گروه G را در نظر بگیرید و فرض کنید $Inn(G)$ گروه خودریختی هلی داخلی G است. ثابت کنید $Inn(G)$ زیرگروه نرمال $Aut(G)$ است و $G/Z(G) \cong Inn(G)$

اول باید اثبات کنیم Inn(G) زیرگروه است:

$$\forall(\tau_m, \tau_n \in Inn(G)), \tau_m \circ \tau_n^{-1} \in Inn(G)$$
$$\tau_m(x) = m.x.m^{-1}$$
$$\tau_n(x) = n.x.n^{-1} \rightarrow \tau_n^{-1}(x) = n^{-1}.x.n$$
$$\tau_m(\tau_n^{-1}(x)) = \tau_m(n^{-1}.x.n) = m.(n^{-1}.x.n).m^{-1} = (m.n^{-1}).x.(n.m^{-1})$$

از اون‌جایی که

$$n.m^{-1} = (m.n^{-1})^{-1}$$
$$(m.n^{-1}).x.(m.n^{-1})^{-1} \in Inn(G)$$

فرض می‌کنیم $m.n^{-1} = r$ باشه، پس این خودریخت داخلی به فرم $\tau_r(x) = r.x.r^{-1}$ در Inner موجوده.

حال نرمال بودن Inn(G) رو بررسی می‌کنیم: یعنی

$$\forall(f \in Aut(G)), f \circ Inn(G) \circ f^{-1} \subseteq Inn(G)$$

خودریخت داخلی τ_m رو از Inner می‌گیریم اثبات می‌کنیم که ترکیبش مثل بالا باز داخل Inner هست:

$$\tau_m(x) = m.x.m^{-1} \in Inn(G) \rightarrow f(\tau_m(f^{-1}(x))) \in Inn(G)$$

فرض می‌کنیم $f^{-1}(x) = x'$:

$$f(\tau_m(x')) = f(m.x'.m^{-1})$$

از اون‌جایی که f خودریخت است:

$$f(m.x'.m^{-1}) = f(m).f(x').f(m^{-1})$$

چون f یک‌به‌یک و پوشا ست پس

$$f(x') = f(f^{-1}(x)) = x$$

همچنین در خاصیت هم‌ریختی داریم:

$$f(m^{-1}) = f(m)^{-1}$$

همچنین فرض می‌کنیم $f(m) = m'$ پس

$f(m).f(x').f(m)^{-1} = m'.x.m'^{-1} \in Inn(G)$

بنابراین در Inner موجوده. $\square$

$\phi : G \to Inn(G)$
$\phi(g) = (\tau_g(x) = gxg^{-1})$

$Ker(\phi) = \{g \in G : \phi(g) = \tau_e(x) = I\} = \{g \in G : \forall x \in G,\, gxg^{-1} = x\} = \{g \in G : \forall x \in G,\, gx = xg\}$

از قضیه اول یکریختی گروه‌ها خواهیم داشت

$G/Ker(\phi) = G/Z(G) \cong Im(\phi) = \phi(G) = Inn(G)\square$

گروه چهارتایی کلاین را درنظر بگیرید (k_4) حال ثابت کنید $Aut(k_4) \cong S_3$

خودریخت‌های چهارتایی کلاین

$$
\begin{aligned}
&k_4 = \{e, a, b, ab\}\\
&a^2 = e\\
&b^2 = e\\
&(ab)^2 = e\\
&a.(ab) = (ab).a = b\\
&b.(ab) = (ab).b = a
\end{aligned}
$$

توی هر خودریختش e باید به e بره پس فقط روی اعضای a و b و ab بحث می‌کنیم
می‌تونیم خودریخت‌ها رو این‌طور تعریف کنیم که هر کدوم از این سه تا به همدیگه برن یعنی مثلا جای a و b عوض شه

$$
\begin{aligned}
&a \to b\\
&b \to a\\
&ab \to ab
\end{aligned}
$$

به یه زبان دیگه، جایگشت‌های ممکن بین a b ab می‌شه که یعنی ۶ تا خودریخت خواهیم داشت که یکریخت است با S_3 $\square$

ثابت کنید تنها خودریختی گروه دوری از مرتبه ۲ خودریختی همانی است.

