Determinant

Ali Nesin

24 Eylül 2022

Matematik Köyü'nde verdiğim günde (en fazla) birer saatten 6 günlük dersin notlarıyla karşı karşıyasınız. Birinci bölümde ihtiyacımız olan mültilineer cebir işleniyor. Asıl determinant konusunu ikinci bölümde bulacaksınız. Determinantları değişmeli herhangi bir halka üzerine işlediğimize dikkatinizi çekerim.

Yazıyı iyi anlamak için biraz modül teori bilmek gerekiyorsa da, biz daha çok değişmeli bir R halkası için R^n biçimindeki modüllerle çalışacağımız için modül bilgisi pek elzem olmayacak. Dileyen okur "modül" sözcüğünü "vektör uzayı", "halka" sözcüğünü "cisim" olarak okuyabilir. Meraklılar için modülün tanımını verelim: Bir R-modül aynen K-vektör uzayları gibi tanımlanır, tek farkla ki, vektör uzaylarında cisim olan K yerine, bir R halkası alınır[1]. Bu ufak değişiklik dramatik farklılıklara yol açar. Mesela her vektör uzayının bir tabanı varken, her modülün tabanı yoktur. Öte yandan R^n modüllerinin bir tabanı vardır elbette.

Birçok ayrıntıyı soru olarak dipnotlara yerleştirdik. Hemen hemen her biri kolaydır. Temel bir lineer cebir altyapısı olan her öğrenci bu soruların yanıtlarını zorlanmadan bulabilmeli. Kombinasyon hesapları ya da permütasyon gruplarıyla ilgili bir iki soru daha çetin olabilir; ilk okuyuşta o sorulara okurun fazla zaman harcamaması yerinde olur.

1 Mültilineer Formlar

1.1 Genel Teori

R değişmeli bir halka ve M bir R-modül olsun[2]. $k > 0$ bir doğal sayı olsun. Her koordinata göre R-lineer olan bir $f : M^k \longrightarrow R$ fonksiyonuna R-***mülti-***

[1] Halkalarımız her zaman değişmeli olacak ve çarpımsal birim elemanını içerecek.

[2] Modüllerle aşina olmayanlar $M = R^n$ alabilirler. Nitekim bir sonraki paragrafta biz de öyle yapacağız.

lineer form denir[3]. R-mültilineer formlar kümesini $\mathcal{L}_k M$ olarak gösterelim. Elbette $\mathcal{L}_k M$ de bir R-modüldür[4]. Eğer X, M'nin bir üreteç kümesiyse, her $f \in \mathcal{L}_k M$ formu X^k kümesinde aldığı değerlerle belirlenir[5].

Eğer $M \simeq R^n$ ise (yani M, n boyutlu serbest bir modülse, bir başka deyişle n elemanlı bir tabanı varsa[6]) ve $e_1, \ldots, e_n$ elemanları M'nin sıralı bir tabanıysa, o zaman her $f \in \mathcal{L}_k M$ formu, $i_1, \ldots, i_k \in \{1, 2, \ldots, n\}$ için $f(e_{i_1}, \ldots, e_{i_k}) \in R$ değerleri tarafından, yani R^{n^k} kümesinin bir elemanı tarafından belirlenir[7]. Ayrıca R^{n^k} kümesinin her elemanı bir form belirler[8]. Daha güçlü bir ifade doğrudur:

$$f \mapsto (f(e_{i_1}, \ldots, e_{i_k}))_{i_1,\ldots,i_k}$$

kuralı, $\mathcal{L}_k M$ ile R^{n^k} modülleri arasında bir R-modül izomorfisi tanımlar[9]. Demek ki M, n boyutlu serbest modülse $\mathcal{L}_k M$ de serbest bir modüldür ve boyutu n^k olur. $\mathcal{L}_k M$ serbest modülünün bir tabanını bulmayı okura bırakıyoruz[10].

1.2 Simetrik Formlar

Bu yazıda simetrik formlara ihtiyacımız olmayacak ama genel kültür için konuya biraz dokunalım.

Eğer $f \in \mathcal{L}_k M$ formu, her $\sigma \in \mathrm{Sym}\, k$ ve her $m_i \in M$ için

$$f(m_1, \ldots, m_k) = f(m_{\sigma(1)}, \ldots, m_{\sigma(1)})$$

eşitliğini sağlıyorsa, f'ye ***simetrik form*** denir. Simetrik formlar kümesini $\mathcal{S}_k M$ olarak gösterelim. $\mathcal{S}_k M$ bir R-modüldür[11].

