TÜİB Üzerine Modüller

Değişmeli, sıfır böleni olmayan ($rs = 0$ ise ya r ya da $s = 0$) ve her ideali tek bir eleman tarafından üretilen halkalara kısaca ***TÜİB*** (tek üreteçli ideal bölgesi) denildiğini anımsatalım. (İngizilicesi *PID*) Bu yazıdaki tüm modüller, aksi söylenmedikçe, TÜİB olan bir R halkası üzerine sol R-modüllerdir.

Bu yazıda kanıtlayacağımız ana teorem şu:

Teorem 1. *M, sonlu sayıda eleman tarafından gerilmiş bir R-modül olsun. O zaman, M, tek eleman tarafından üretilmiş sonlu sayıda altmodülün Kartezyen çarpımıdır.*

Tek eleman tarafından üretilmiş modüller bir $a \in R$ için R/aR'ye izomorf olduklarından (neden?), yukardaki teoremden, sonlu sayıda eleman tarafından üretilmiş bir modülün,

$$R/a_1R \times R/a_2R \times ... \times R/a_nR$$

sol R-modülüne izomorf olduğu çıkar.

Bu teoremi kanıtlamak için herbiri diğerinden önemli ve yararlı birçok sonuç kanıtlayacağız. Sadece sonuçlar değil, sonuçlara giden kanıt yöntemleri de önemlidir. Ayrıca sonuçlarımızın kimi zaman gerekenden daha genel olacağını söyleyelim.

Teorem 2. *F, R üzerine n boyutlu özgür bir modül olsun. $M \leq F$ olsun. O zaman M de özgürdür ve boyutu en fazla n'dir.*

Kanıt: F modülü, $x_1, x_2, ..., x_n$ elemanları tarafından özgürce gerilmiş olsun. Her $j = 0, 1, ..., n$ için

$$F_j = \langle x_1, x_2, ..., x_j \rangle$$

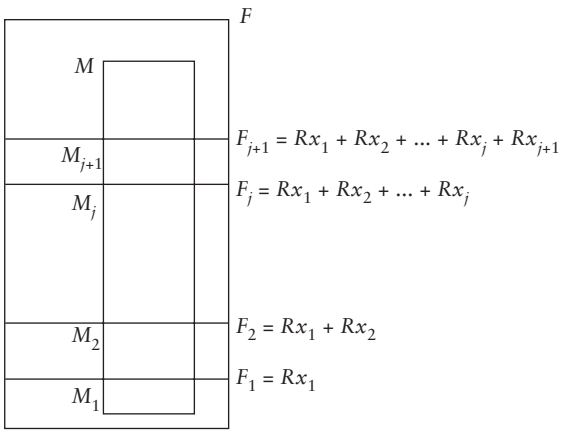
ve

$$M_j = M \cap F_j$$

tanımlarını yapalım. $F_0 = 0$ ve $F_n = F$ eşitliklerine dikkatinizi çekeriz. Her F_j, boyutu j olan özgür bir altmodüldür ve her M_j bir altmodüldür.

$M_n = M$ olduğundan, her M_j'nin boyutu en fazla j olan özgür bir modül olduğunu kanıtlamak yeterli. Bunu j üzerine tümevarımla yapacağız.

Eğer $j = 0$ ise, $M_0 = 0$ olduğundan, bu durumda sorun yok. Tümevarıma başlayabiliriz; ama kanıtı $j = 1$ durumunda da vermek aydınlatıcı olacaktır. Bunun iki değişik kanıtını sunacağız. (Bizim favorimiz ikinci kanıttır.)



$j = 1$ için birinci kanıt: Eğer $F_1 = 0$ ise kanıtlayacak fazla bir şey yok. Bundan böyle $F_1 \neq 0$ varsayımını yapalım.

$$M_1 = M \cap F_1 = M \cap Rx_1$$

olduğundan M_1'in elemanları bazı $r \in R$ elemanları için rx_1 biçiminde yazılır. Bu r elemanlarının kümesine bakalım:

$$I = \{r \in R : rx_1 \in M_1\}$$

olsun. Demek ki

$$M_1 = Ix_1.$$

Öte yandan I'nın bir ideal olduğu belli. R bir TÜİB olduğundan, bir $a \in R$ için $I = Ra$. Dolayısıyla,

$$M_1 = Ix_1 = Rax_1.$$

Yani ax_1 elemanı M_1 modünü geriyor; ama bakalım özgürce mi geriyor: Eğer $r, s \in R$ için $r(ax_1) = s(ax_1)$ ise, $(ra)x_1 = (sa)x_1$ olur. Ama x_1, F'nin bir tabanının bir elemanı olduğu için, buradan $ra = sa$ elde ederiz. R'de sıfırbölen olmadığından, bundan da $r = s$ çıkar. Birinci kanıt tamamlanmıştır.