$G = \langle a \rangle = \{e, a\}$

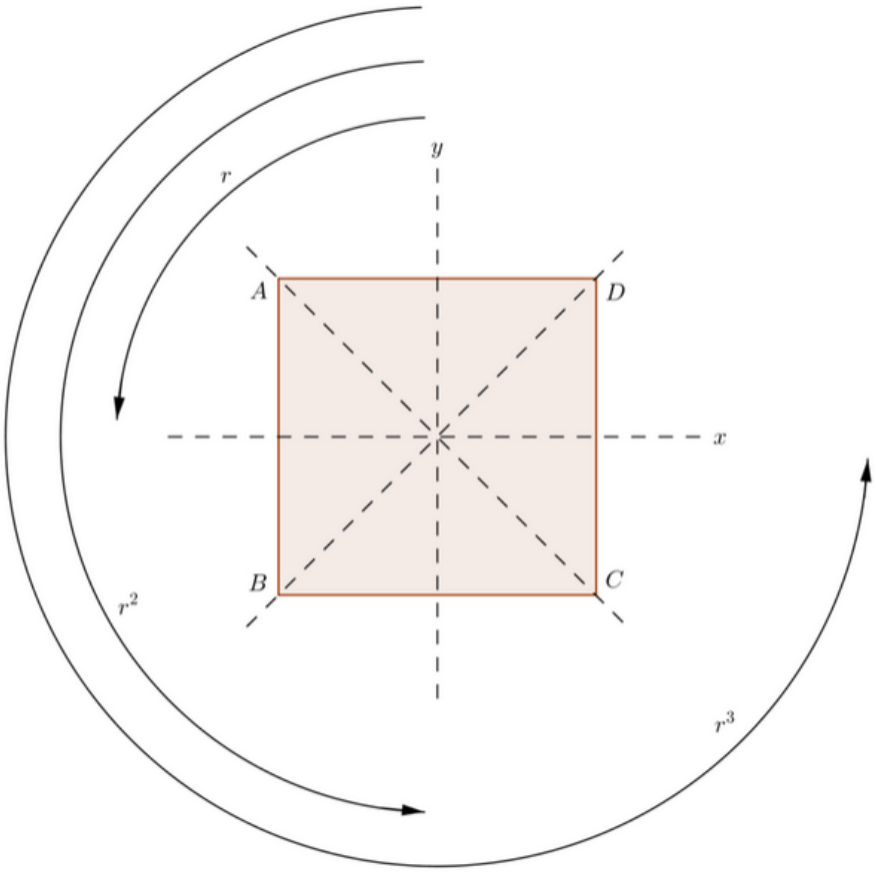
هر خودریختی گروه دوری باید مولد گروه را به مولدی دیگر ببرد زیرا

$\phi : G \to G$
$\phi(a^k) = \phi(a)^k$

و G تنها یک مولد دارد پس فقط یک خودریختی موجود است و آن نیز همانی است. $\square$

اگر G گروه دووجهی از مرتبه ۸ باشد، Aut(G) و Inn(G) و Aut(G)/Inn(G) را بیابید.

برابر است با گروه تقارن‌های مربع.



$$G = D_4 = \{e, r^1, r^2, r^3, t_x, t_y, t_{AC}, t_{BD}\} = \{e, r^1, r^2, r^3, t_x, r^1t_x, r^2t_x, r^3t_x\}$$

r^i ها توسط r و r^3 تولید خواهند شد همچنین r^it_xها توسط مابقی یعنی خودریختی‌ها برابر خواهند بود با

$$(r, t_x)\,(r, rt_x)\,(r, r^2t_x)\,(r, r^3t_x)$$
$$(r^3, t_x)\,(r^3, rt_x)\,(r^3, r^2t_x)\,(r^3, r^3t_x)$$

منظور از (r^3, rt_x) تابع خودریختی است که r را به r^3 و t_x را به rt_x مپ می کند.

یعنی $|Aut(G)| = 2*4 = 8$ خودریختی خواهیم داشت و برای Inn(G) می‌توان از $G/Z(G) \cong Inn(G)$ استفاده کرد

$$\lambda : G/Z(G) \to Inn(G)$$
$$\lambda(g + Z(G)) = \tau_g$$
$$Z(G) = \{g \in G \,:\, \forall x \in G,\, xg = gx\} = \{e, r^2\}$$
$$G/Z(G) = \{Z(G),\, r + Z(G),\, t_x + Z(G),\, rt_x + Z(G)\}$$
$$Inn(G) = \lambda(G/Z(G)) = \{\tau_e,\, \tau_r, \tau_{t_x},\, \tau_{rt_x}\}$$