Eğer $M \simeq R^n$ ise ve $e_1, \ldots, e_n$ elemanları M'nin sıralı bir tabanıysa, o zaman her $f \in \mathcal{L}_k M$ formu, $1 \le i_1 \le \ldots \le i_k \in \{1, 2, \ldots, n\}$ için $f(e_{i_1}, \ldots, e_{i_k}) \in R$ değerleri tarafından belirlenir. Öte yandan,

$$\{(i_1, \ldots, i_k) : i_j \in \{1, 2, \ldots, n\} \text{ ve } i_1 \le \ldots \le i_k\}$$

[3] Yani k kordinattan hangi $k-1$ tanesini sabitlersek sabitleyelim, fonksiyon, sabitlenmeyen değişken üzerine R-lineer olur.

[4] Kanıtlayın. (1)

[5] Kanıtlayın. (2)

[6] Eğer R değişmeli bir halkaysa, $R^n \simeq R^m$ (R-modül olarak) ise $n = m$ olur. Değişmeli olmayan halkalar üzerine her zaman doğru olmayan bu önermeyi bir başka yazımızda kanıtlarız.

[7] Kanıtlayın. (3)

[8] Kanıtlayın. (4)

[9] Kanıtlayın. (5)

[10] Bulun. (6)

[11] Kanıtlayın. (7)

kümesinin $\binom{n+k-1}{k}$ tane elemanı vardır[12]. Demek ki (aynen yukarıdaki gibi) $\mathcal{S}_k M$ ile $R^{\binom{n+k-1}{k}}$ modülleri arasında bir R-modül izomorfisi vardır[13]. $\mathcal{S}_k M$ serbest modülünün bir tabanını bulmaya çalışabilirsiniz, ilginç ve eğitici olacaktır[14].

1.3 Alterne Formlar

Eğer $f \in \mathcal{L}_k M$ formu, $i \neq j$ için $m_i = m_j$ olduğunda $f(m_1, \ldots, m_k) = 0$ eşitliğini sağlıyorsa, o zaman f'ye ***alterne form*** denir. Bu durumda $i \neq j$ için

$$f(m_1, \ldots, m_i, \ldots, m_j, \ldots, m_k) = -f(m_1, \ldots, m_j, \ldots, m_i, \ldots, m_k)$$

olur[15]. Dolayısıyla her $\sigma \in \operatorname{Sym} k$ ve her $m_i \in M$ için

$$f(m_1, \ldots, m_k) = \operatorname{sg}(\sigma) f(m_{\sigma(1)}, \ldots, m_{\sigma(1)})$$

olur[16]. Alterne formlar kümesini $\mathcal{A}_k M$ olarak gösterelim. $\mathcal{A}_k M$ bir R-modüldür[17].

Önemli: Eğer $m_1, \ldots, m_n \in M$ elemanlarından biri diğerlerinin lineer kombinasyonuysa, o zaman her f alterne formu için $f(m_1, \ldots, f_n) = 0$ olur[18].

Eğer $M \simeq R^n$ ise ve $e_1, \ldots, e_n$ elemanları M'nin sıralı bir tabanıysa, o zaman her $f \in \mathcal{L}_k(M)$ formu, $1 \leq i_1 < \ldots < i_k \leq n$ doğal sayıları için, $f(e_{i_1}, \ldots, e_{i_k}) \in R$ değerleri tarafından belirlenir. Öte yandan,

$$\{(i_1, \ldots, i_k) : i_j \in \{1, 2, \ldots, n\} \text{ ve } i_1 < \ldots < i_k\}$$

---

[12] Kanıtlayın. (8)

[13] İzomorfiyi bulun. (9)

[14] Tabanı bulun. (10) Bu arada tabanın elemanlarının $\mathcal{S}_k M$ modülünün elemanları olması gerektiğini unutmayın!