$j = 1$ için ikinci kanıt: F_1, bir eleman tarafından gerilmiş özgür modül olduğundan, $F_1 \approx R$ olur. (Sözkonusu olan modül izomorfizmasıdır elbet, başka bir izomorfizma olamaz.) Dolayısıyla R'nin altmodüllerinin boyutu en fazla 1 olan özgür modül olduklarını kanıtlamalı. Ama R'nin R altmodüllerinin R'nin idealleridir ve R'nin idealleri de bir $a \in R$ için aR biçimindedir. Eğer $a \neq 0$ ise,

$$r \mapsto ar$$

kuralıyla tanımlanan $f : R \to aR$ fonksiyonu bir R-modül izomorfizması olduğundan, $aR \approx R$ ve kanıt tanımlanmıştır.

Tümevarım Adımı: Şimdi M_j'nin boyutu en fazla j olan özgür bir modül olduğunu varsayıp M_{j+1}'in boyutu en fazla j olan özgür bir modül olduğunu kanıtlayalım.

Eğer $M_{j+1} = M_j$ ise, işimiz bitmiştir. Bundan böyle $M_j < M_{j+1}$ eşitsizliğini varsayalım.

$M_{j+1} \leq F_{j+1}$ olduğundan, M_{j+1}'nin her elemanı, $m \in F_j$ ve $r \in R$ için

$$m + rx_{j+1}$$

biçiminde yazılır. x_{j+1}'in katsayılarının kümesine bakalım:

$$I = \{r \in R : \text{Bir } m \in F_j \text{ için } m + rx_{j+1} \in M_{j+1}\}$$

olsun. I'nın bir ideal olduğunu görmek kolay. Demek ki bir $a \in R$ için $I = Ra$. Bu arada, $M_j < M_{j+1}$ eşitsizliğinden dolayı a'nın 0 olamayacağını görelim, ilerde gerekecek. Madem ki $a \in I$, öyle bir $m_0 \in F_j$ vardır ki,

$$m_0 + ax_{j+1} \in M_{j+1}$$

olur. Şimdi M_{j+1}'den rastgele bir m elemanı alalım. $m_1 \in F_j$ ve $r \in R$ için,

$$m = m_1 + rx_{j+1}$$

biçiminde yazalım. Tanıma göre, $r \in I = Ra$, demek ki bir $s \in R$ için $r = sa$. Şimdi şu hesabı yapalım:

$$\begin{aligned} m - s(m_0 + ax_{j+1}) &= (m_1 + rx_{j+1}) - s(m_0 + ax_{j+1}) \\ &= (m_1 + sax_{j+1}) - s(m_0 + ax_{j+1}) \\ &= m_1 - sm_0. \end{aligned}$$

Demek ki M_{j+1}'in $m - s(m_0 + ax_{j+1})$ elemanı F_j'nin $m_1 - sm_0$ elemanına eşit, yani

$$m - s(m_0 + ax_{j+1}) \in M_{j+1} \cap F_j = M_j.$$

Bundan da

$$m \in M_j + R(m_0 + ax_{j+1})$$

çıkar. Demek ki

$$M_{j+1} \leq M_j + R(m_0 + ax_{j+1}).$$

Diğer içindelik bariz olduğundan,

$$M_{j+1} = M_j + R(m_0 + ax_{j+1})$$

buluruz. Şimdi toplamın direkt olduğunu gösterelim:

$$m \in M_j \cap R(m_0 + ax_{j+1})$$

olsun. O zaman bir $r \in R$ için,

$$m = r(m_0 + ax_{j+1})$$

olur, yani

$$rax_{j+1} = m - rm_0 \in F_j$$

olur. Ama $x_1, x_2, ..., x_j, x_{j+1}$ elemanları lineer bağımsız olduklarından, bundan $ra = 0$ çıkar. $a \neq 0$ olduğundan, $r = 0$ ve $m = r(m_0 + ax_{j+1}) = 0$ elde ederiz. Böylece

$$M_{j+1} = M_j \oplus R(m_0 + ax_{j+1})$$

eşitliğini kanıtlamış olduk. Tümevarım varsayımına göre M_j, boyutu en fazla j olan özgür bir modül olduğundan, geriye $R(m_0 + ax_{j+1})$ modülünün 1 boyutlu özgür modül olduğunu kanıtlamak kaldı. Bu da oldukça kolay:

$$r \mapsto r(m_0 + ax_{j+1})$$

kuralıyla tanımlanmış

$$R \to R(m_0 + ax_{j+1})$$

modül homomorfizması elbette örtendir, ama aynı zamanda birebirdir de: $r(m_0 + ax_{j+1}) = 0$ ise,

$$rax_{j+1} = -rm_0 \in Rx_{j+1} \cap F_j = 0$$

olur ve x_{j+1} elemanı bir tabanın parçası olduğundan bundan $ra = 0$ çıkar. $a \neq 0$ olduğundan, bundan da $r = 0$ çıkar. □