$$\tau_e(r) = r$$
$$\tau_e(t_x) = t_x$$
$$(r, t_x)$$

$$\tau_r(r) = r.r.r^3 = (r^2).r^3 = r$$
$$\tau_r(t_x) = r.t_x.r^3 = (rt_x).r^3 = r^2t_x$$
$$(r, r^2t_x)$$

$$\tau_{t_x}(r) = t_x.r.t_x = (r^3t_x).t_x = r^3$$
$$\tau_{t_x}(t_x) = t_x.t_x.t_x = (e).t_x = t_x$$
$$(r^3, t_x)$$

$$\tau_{rt_x}(r) = rt_x.r.rt_x = (t_x).rt_x = r^3$$
$$\tau_{rt_x}(t_x) = rt_x.t_x.rt_x = (r).rt_x = r^2t_x$$
$$(r^3, r^2t_x)$$

و برای $Aut(G)/Inn(G)$ خواهیم داشت:

$$Aut(G)/Inn(G) = \{Inn(G), (r, rt_x) \circ Inn(G)\}$$

فرض کنید A و B زیرگروه‌های نرمالی از G باشند به طوری که

$$i)\, G = AB \ \ , \ \ ii)\, A \cap B = \{e\}$$

در این صورت ثابت کنید $G \cong A \times B$

$$\phi : A \times B \to G$$
$$\phi((a,b)) = a.b$$

اثبات جابه‌جایی بودن G:

$$a, a^{-1} \in A$$
$$b, b^{-1} \in B$$

$$b.a^{-1}.b^{-1} \in A \to a.(b.a^{-1}.b^{-1}) \in A$$
$$a.b.a^{-1} \in B \to (a.b.a^{-1}).b^{-1} \in B$$

$$a.b.a^{-1}.b^{-1} \in A \cap B$$
$$A \cap B = \{e\} \to a.b.a^{-1}.b^{-1} = e$$
$$a.b.a^{-1}.b^{-1}.b.a = b.a \to a.b = b.a\square$$

اثبات همریختی:

$$\phi((a_1,b_1).(a_2,b_2)) = \phi((a_1a_2,b_1b_2)) = \phi((a_1,b_1)).\phi((a_2,b_2)) = a_1b_1a_2b_2 = a_1a_2b_1b_2\square$$

یک به یک بودن:

$$Ker(\phi) = \{(a,b) \in A \times B : \phi((a,b)) = e\} = \{(a,b) \in A \times B : a.b = e\} = \{(e,e)\}$$
$$|Ker(\phi)| = 1 \leftrightarrow \forall a,b \in A \ \ c,d \in B,\ f((a,c)) = f((b,d)) \to (a,c) = (b,d)\square$$

پوشا بودن:

$$\forall g \in G,\ \exists a \in A \ \ b \in B,\ f((a,b)) = g$$
$$a.b = g$$

از ii خواهیم داشت که f پوشا است. $\square$

حلقه کواترنیون‌ها را توصیف کنید.

$1 = (1, 0, 0, 0)$
$i = (0, 1, 0, 0)$
$j = (0, 0, 1, 0)$
$k = (0, 0, 0, 1)$

$1 * 1 = 1$
$i * i = j * j = k * k = i * j * k = -1$
$i * 1 = 1 * i = i$
$j * 1 = 1 * j = j$
$k * 1 = 1 * k = k$
$i * j = k$
$i * k = -j$
$j * i = -k$
$j * k = i$
$k * i = j$
$k * j = -i$

$H = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$

$(a_1+b_1i+c_1j+d_1k)+(a_2+b_2i+c_2j+d_2k) = (a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k$
$(a_1 + b_1i + c_1j + d_1k) * (a_2 + b_2i + c_2j + d_2k) = (a_1 * a_2) + (a_1 * b_2)i + ... + (c_1 * b_2)(j * i) + ... + (d_1 * d_2)k^2$

نکته: حلقه کواترنیون‌ها جابه‌حایی نیست.

یک حلقه R دارای قانون حذف از چپ و راست است اگر و تنها اگر R دارای مقسوم علیه صفر نباشد.