[15] Eğer R'de $2 = 0$ ise bu eşitlik bize pek yeni bir şey vermez, bir önceki altbölümdeki simetrik formları elde ederiz. Öte yandan eğer $2 \in R$ bir sıfırbölen değilse, bu eşitlikler alterne formun tanımına denktir. Kanıtlayın. (11)

[16] $\operatorname{sg}(\sigma)$, σ permütasyonunun "imzası"dır, yani σ tek sayıda makasın çarpımıysa $\operatorname{sg}(\sigma) = -1$, çift sayıda makasın çarpımıysa $\operatorname{sg}(\sigma) = 1$ olarak tanımlanır. Bunun anlamlı bir tanım olduğu hiç de bariz değildir. Güzel bir kanıtını Lang'da bulabilirsiniz. Bir başka yazımızda kanıtlarız. Kanıt fikri: $\operatorname{Sym} k$ grubunu $\mathbb{Z}[X_1, \ldots, X_k]$ polinom halkası üzerine ($X_1, \ldots, X_n$ değişkenlerini σ'ya göre değiştirerek) etkiyin. Şimdi $f = \Pi_{i<j}(X_i - X_j)$ ise, her τ makası için (yani $(i\ j)$ biçiminde bir permütasyon için) $\tau f = -f$ olur. Buradan $\sigma f = \operatorname{sg}(\sigma) f$ çıkar. Bu kanıtın ayrıntılarını yazın (12). $\operatorname{sg}(\alpha\beta) = \operatorname{sg}(\alpha)\operatorname{sg}(\beta)$ olur tabii. Metindeki eşitliği kanıtlayın. (13)

[17] Kanıtlayın. (14)

[18] Neden? (15)

kümesinin $\binom{n}{k}$ tane elemanı vardır[19]. Demek ki (aynen yukarıdaki gibi) $\mathcal{A}_k M$ ile $R^{\binom{n}{k}}$ modülleri arasında bir R-modül izomorfisi vardır[20]. $\mathcal{S}_k M$ serbest modülünün bir tabanını bulun[21]. Demek ki $k > n$ ise $\mathcal{A}_k M = 0$. Ama bizi en çok

$$\dim_R \mathcal{A}_n M = 1$$

eşitliği ilgilendiriyor: $\mathcal{A}_n M \simeq R$. Bu son ifadeyi daha ayrıntılı bir biçimde açıklayalım, bir sonraki bölümde ölümcül bir öneme sahip olacak.

$\mathcal{A}_n M$ kümesinin (aslında R-modülünün) her f elemanının $f(e_1, \ldots, e_n)$ tarafından belirlendiğini gördük. Yani

$$f \mapsto f(e_1, \ldots, e_n)$$

kuralı bize $\mathcal{A}_n M$ modülünden R-modülüne giden birebir bir fonksiyon (aslında bir R-modül homomorfisi) verir[22]. Ama bu homomorfi ayrıca örtendir de, nitekim her $a \in R$ için $f(e_1, \ldots, e_n) = a$ eşitliğini veren bir $f \in \mathcal{A}_n M$ mültilineer formu vardır[23]. Bir başka deyişle bu fonksiyon bir R-modül izomorfisidir. Bunun özel bir durumu olarak $f(e_1, \ldots, e_n) =$ eşitliğini veren bir $f \in \mathcal{A}_n M$ mültilineer formu vardır. Bu forma bir sonraki bölümde $\det_e$ adını vereceğiz. Elbette

$$\mathcal{A}_n M = R \det_e$$

olur.

2 Determinant

2.1 Tanım

Bundan böyle bir $0 \neq n \in \mathbb{N}$ için $M \simeq R^n$ olacak. M'nin sıralı bir tabanını seçelim, diyelim $e_1, \ldots, e_n$. Bu tabana e adını verelim. $(e_1, \ldots, e_n)$ elemanında 1 değerini alan bir ve bir tane $\det_e \in \mathcal{A}_n M$ var.

$$\mathcal{A}_n M = R \det_e$$

olur[24].

[19] Kanıtlayın. (16)

[20] İzomorfiyi bulun. (17)

[21] Tabanı bulun (18). Bu arada tabanın elemanlarının $\mathcal{A}_k(M)$ modülünün elemanları olması gerektiğini unutmayın!

[22] Bu homomorfi seçilen tabana göre değişir, yani hiçbir şekilde ilahi (canonical) değildir.

[23] Niye? (19)

[24] Kanıtlayın. (20)

Şimdi bir $\varphi \in \operatorname{End}_R M$ için,

$$\det_e \varphi = \det_e(\varphi e_1, \ldots, \varphi e_n)$$

tanımını yapalım. Şimdilik $\det_e \varphi$ tanımı taban seçimine bağımlıymış gibi görünüyorsa da yakında tabandan bağımsız olduğunu kanıtlayacağız.

$$\det_e \mathrm{Id} = 1$$

eşitliğine dikkatinizi çekerim ve eğer $a \in R$ ise ve her $m \in M$ için $\mu_a(m) = am$ olarak tanımlanmışsa,

$$\det_e \mu_a = a^n$$

olur[25].

