\alpha$ ، n را عاد می کند . نتیجه بگیرید که عامل تحویل ناپذیر $X^{P^n} - X$ در $F[X]$ دارای درجه حداقل n است .

عوامل تحویل ناپذیر $X^9 - X$ را در $GF(3)[X]$ را بیابید .

۴- ثابت کنید که یک R - مدول نوتری است (یعنی در شرط زنجیر صعودی از زیر مدول ها صدق می کند) ، اگر و فقط اگر هر زیر مدول M متناهی - مولد باشد .

فرض کنید M و N ، R– مدول های نوتری بوده و P یک R - مدول باشد به طوری که دنباله

$$0 \longrightarrow M \xrightarrow{f} P \xrightarrow{g} N \longrightarrow 0$$

یک دنباله دقیق کوتاه است .

اگر A زیر مدول P باشد ، آنگاه $A \cap \operatorname{Im} f$ متناهی - مولد می باشد (مثلاً مجموعه مولد را $\{x_1, \dots, x_r\}$ بگیرید) .

نشان دهید که عناصر $y_1 ,\dots, y_n \in A$ وجود دارد به طوری که $A, \{y_1, \dots, y_n, x_1, \dots, x_r\}$ را تولید می کند . همچنین نتیجه بگیرید که P نوتری است.

بنابراین نشان دهید که اگر P یک R – مدول و M زیر مدولی از P باشد ، آنگاه P نوتری است اگر و فقط اگر M و P/M نوتری باشند .

۵- اگر P یک R – مدول باشد ، ثابت کنید که گزاره های زیر معادلند :

P تصویری است ؛

هر دنباله دقیق $M \to P \to 0$ شکافنده است ؛

P یک جمعوند مستقیم از یک R – مدول آزاد است .

فرض کنید Δ_n حلقه ماتریس $n \times n$ ، پایین مثلثی $X=[x_{ij}]$ روی میدان F باشد (یعنی $x_{ij}=0$ ، اگر $i<j$) . $B, A \in \Delta_n$ را ماتریس هایی در نظر بگیرید که به ترتیب به صورت زیر داده شده اند ،

$$a_{ij} = \begin{cases} 1 & \text{اگر } i = j + 1 \\ 0 & \text{در غیر این صورت} \end{cases} \quad \text{و} \quad b_{ij} = \begin{cases} 1 & \text{اگر } i = j = 1 \\ 0 & \text{در غیر این صورت} \end{cases}$$

اگر $\theta_n = \{X \in \Delta_n | x_{ii} = 0, i = 1, \dots, n\}$، ثابت کنید که دنباله

$$0 \longrightarrow \Delta_n B \xrightarrow{f} \Delta_n \xrightarrow{g} \theta_n \longrightarrow 0 ،$$

که در آن f تابع شمول کانونی و g با ضابطه $g(X)=XA$ می باشد ، یک دنباله دقیق شکافنده از Δ_n – مدول ها می باشد . نتیجه بگیرید که θ_n یک Δ_n – تصویری است .

مراجع

دروس جبر مجرد در محتوا و شکل بسیار متفاوت می باشند . همانطور ، کتابهای توصیه شده برای این دروس نه تنها از نقطه نظر علامت ها و تشریح مفاهیم ، بلکه از نظر سطح تحقیقاتی نیز از تفاوتهای عمده ای بهره می برند . در اینجا فهرستی از کتب اصلی که به طور وسیعی مورد استفاده قرار می گیرند ، جهت آنکه خواننده بعنوان پیش نیاز می تواند به آنها رجوع کند ارائه شده است . مطالب این کتابها ، مطالب هر شش کتاب جبر به روش تمرین را پوشش داده و در بعضی از موردها مطالب بیشتری نیز دارند . برای راحتی خواننده ، فهرستی مربوط به اینکه چه قسمتی از این کتابها به کدام فصل از این کتاب مربوط می شود نیز ارائه شده است .

[1] *I. T. Adamson,* Introduction to Field Theory, *Cambridge University Press, 1982* .

[2] *F. Ayres, Jr,* Modern Algebra, *Schaum's Outline Series, McGraw-Hill, 1965* .

[3] *D.Burton,* A first sourse in rings and ideals, *Addison-Wesley, 1970* .

[4] *P.M.Cohn,* Algebra *Vol. I, Wiley, 1982* .

[5] *D.T.Finkbeiner II,* Introduction to Matrices and Linear Transformations, *Freeman, 1978* .

[6] *R. Godement,* Algebra, *Kershrw, 1983* .

[7] *J. A. Green,* Sets and Groups, *Routledge and Kegan Paul, 1965* .

[8] *I. N. Herstein*, Topics in Algebra, *Wiley, 1977* .

[9] *K. Hoffman and R. Kunze,* Linear Algebra, *Prentice Hall, 1971* .

[10] *S. Lang,* Introduction to Linear Algebra, *Addison-Wesley, 1970* .

[11] *S. Lipschutz,* Linear Algebra, *Schaum's Outline Series, McGraw-Hill, 1974* .

[12] *I. D. Macdonald,* The Theory of Groups, *Oxford University Press, 1968* .

[13] *S. MacLane and G.Birkhoff,* Algebra, *Macmillan, 1968 .*
[14] *N. H. McCoy,* Introduction to Modern Algebra, *Allyn And Bacon, 1975 .*
[15] *J.J. Rotman,* The Theory of Groups : *An Introduction, Allyn and Bacon, 1973 .*
[16] *I. Stewrt,* Galois Theory, *Chapman and Hall, 1975 .*
[17] *I. Stewrt and D. Tall,* The Foundations of Mathematics, *Oxford University Press, 1977 .*

Reference useful for Book 6

1: *Ideals [**3**, Chapters 2-5], [**4**, Section 10.1], [**8**, Chapter 3], [**13**, Chapter 4] .*
2: *Divisibility [**3**, Chapter 6], [**6**, Chapters 9,31,32], [**8**, Chapter 3], [**13**, Chapter 4] .*
3: *Fielbs [**1**, Chapters 2,3], [**8**, Chapter 5], [**16**, Chapters 3,4,7-12] .*
4: *Modules [**3**, Chapter 12], [**4**, Sections 10.2-10.6], [**13**, Chapter 6] .*
*In [**4**], [**6**] and [**13**] all rings have a 1, and a subring must contain the ring identity . Ring morphisms (called ring homomorphisms in [**4**] and [**6**]) must map the identity element . In [**4**] ring morphisms are written as mappings on the right . The definition of and integral domain given in [**6**] does not require it to be commutative*

Algebra through practice

Acoollection of problems in algebra, with solutions

Rings , fields and Modules

T. S. BLYTH ◦ E. F. ROBERTSON

Algebra Throuogh Practice

T.S. Blyth - E.F.Robertson

A Collection of Problems in Algebra, With Solutions

Rings, Fields & Modules

Translated by:
Dr. H. R. Meymany