اگر حلقه R دارای قانون حذف از چپ و راست باشد آنگاه مقسوم علیه صفر ندارد:
فرض می‌کنیم که داشته باشد آنگاه

$$a, b \neq 0 \in R$$

$$a * b = 0$$
$$a * b = 0$$
$$a * b = a * 0$$
$$b = 0$$

که بر خلاف فرض است. $\perp$

اگر مقسوم علیه صفر نداشته باشد آنگاه حلقه R دارای قانون حذف از چپ و راست است:

$$a = b$$
$$a - b = 0$$
$$c * (a - b) = 0$$
$$c * a - c * b = 0$$
$$c * a = c * b \star$$

$$(a - b) * c = 0$$
$$a * c - b * c = 0$$
$$a * c = b * c \star$$

$\square$

فرض کنید R یک حلقه و $S \subseteq R$ باشد، S زیرحلقه از R است اگر و تنها اگر

$$i) \forall a, b \in S,\ a - b \in S$$
$$ii) \forall a, b \in S,\ ab \in S$$

اگر S زیر حلقه‌ای از R باشد،آنگاه i و ii صدق خواهند کرد:
چون با عمل جمع یک گروه آبلی است بنابراین i صدق خواهد کرد.
چون زیرحلقه نسبت به عمل ضرب بسته است، ii نیز برقرار است. □

اگر i و ii آنگاه S زیر حلقه‌ای از R می‌باشد:
از i خواهیم داشت:

$$\forall a, b \in S$$
$$a - (-b) = a + b \in S$$
$$a - a = 0 \in S$$
$$0 - a \in S$$

و همچنین چون $S \subseteq R$ پس با عمل جمع جابه‌جایی و شرکت‌پذیر است، بنابر این با عمل جمع یک گروه آبلی را تعریف می‌کند.

و از ii خواهیم داشت که S نسبت به عمل ضرب بسته است و چون $S \subseteq R$ با عمل ضرب نیز شرکت‌پذیر و روی جمع نیز توزیع پذیر است، بنابراین S زیرحلقه‌ای از R است. □

قضیه اول یک‌ریختی حلقه‌ها را بیان و اثبات کنید.

$(R, +, \times)$ $(E, +', \times')$
$\phi : R \to E$
$\phi(r + t) = f(r) +' f(t)$
$\phi(r \times t) = f(r) \times' f(t)$

آنگاه $R/Ker(\phi) \cong Im(\phi)$ خواهد بود.

اثبات آیده‌آل بودن $Ker(\phi)$ برای R:

$\forall r, t \in Ker(\phi),\ r - t \in Ker(\phi)$
$f(r) - f(t) = 0_E - 0_E = 0_E = f(r - t) \to r - t \in Ker(\phi)$

$\forall r \in R,\ t \in Ker(\phi),\ r \times t \in Ker(\phi)$
$f(r) \times f(t) = f(r) \times 0_E = 0_E = f(r \times t) \to r \times t \in Ker(\phi)$

اثبات زیر حلقه بودن $Im(\phi)$ برای E:

$\forall r, t \in Im(\phi),\ r -' t \in Im(\phi)$
$r, t \in Im(\phi) \to \exists s, u \in R,\ \phi(s) = r \wedge \phi(u) = t$
$r -' t = \phi(s) -' \phi(u) = \phi(s) +' \phi(-u) = \phi(s - u)$
$s -' u \in Im(\phi)$

$\forall r, t \in Im(\phi),\ r \times' t \in Im(\phi)$
$r, t \in Im(\phi) \to \exists s, u \in R,\ \phi(s) = r \wedge \phi(u) = t$
$r \times' t = \phi(s) \times' \phi(u) = \phi(s \times u)$
$r \times' t \in Im(\phi)$

تابع همریختی λ رو این‌گونه تعریف می‌کنیم:

$\lambda : R/Ker(\phi) \to Im(\phi)$
$\lambda(r + Ker(\phi)) = \phi(r)$

اثبات همریختی λ:

$\lambda((r+Ker(\phi))+(t+Ker(\phi))) = \lambda((r+t)+Ker(\phi)) = \phi(r+t) = \phi(r)+'\phi(t) = \lambda(r+Ker(\phi)) +' \lambda(t+Ker(\phi))$

$\lambda((r+Ker(\phi))\times(t+Ker(\phi))) = \lambda((r\times t)+Ker(\phi)) = \phi(r\times t) = \phi(r)\times'\phi(t) = \lambda(r+Ker(\phi)) \times' \lambda(t+Ker(\phi))$

اثبات یک به یک بودن λ:

$Ker(\lambda) = \{r + Ker(\phi) \in R/Ker(\phi) \ : \ \lambda(r + Ker(\phi)) = 0\} = \{Ker(\phi)\}$

چون کاردینال $Ker(\lambda)$ برابر یک است بنابر این یک به یک است.