2.2 Birinci Önemli Fikir

Şimdi,

$$(A) \qquad (m_1, \ldots, m_m) \mapsto \det_e(\varphi m_1, \ldots, \varphi m_n)$$

kuralıyla tanımlanmış $M^n \longrightarrow R$ fonksiyonuna bakalım[26]. Bu fonksiyon $\mathcal{A}_n(M) = R \det_e$ kümesinde olduğundan, bir $a \in R$ için,

$$\det_e(\varphi m_1, \ldots, \varphi m_n) = a \det_e(m_1, \ldots, m_n)$$

buluruz. Bu eşitlikte $m_i = e_i$ alırsak,

$$a = \det_e(\varphi e_1, \ldots, \varphi e_n) = \det_e \varphi$$

buluruz. Demek ki,

$$(1) \qquad \det_e(\varphi m_1, \ldots, \varphi m_n) = \det_e \varphi \det_e(m_1, \ldots, m_n)$$

olur. $\alpha, \beta \in \operatorname{End}_R M$ için, (1) eşitliğini $\alpha \circ \beta$ andomorfisine uygulayalım:

$$(2) \qquad \det_e((\alpha \circ \beta) m_1, \ldots, (\alpha \circ \beta) m_n) = \det_e(\alpha \circ \beta) \det_e(m_1, \ldots, m_n)$$

çıkar. Ama yine (1)'den dolayı,

$$\begin{aligned} \det_e((\alpha \circ \beta) m_1, \ldots, (\alpha \circ \beta) m_n) &= \det_e \alpha \det_e(\beta m_1, \ldots, \beta m_n) \\ &= \det_e \alpha \det_e \beta \det_e(m_1, \ldots, m_n) \end{aligned}$$

olur. Eğer $m_1 = e_1, \ldots, m_n = e_n$ alırsak, (2)'den ve yukarıdaki eşitlikten şu teorem çıkar:

---

[25] Bu eşitlikleri kanıtlayın. (21)

[26] Bu yazıda iki önemli fikir vardır (geri kalan her şey standart ve faso fiso). Birincisi bu tanımdır.

Teorem 1. *$\alpha, \beta \in \operatorname{End}_R M$ için* $\det_e(\alpha \circ \beta) = \det_e \alpha \det_e \beta$. □

Sonuç 2. *Eğer $\alpha \in \operatorname{GL}_R M$ ise,* $\det_e \alpha \in R^\star$ *ve* $\det_e(\alpha^{-1}) = (\det_e \alpha)^{-1}$ *olur*[27]. □

Sonuç 3. *Eğer R bir cisimse ve* $\det_e \varphi \in R^\star$ *ise* $\phi \in GL(M)$ *olur*[28].

Kanıt. Varsayıma göre $\det_e(\varphi e_1, \ldots, \varphi e_n) \neq 0$. Ama$R$ bir cisim olduğundan (yoksa doğru değil!), bundan $\varphi e_1, \ldots, \varphi e_n$ elemanlarının lineer bağımsız olduğu çıkar. Demek ki φ örten. Buradan da $\varphi \in \operatorname{GL} M$ çıkar. □

Sonuç 4. *Her $\alpha \in \operatorname{GL}_R M$ ve $\beta \in \operatorname{End}_R M$ için* $\det_e(\alpha^{-1} \circ \beta \circ \alpha) = \det_e \beta$ *olur*[29]. □

Artık R'nin $\det_e \alpha$ elemanının e tabanından bağımsız olduğunu kanıtlayabiliriz[30]. Bu amaçla bir de ayrıca bir $f_1, \ldots, f_n$ tabanı alalım; bu tabana f adını verelim. $\det_f \in \mathcal{A}_n M$ formunu aynen $\det_e$ gibi tanımlıyoruz, sadece e yerine f tabanını alıyoruz: $\det_f \in \mathcal{A}_n M$ alterne formu, $f_1, \ldots f_n$ tabanında 1 değerini alan yegâne alterne formdur.