Teorem 2, sonsuz boyutlu özgür modüller için de geçerlidir. Ama bu sefer, Zorn Önsavı'nı kullanıp tabanı bir ordinalle iyisıralayıp ordinaller üzerine tümevarım yapmak ve ayrıca Zorn Önsavı'nı (ikinci bir kez) akıllıca kullanmak gerekir. Eğer α bir ordinalse, $M_{\alpha+1}$ için kanıt aynen yukardaki gibidir ama λ bir limit ordinalse,

$$M_\lambda = \bigcup_{\alpha<\lambda} M_\alpha$$

olarak tanımlanan M_λ altmodülü için isteneni kanıtlayamayız çünkü M_α'lar özgür olsalar da M_λ özgür olmayabilir. Örnek: $R = \mathbb{Z}$, $\lambda = \omega = \mathbb{N}$, $M_n = (1/n!)\mathbb{Z}$ ve $M_\lambda = \bigcup_{n<\omega} M_n = \mathbb{Q}$ olur ve M_n'ler özgür olmalarına karşın bileşimleri olan $\mathbb{Q}$ özgür bir $\mathbb{Z}$-modül değildir. (Neden?) Zorn Önsavı'nı biraz daha usturuplu bir biçimde kullanmak gerekir. Bunun kanıtını bir başka yazıda göstereriz. Bu yazıdanın Teorem 9'unda benzer bir yöntem kullanılıyor.

Sonuç 3. *$\mathbb{Z}^n$'nin her altgrubu, bir $i \leq n$ için $\mathbb{Z}^i$'ye eşyapısaldır.*

Sonuç 4. *n tane eleman tarafından gerilmiş bir R-modülün her altmodülü en fazla n tane elemanla gerilmiştir.*

Kanıt: M, n tane eleman tarafından gerilmiş bir modül ve $N \leq M$ bir altmodül olsun. Bu elemanlara $x_1, x_2, ..., x_n$ diyelim.

$$F = R^n = R \times R \times ... \times R$$

olsun ve

$$\varphi(r_1, r_2, ..., r_n) = r_1x_1 + r_2x_2 + ... + r_nx_n$$

kuralıyla tanımlanan

$$\varphi : F \to M$$

modül homomorfizmasını ele alalım. Bu, örten bir

homomorfizmadır. Teorem 1'e göre $\varphi^{-1}(M)$, boyutu en fazla n olan özgür bir modüldür. Eğer, $y_1, y_2, ..., y_m$ elemanları $\varphi^{-1}(M)$'yi geriyorlarsa, o zaman, $\varphi(y_1), \varphi(y_2),, ..., \varphi(y_m)$ elemanları M'yi gerer. □

Eğer bir ${}_RM$ sol modülde her $r \in R \setminus \{0\}$ ve her $m \in M \setminus \{0\}$ için $rm \neq 0$ oluyorsa, o zaman M'ye ***burulmasız halka*** denir. (İngilizcesi *torsion-free*)

Teorem 5. *Sonlu sayıda* (*diyelim n tane*) *eleman tarafından gerilmiş ve burulmasız olan bir modül özgürdür ve en fazla n tane eleman tarafından gerilmiştir.*

Kanıt: Modüle M diyelim. M'nin $x_1, x_2, ..., x_n$ elemanları tarafından gerildiğini varsayalım.

Birinci Kanıt: n üzerine tümevarım yapacağız. Eğer $n = 0$ ya da 1 ise kanıtlayacak fazla bir şey yok. Şimdi teoremin n'den az üreteçli modüller için doğru olduğunu varsayalım.

$$N = \langle x_1, x_2, ..., x_{n-1} \rangle$$

olsun. Tümevarım varsayımından dolayı N özgür bir modüldür ve boyutu en fazla $n - 1$'dir. Ve elbette $M = N + Rx_n$ eşitliği geçerlidir.