اثبات پوشا بودن λ:

$\lambda(R/Ker(\phi)) = \phi(R) = Im(\phi)$

$\square$

حلقه چندجمله‌ای‌ها را توصیف کنید

$(R, +, \times)$

$x^0 = 1 = (1, 0, 0, 0, ...)$
$x^1 = (0, 1, 0, 0, ...)$
$x^2 = (0, 0, 1, 0, ...)$
.
.
.

$R[x] = \{f(x) = \Sigma_{i=0}^{n} a_i x^i \ : \ n \in \mathbb{Z}_0^+ \ \ a_i \in R\}$

$n < m$
$f(x) + g(x) = \Sigma_{i=0}^{n} a_i x^i \ + \ \Sigma_{i=0}^{m} b_i x^i = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n + ... + (b_m)x^m$
$f(x) \times g(x) = \Sigma_{i=0}^{n} a_i x^i \ \times \ \Sigma_{i=0}^{m} b_i x^i = (a_0 \times b_0) + (a_0 \times b_1)x + ... + (a_n \times b_m)x^{nm}$

نکته: حلقه چندجمله‌ای ها یک حلقه جابه‌جایی است اگر و تنها اگر R حلقه جابه‌جایی باشد.
نکته: حلقه چندجمله‌ای ها یک حوزه صحیح است اگر و تنها اگر R حوزه صحیح باشد.

فرض کنید $\mathbb{R}$ میدان اعداد حقیقی باشد و $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a,b) : a,b \in \mathbb{R}\}$ اعمال $+$ و $\times$ را روی $\mathbb{C}$ به این صورت تعریف می‌کنیم:

$$(a,b) + (c,d) = (a+c, b+d)$$
$$(a,b) \times (c,d) = (ac - bd, ad + bc)$$

ثابت کنید یک میدان است.

گروه آبلی با عمل جمع:

۱) بسته بودن:
بدیهی ست که بسته است

۲) شرکت‌پذیری:

$$((a,b) + (c,d)) + (e,f) = (a+c, b+d) + (e,f) = (a+c+e, b+d+f) = (a,b) + (c+e, d+f) = (a,b) + ((c,d) + (e,f))$$

۳) عضو خنثی:

$$(a,b) + 0 = (a,b)$$
$$0 = (0,0)$$

۴) عضو وارون:

$$(a,b) + (a,b)^{-1} = (0,0)$$
$$(a,b)^{-1} = (-a,-b)$$

۵): جابه‌جایی:

$$(a,b) + (c,d) = (a+c, b+d) = (c+a, d+b) = (c,b) + (a,b)$$

گروه آبلی با عمل ضرب:
(1 بسته بودن:
بدیهی ست که بسته است

۲) شرکت‌پذیری:

$((a,b)\times(c,d))\times(e,f) = (ac-bd, ad+bc)\times(e,f) = (ace-bde-adf-bcf, acf-bdf+ade+bce) = (a,b)\times(ce-df, cf+de) = (a,b)\times((c,d)\times(e,f))$

۳) عضو خنثی:

$(a,b)\times 1 = (a,b)$
$1 = (1,0)$

۴) عضو وارون:

$(a,b)\times(a,b)^{-1} = (1,0)$
$(a,b)\times(a,b)^{-1} = (a,-b)\times(a,-b)^{-1}$
$(a,b)^{-1} = (a,-b)\times(a,-b)^{-1}\times(a,b)^{-1}$
$(a,b)^{-1} = (a,-b)\times((a,-b)\times(a,b))^{-1}$
$(a,b)^{-1} = (a,-b)\times(a^2+b^2,0)^{-1}$
$(a,b)^{-1} = (a,-b)\times(a^2+b^2,0)^{-1}$
$(a,b)^{-1} = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$

۵): جابه‌جایی:

$(a,b)\times(c,d) = (ac-bd, ad+bc) = (ca-db, da+cb) = (c,b)\times(a,b)$

توزیع‌پذیری ضرب روی جمع:

$(a,b)\times((c,d)+(e,f)) = (a,b)\times(c+e, d+f) = (ac+ae-bd-bf, ad+af+bc+be) = (ac-bd+ae-bf, ad+bc+af+be) = ((a,b)\times(c,d)) + ((a,b)\times(e,f)) = ((c,d)\times(a,b)) + ((e,f)\times(a,b)) = ((c,d)+(e,f))\times(a,b)\square$

فرض کنید R یک حلقه باشد نشان دهید R در $R[x]$ نشاندنی است.

$$\phi : R \to R[x]$$
$$\phi(r) = rx^0$$

$$\phi(r+t) = (r+t)x^0 = rx^0 + tx^0 = \phi(r) + \phi(t)$$
$$\phi(r \times t) = (r \times t)x^0 = rx^0 \times tx^0 = \phi(r) \times \phi(t)$$

یک به یک بودن:

$$\phi(r) = \phi(t) \to r = t$$
$$rx^0 = tx^0$$
$$r = t$$

$\square$

یک ایده‌آل برای حلقه چندجمله‌ای‌های $\mathbb{R}[x]$ بیابید.

$$I = \{f(x) \in \mathbb{R}[x] \,:\, f(0) = 0\}$$

اثبات ایده‌آل بودن:

$$\forall f(x), g(x) \in I,\ f(x) - g(x) \in I$$
$$f(x) - g(x) = t(x)$$
$$f(0) - g(0) = t(0)$$
$$0 - 0 = 0 = t(0)$$
$$t(x) \in I$$

$$\forall f(x) \in \mathbb{R}[x],\ g(x) \in I,\ f(x) \times g(x) \in I$$
$$f(x) \times g(x) = t(x)$$
$$f(0) \times g(0) = t(0)$$
$$f(0) \times 0 = 0 = t(0)$$
$$t(x) \in I \square$$

فرض کنید $R[\sqrt{p}] = \{a + b\sqrt{p} \,|\, a, b \in \mathbb{Q}\} \quad p \in P(Set\,of\,prime\,numbers)$
ثابت کنید که $(R[\sqrt{p}], +, \times)$ که در آن $+$ و $\times$ جمع و ضرب اعداد حقیقی هستند، یک میدان می‌باشد.

اثبات گروه آبلی بودن با عمل جمع:

$$a_1 + b_1\sqrt{p}, a_2 + b_2\sqrt{p} \in R[\sqrt{p}]$$

۱. بسته بودن:

$$(a_1 + b_1\sqrt{p}) + (a_2 + b_2\sqrt{p})$$

از خاصیت شرکت‌پذیری و جابه‌جایی عمل جمع و توزیع پذیری عمل ضرب روی جمع $\mathbb{R}$ خواهیم داشت:

$$(a_1 + a_2) + (b_1 + b_2)\sqrt{p} \in R[\sqrt{p}]$$

۲. شرکت‌پذیری:
از شرکت‌پذیر بودن $\mathbb{R}$ نتیجه می‌شود که $R[\sqrt{p}]$ نیز شرکت‌پذیر است.

۳. عضو همانی:

$$(a_1 + b_1\sqrt{p}) + (a_2 + b_2\sqrt{p}) = (a_1 + b_1\sqrt{p})$$
$$(a_2 + b_2\sqrt{p}) = 0 + 0\sqrt{p}$$

۴. عضو وارون:

$$(a + b\sqrt{p}) + (a^{-1} + b^{-1}\sqrt{p}) = 0 + 0\sqrt{p}$$
$$(a + a^{-1}) + (b + b^{-1})\sqrt{p} = 0 + 0\sqrt{p}$$
$$a^{-1} + b^{-1}\sqrt{p} = -a + -b\sqrt{p}$$

۵. آبلی بودن:

$$(a_1 + b_1\sqrt{p}) + (a_2 + b_2\sqrt{p}) = (a_2 + b_2\sqrt{p}) + (a_1 + b_1\sqrt{p})$$
$$(a_1 + a_2) + (b_1 + b_2)\sqrt{p} = (a_2 + a_1) + (b_2 + b_1)\sqrt{p}$$

از آبلی بودن گروه $\mathbb{R}$ با عمل جمع می‌تونیم نتیجه بگیریم که $R[\sqrt{p}]$ با عمل جمع هم آبلی ست.