Rastgele bir $\alpha \in \operatorname{End}_R M$ alalım. Sonra $\beta \in GL_R M$ otomorfisini her i için $\beta f_i = e_i$ olacak biçimde tanımlayalım ve ardından

$$(m_1, \ldots, m_n) \mapsto \det_e(\beta m_1, \ldots, \beta m_n)$$

kuralıyla tanımlanmış $M^n \longrightarrow R$ fonksiyonuna bakalım. Bu elbette alterne bir formdur[31]. Eğer

$$\tilde{\beta}(m_1, \ldots, m_n) = (\beta m_1, \ldots, \beta m_n)$$

tnımını yaparsak, bu alterne formu $\det_e \circ \tilde{\beta}$ olarak daha kolay bir biçimde yazabiliriz. Ama $\det_e \circ \tilde{\beta}(f_1, \ldots, f_n) = 1$ olduğundan[32],

$$\det_e \circ \tilde{\beta} = \det_f$$

olmalı[33]. İş basit bir hesaba kaldı:

$$\begin{aligned}
\det_f \alpha &= \det_f(\alpha f_1, \ldots, \alpha f_n) \\
&= \det_e \circ \tilde{\beta}(\alpha f_1, \ldots, \alpha f_n) \\
&= \det_e((\beta \circ \alpha) f_1, \ldots, (\beta \circ \alpha) f_n) \\
&= \det_e((\beta \circ \alpha \circ \beta^{-1}) e_1, \ldots, (\beta \circ \alpha) \circ \beta^{-1}) e_n) \\
&= \det_e(\beta \circ \alpha \circ \beta^{-1}) = \det_e \beta.
\end{aligned}$$

[27] Kanıtlayın. (22)

[28] Bir sonraki altbölümde bu teoremi halkalara genelleştireceğiz.

[29] Kanıtlayın. (23)

[30] Ama dikkat, farklı e ve f tabanları için, $\mathcal{A}_n M$ modülünde $\det_e \neq \det_f$ olabilir. Ama $\det_e$ ve $\det_f$'yi $\operatorname{End}_R M$ kümesinden R'ye giden bir fonksiyon olarak görürsek, o zaman bu fonksiyonlar eşit olur; kanıtı birazdan.

[31] Kanıtlayın. (24)

[32] Neden? (25)

[33] Neden? (26)

İstediğimiz kanıtlanmıştır:

Teorem 5. *Her $\alpha \in \operatorname{End}_R M$ için, $\det_e \alpha \in R$ elemanı e tabanından bağımsızdır.* $\square$

Bundan böyle $\det_e \alpha$ yerine, sadece $\det \alpha$ yazacağız; hatta det'i $\operatorname{End}_R M$'den R'ye giden bir fonksiyon olarak görüp $\det_e$ yerine det yazacağız[34].

2.3 İkinci Önemli Fikir

Verilmiş bir $\varphi \in \operatorname{End}_R M$ ve $m \in M$ için,

$$(B) \qquad \varphi^\star m = \det_e(m, \varphi e_2, \ldots, \varphi e_n)e_1 + \cdots + \det_e(\varphi e_1, \ldots, \varphi e_{n-1}, m)e_n$$

tanımını yapalım[35]. Böylece bir

$$\varphi^\star : M \longrightarrow M$$

fonksiyonu elde ederiz. Elbette $\varphi^\star \in \operatorname{End}_R M$ olur[36]. Şimdi $\varphi^\star \circ \varphi$ homomorfisine bakalım. Kolayca görüleceği üzere her $i = 1, \ldots, n$ için,

$$(\varphi^\star \circ \varphi)e_i = (\det \varphi)\, e_i$$

olur[37], yani

$$\varphi^\star \circ \varphi = (\det \varphi) \operatorname{Id}_M \tag{3}$$

olur[38].

Önsav 6. $\det \varphi^\star \det \varphi = (\det \varphi)^n$ *olur. Eğer* $\det \varphi$ *bir sıfırbölen değilse*[39], $\det \varphi^\star = (\det \varphi)^{n-1}$ *olur*[40]. $\square$

Sonuç 2'nin ters istikametini de artık kanıtlayabiliriz:

---

[34] Burada dikkat edilmesi gereken bir ayrıntı var. M'nin birbirinden farklı e ve f tabanları için $\det_e(m_1, \ldots, m_n)$ ve $\det_f(m_1, \ldots, m_n)$ birbirinden farklı elemanlar olabilir, ama her $\varphi \in \operatorname{End}_R M$ için $\det_e \varphi = \det_f \varphi$ olur. Birincisinde $\det_e$'yi $\mathcal{A}_n M$'nin bir elemanı olarak görüyoruz, ikincisinde ise $\operatorname{End}_R M$'den R'ye giden bir fonksiyon olarak.