$$I = \{r \in R : rx_n \in N\}$$

olsun. I'nin bir ideal olduğu bariz. Eğer $I = 0$ ise o zaman, $M = N \oplus Rx_n$ eşitliği geçerlidir ve bu durumda istenen kanıtlanmıştır. Bundan böyle I'nin 0 olmadığını varsayalım. $I = aR$ olsun. Elbette $a \neq 0$. Şimdi

$$\varphi(x) = ax$$

kuralıyla tanımlanmış,

$$\varphi : M \to M$$

homomorfisine bakalım. $a \neq 0$ ve M burulmasız olduğundan, φ birebirdir. Demek ki,

$$M \approx \varphi(M).$$

Öte yandan, a'nın ve I'nın tanımlarından dolayı,

$$\varphi(M) = aM = a(N + Rx_n) = aN + Rax_n \leq N.$$

Yani $\varphi(M)$, N'nin bir altmodülü. Ama N özgür. Demek ki Teorem 2'ye göre $\varphi(M)$ de özgür. Dolayısıyla M de özgürdür.

İkinci Kanıt: $y_1, ..., y_m$ elemanları, $x_1, x_2, ..., x_n$ arasından seçilmiş lineer bağımsız maksimal sayıda eleman olsun. (Ya da $y_1, ..., y_m$ elemanları M'nin maksimal sayıda lineer bağımsız elemanları olsun; kanıtta bir değişiklik olmaz.) Demek ki

$$\langle y_1, ..., y_m \rangle$$

özgür bir modüldür. $\{y_1, ..., y_m\}$ kümesinin maksimalliğinden dolayı, her $i = 1, ..., n$ için,

$$x_i, y_1, ..., y_m$$

elemanları arasında bariz olmayan lineer bir bağımlılık vardır, yani öyle bir $r_i \in R \setminus \{0\}$ vardır ki,

$$r_i x_i \in \langle y_1, ..., y_m \rangle$$

olur. $r = r_1 r_2 ... r_n \neq 0$ olsun. O zaman her $i = 1, ..., n$ için,

$$rx_i \in \langle y_1, ..., y_m \rangle$$

olur, yani

$$rM \leq \langle y_1, ..., y_m \rangle$$

olur. Şimdi,

$$\varphi(x) = rx$$

kuralıyla tanımlanmış,

$$\varphi : M \to \langle y_1, ..., y_m \rangle$$

homomorfizmasına bakalım. M burulmasız olduğundan, φ birebirdir. Demek ki,

$$M \approx \varphi(M) \leq \langle y_1, ..., y_m \rangle$$

ve $\varphi(M)$, dolayısıyla M de, Teorem 2'ye göre özgür bir halkadır. □

Eğer $m \in M$ elemanı, bir $r \in R \setminus \{0\}$ için $rm = 0$ eşitliğini sağlıyorsa, m'ye ***burulmalı eleman*** denir. M'nin 0 elemanı elbette burulmalı bir elemandır. Eğer M özgür bir halkaysa (örneğin bir vektör uzayıysa), M'nin sadece 0 elemanı burulmalıdır. Eğer R bir bölüm halkasıysa, burulmalı elemanlar kümesi bir altmodül olur. Bunun basit kanıtı okura bırakılmıştır. (Eğer R bir bölüm halkası değilse, bu yanlıştır. Örneğin $\mathbb{Z}/6\mathbb{Z}$'yi bir $\mathbb{Z}/6\mathbb{Z}$-modül olarak görürsek, 2 ve 3 burulmalı elemanlardır ama toplamı olan 5, yani –1, burulmalı bir eleman değildir.)

Şimdi Teorem 1'in kanıtında önemli bir adım atacağız:

Teorem 6. *M sonlu sayıda* (*diyelim n tane*) *eleman tarafından gerilen bir modül olsun. T, M'nin burulmalı elemanlarından oluşan altmodül olsun. O zaman boyutu n'den küçükeşit olan özgür bir F altmodülü için, M = T ⊕ F olur.* (*Yani T, M'de ayrışır ve tümleyeni özgürdür.*) *Ayrıca* (*Sonuç* 4'*e göre*) *T de sonlu eleman tarafından gerilir.*

Kanıt: M/T burulmasızdır ve sonlu eleman tarafından gerilmiştir ve geren eleman sayısı en fazla m'dir. (Bunun kolay kanıtı okura bırakılmıştır.) Demek ki bir önceki teoreme göre M/T özgür bir halkadır. $\bar{x}_1, \bar{x}_2, ..., \bar{x}_k$ elemanları M/T'yi özgürce gersinler. $k \leq n$ olmalı elbette. $F = \langle x_1, x_2, ..., x_k \rangle$ olsun. $x_1, x_2, ..., x_k$ elemanları arasındaki herhangi bir lineer bağımlılık, izdüşümle anında $\bar{x}_1, \bar{x}_2, ..., \bar{x}_k$ elemanlarına sirayet ettiğinden, $x_1, x_2, ..., x_k$

elemanları lineer bağımsızdır; dolayısıyla F özgür bir halkadır.