اثبات گروه آبلی بودن با عمل ضرب:

$a_1 + b_1\sqrt{p}, a_2 + b_2\sqrt{p} \in R[\sqrt{p}]$

۱. بسته بودن:

$(a_1 + b_1\sqrt{p}) \times (a_2 + b_2\sqrt{p}) =$
$a_1a_2 + a_1b_2\sqrt{p} + a_2b_1\sqrt{p} + (b_1\sqrt{p})(b_2\sqrt{p}) =$
$(a_1a_2 + b_1b_2p) + (a_1b_2 + a_2b_1)\sqrt{p} \in R[\sqrt{p}]$

۲. شرکت‌پذیری:

$a_3 + b_3\sqrt{p} \in R[\sqrt{p}]$
$((a_1 + b_1\sqrt{p}) \times (a_2 + b_2\sqrt{p})) \times (a_3 + b_3\sqrt{p}) = ((a_1 + b_1\sqrt{p}) \times (a_2 + b_2\sqrt{p})) \times (a_3 + b_3\sqrt{p})$

اگه دو طرف رو طبق خاصیت توزیع‌پذیری عمل ضرب روی جمع $\mathbb{R}$ باز کنیم به این نتیجه خواهیم رسید که دو طرف معادله یکسان هستند

۳. عضو همانی:

$(a_1 + b_1\sqrt{p}) \times (a_2 + b_2\sqrt{p}) = (a_1 + b_1\sqrt{p})$
$a_2 + b_2\sqrt{p} = 1 + 0\sqrt{p}$

۴. عضو وارون:

$(a + b\sqrt{p}) \times (a^{-1} + b^{-1}\sqrt{p}) = 1$
$(a^{-1} + b^{-1}\sqrt{p}) = \frac{1}{a + b\sqrt{p}}$
$(a^{-1} + b^{-1}\sqrt{p}) = \frac{a - b\sqrt{p}}{a^2 - b^2p} = \frac{a}{a^2 - b^2p} + \frac{-b}{a^2 - b^2p}\sqrt{p}$

۵. آبلی بودن:

$(a_1 + b_1\sqrt{p}) \times (a_2 + b_2\sqrt{p}) = (a_2 + b_2\sqrt{p}) \times (a_1 + b_1\sqrt{p})$

اگه باز کنیم دو طرف معادله یکسان خواهند شد.

توزیع‌پذیری عمل ضرب روی جمع:

$(a_1 + b_1\sqrt{p}) \times ((a_2 + b_2\sqrt{p}) + (a_3 + b_3\sqrt{p})) = (a_1 + b_1\sqrt{p}) \times (a_2 + b_2\sqrt{p}) + (a_1 + b_1\sqrt{p}) \times (a_3 + b_3\sqrt{p})$
$(a_1 + b_1\sqrt{p}) \times ((a_2 + a_3) + (b_2 + b_3)\sqrt{p})) =$
$a_1(a_2 + a_3) + a_1\sqrt{p}(b_2 + b_3) + b_1\sqrt{p}(a_2 + a_3) + b_1p(b_2 + b_3) = a_1(a_2 + a_3) + b_1p(b_2 + b_3) + \sqrt{p}(a_1b_2 + a_2b_1 + a_1b_3 + a_3b_1)$

$(a_1 + b_1\sqrt{p}) \times (a_2 + b_2\sqrt{p}) + (a_1 + b_1\sqrt{p}) \times (a_3 + b_3\sqrt{p}) = (a_1a_2 + b_1b_2p) + (a_1b_2 + a_2b_1)\sqrt{p} + (a_1a_3 + b_1b_3p) + (a1_b3 + a_3b_1)\sqrt{p} = a_1(a_2 + a_3) + b_1p(b_2 + b_3) + \sqrt{p}(a_1b_2 + a_2b_1 + a_1b_3 + a3_b1)$

دو طرف معادله یکسان است پس یک میدان است. $\square$

همریختی حلقه‌ها را تعریف و چند ویژگی همریختی را بیان کنید و ثابت کنید.

$(R, +, \times)$, $(E, +', \times')$

$\phi : R \to E$
$\phi(x + y) = \phi(x) +' \phi(y)$
$\phi(x \times y) = \phi(x) \times' \phi(y)$

$\phi(0_R) = 0_E$
$Proof.$
$\phi(x + 0_R) = \phi(x) +' \phi(0_R) = \phi(x) \to \phi(0_R) = 0_E \square$

$\phi(-x) = -\phi(x)$
$Proof.$
$\phi(x - x) = \phi(x) +' \phi(-x) = \phi(0_R) = 0_E \to \phi(-x) = -\phi(x) \square$