[35] Yazının ikinci önemli fikri. Başka da önemli fikir olmayacak.

[36] Kanıtlayın. (27)

[37] Gösterin. (28)

[38] Niye? (29)

[39] Değişmeli bir halkada bir $x \neq 0$ elemanı için $ax = 0$ oluyorsa, a'ya ***sıfırbölen*** denir. Eğer a sıfırbölen değilse, $ax = ay$ ise $x = y$ olur. Kanıtlayın. (30)

[40] Teoremin her iki cümlesini de kanıtlayın. (31)

Teorem 7. *$\varphi \in \operatorname{End}_R M$ ise*

$$\varphi \in \operatorname{GL} M \iff \det\varphi \in R^\star$$

olur. Ve bu durumda

$$\varphi^{-1} = (\det\varphi)^{-1}\varphi^\star$$

olur.

Kanıt. Soldan sağa Sonuç 2'de kanıtlanmıştı. Şimdi $\det\phi \in R^\star$ varsayımını yapalım. (3)'ten dolayı, $(\det\varphi)^{-1}\varphi^\star$ andomorfisi φ'nin soldan tersidir; ve tabii ki φ andomorfisi de $(\det\varphi)^{-1}\varphi^\star$ andomorfisinin sağdan tersidir. Demek ki $\det\varphi \in R^\star$ ise φ'nin soldan tersi vardır.

Öte yandan Önsav 6'e göre $\det\varphi^\star \in R^\star$ olur. Demek ki $\det((\det\varphi)^{-1}\varphi^\star) \in R^\star$. Bir önceki paragraftan $(\det\varphi)^{-1}\varphi^\star$ andomorfisinin soldan tersi olduğu anlaşılır. Demek ki $(\det\varphi)^{-1}\varphi^\star$ andomorfisinin hem soldan hem de sağdan tersi vardır. Sağdaki tersi φ olduğundan (ve sağ ve sol tersler birleşme özelliğini sağlayan her yapıda eşit olduğundan), φ andomorfisi $(\det\varphi)^{-1}\varphi^\star$ andomorfisinin tersidir; dolayısıyla $(\det\varphi)^{-1}\varphi^\star$ andomorfisi de φ andomorfisinin tersidir[41]. □

Teorem 8. *$\varphi \in \operatorname{End}_R M$ ise*

$$\varphi \textit{ birebir} \iff \det\varphi \textit{ sıfırbölen değilse}$$

önermesi doğrudur.

Kanıt. Eğer $\det\varphi$ sıfırbölen değilse, $(\det\varphi)\operatorname{Id}_M$ birebirdir. Ama $\varphi^\star \circ \varphi = (\det\varphi)\operatorname{Id}_M$ olduğundan φ de birebirdir[42].

Şimdi $\det\varphi$'nin sıfırbölen olmadığını varsayalım. Bir $m \in M^\sharp$ için $\varphi m = 0$ olsun. Demek ki $\varphi^\star(\varphi m) = 0$ olur. (B)'den,

$$\det_e(\varphi m, \varphi e_2, \ldots, \varphi e_n)e_1 + \cdots + \det_e(\varphi e_1, \ldots, \varphi e_{n-1}, \varphi m)e_n = 0,$$

çıkar. e_i'ler bir taban oluştuğundan,

$$\begin{gathered}\det_e(\varphi m, \varphi e_2, \ldots, \varphi e_n) = 0\\ \vdots \\ \det_e(\varphi e_1, \ldots, \varphi e_{n-1}, \varphi m) = 0\end{gathered}$$

[41] Ayrıntıları (eğer kalmışsa!) tamamlayın. (32)

[42] Ayrıntıları tamamlayın. (33)

çıkar, yani (1)'den dolayı

$$\begin{gathered}\det\varphi \det_e(m, e_2, \ldots, e_n) = 0 \\ \vdots \\ \det\varphi \det_e(e_1, \ldots, e_{n-1}, m) = 0\end{gathered}$$

çıkar. Ama $\det\varphi$'nin sıfırbölen olmadığını varsaymıştık. Demek ki

$$\begin{gathered}\det_e(m, e_2, \ldots, e_n) = 0 \\ \vdots \\ \det_e(e_1, \ldots, e_{n-1}, m) = 0\end{gathered}$$

olur. Ama $e_1, \ldots, e_n$ bir taban olduğundan buradan $m = 0$ çıkar[43]. □

[43]Neden? (34)