$\phi(nx) = n\phi(x)$
$Proof.$
$\phi(x + x + x + ... + x) = \phi(x) +' \phi(x) +' \phi(x) +' ... +' \phi(x) = n\phi(x) \square$

$\phi(1_R) = 1_E$
$Proof.$
$\phi(x \times 1_R) = \phi(x) \times' \phi(1_R) = \phi(x) \to \phi(1_R) = 1_E \square$

$\phi(x^{-1}) = \phi(x)^{-1}$
$Proof.$
$\phi(x \times x^{-1}) = \phi(x) \times' \phi(x^{-1}) = \phi(1_R) = 1_E \to \phi(x) = \phi(x)^{-1} \square$

$\phi(n^x) = \phi(x)^n$
$Proof.$
$\phi(x \times x \times x \times ... \times x) = \phi(x) \times' \phi(x) \times' \phi(x) \times' ... \times' \phi(x) = \phi(x)^n \square$

$T \subseteq R \to \phi(T) \subseteq E$
$Proof.$
$i)$ $\forall x, y \in T$, $\phi(x) - \phi(y) \in \phi(T)$
$\phi(x) -' \phi(y) = \phi(x) +' \phi(-y) = \phi(x - y)$
$x - y \in T \to \phi(x - y) = \phi(x) -' \phi(y) \in \phi(T) \square$

$ii)$ $\forall x, y \in T$, $\phi(x) \times' \phi(y) \in \phi(T)$
$\phi(x) \times' \phi(y) = \phi(x \times y)$
$x \times y \in T \rightarrow \phi(x \times y) = \phi(x) \times' \phi(y) \in \phi(T) \square$

تمام حلقه‌های خارج قسمتی $\mathbb{Z}$ را پیدا کنید.

تمام ایده‌آل‌های $\mathbb{Z}$ ایده‌آل اصلی هستند. اثبات:
فرض کنید n کوچک‌ترین عضو مثبت غیرصفر I باشد. طبق الگوریتم تقسیم خواهیم داشت:

$$\forall a \in I,\ \exists q \in \mathbb{Z},\ r \in I,\ a = qn + r \quad 0 \leq r < n$$
$$r = a - qn$$

چون r و n عضوی از I هستند و $r < n$ بنابر این $r = 0$ بنابراین I تولید شده ایده‌آل تولید شده توسط n است.

بنابر این آیده‌ال‌های $\mathbb{Z}$ به فرم $n\mathbb{Z},\ n \in \mathbb{Z}$ هستند.
حلقه‌های خارج‌قسمتی $\mathbb{Z}$ به فرم زیر خواهند بود

$$\mathbb{Z}/n\mathbb{Z} = \{r + n\mathbb{Z} : r \in \{0, ..., n-1\}\}$$

یک حلقه R را یک حلقه بولی گویند اگر به ازای هر $a \in R$ $a^2 = a$
ثابت کنید در حلقه بولی R
الف) به ازای هر $a \in R$ $a + a = 2a = 0$

$$(2a)^2 = 2a$$
$$(a+a)^2 = a + a$$
$$(a+a)(a+a) = a + a$$
$$(a+a)a + (a+a)a = a + a$$
$$a^2 + a^2 + a^2 + a^2 = a + a$$
$$a + a + a + a = a + a$$
$$a + a = 0 = 2a$$

ب) به ازای هر $a, b \in R$ $ab = ba$ یعنی R یک حلقه جابه‌جایی است.

$$(a+b)^2 = a + b$$
$$(a+b)(a+b) = a + b$$
$$(a+b)a + (a+b)b = a + b$$
$$a^2 + ba + ab + b^2 = a + b$$
$$a + ba + ab + b = a + b$$

از سمت راست با $-b$ جمع می‌کنیم

$$a + ba + ab = a$$

از سمت چپ با $-a$ جمع می‌کنیم

$$ba + ab = 0$$

از الف داریم $2a = a + a = 0$ که به معنای اینه وارون هر عضو، خودشه.
چون R تحت عمل ضرب بسته ست و وارون هر عضو در گروه منحصر به فرد است و وارون دیگه‌ای نداره پس از $ba + ab = 0$ نتیجه خواهیم گرفت که $ba = ab$

یا این‌طور بگیم

$$ba = -(ab)$$

و از الف خواهیم داشت

$$\forall a \in R, a + a = 0$$
$$\forall a \in R, -a = a$$
$$ba = -(ab) = ab \square$$