$M = T + F$ eşitliği oldukça kolay. $m \in M$ ise, M/T'nin $\bar{m}$ elemanı, $r_1, r_2, ..., r_k \in R$ için,

$$\bar{m} = r_1\bar{x}_1 + r_2\bar{x}_2 + ... + r_k\bar{x}_k$$

olarak yazılır; dolayısıyla,

$$m - (r_1x_1 + r_2x_2 + ... + r_kx_k) \in T$$

olur. Bu da $m \in F + T$ demektir.

Şimdi $T \cap F = 0$ eşitliğini kanıtlayalım: Eğer F'nin

$$r_1x_1 + r_2x_2 + ... + r_kx_k$$

elemanı T'deyse, o zaman bir $a \in R \setminus \{0\}$ için

$$a(r_1x_1 + r_2x_2 + ... + r_kx_k) = 0$$

olur, yani

$$ar_1x_1 + ar_2x_2 + ... + ar_kx_k = 0$$

olur. Ama x_i'ler lineer bağımsız olduklarından, bundan, her i için, $ar_i = 0$ çıkar, yani $r_i = 0$, demek ki $r_1x_1 + r_2x_2 + ... + r_kx_k = 0$. □

Yukardaki kanıt aslında şu daha genel teoremin kanıtıdır:

Teorem 7. $\varphi : M \to N$ *bir modül homomorfisi olsun. N özgür bir modül olsun. O zaman M'nin öyle bir F özgür modülü vardır ki* $\varphi_{|F}$, *F ile N arasında bir izomorfidir ve* $M = F \oplus \text{Ker } \varphi$ *olur.*

Kanıt: Aynen yukardaki teorem gibi... Artık kolay olması gereken kanıtı okura bırakıyoruz. □

Teorem 6, Teorem 7'den şöyle çıkar: $N = M/T$ ve $\varphi : M \to M/T = N$ doğal izdüşüm olsun. O zaman $\text{Ker } \varphi = T$ ve hemen Teorem 6'yı elde ederiz.

Demek ki, Teorem 6'ya göre burulmalı (ve sonlu eleman tarafından gerilen) modülleri sınıflandırdık mı Teorem 1'i de kanıtlamış oluruz. Önce bir tanım. M bir modül ve $p \in R$ bir asal olsun.

$$M_p = \{m \in M : \text{bir } n \in \mathbb{N} \text{ için } p^nm = 0\}$$

olsun. M_p'nin M'nin bir altmodül olduğunun kanıtı kolaydır. Eğer p ve q yandaş (İngilizcesi *associate*) asallarsa, $M_p = M_q$ olur. Bundan böyle, her asal yandaşlık sınıfı için bir p asalının seçildiğini varsayacağız.

Örneğin, $R = \mathbb{Z}$ ve $M = \mathbb{Z}/6\mathbb{Z}$ ise, $M_2 = 3M$, $M_3 = 2M$ ve ± 2 ve ± 3'ten değişik asallar için $M_p = 0$'dır.

M_p'ye M'nin ***p*-başat altmodülü*** diyelim. M_p gibi, her m elemanı için $p^nm = 0$ eşitliğini sağlayan bir n doğal sayısı olan modüllere ***p*-burulmalı modül*** diyelim.

Teorem 8. *Her M modülü için,*

$$\langle M_p : p \in R, p \text{ asal} \rangle = \bigoplus_{p \text{ asal}} M_p$$

olur. Eğer M burulmalıysa,

$$M = \bigoplus_{p \text{ asal}} M_p$$

olur.

Kanıt: Önce birinci önermeyi kanıtlayalım. Kanıtlamamız gereken şey şu: Eğer $p_1, p_2, .., p_n$ sonlu sayıda değişik (yani yandaş olmayan) asalsa ve her i için $m_i \in M_{p_i}$ ise ve $\Sigma_i m_i = 0$ ise o zaman her i için $m_i = 0$ olur. Kanıtlayalım. Diyelim, k_i doğal sayısı için, $p_i^{k_i}m_i = 0$. O zaman

$$m_1 = m_2 + ... + m_n$$

olduğundan, öyle $k_1, k_2, .., k_n$ doğal sayıları vardır ki, hem

$$p_1^{k_1}m_1 = 0$$

hem de

$$p_2^{k_2} ... p_n^{k_n}m_1 = 0$$

olur. Ama R'nin $p_1^{k_1}$ ve $p_2^{k_2} ... p_n^{k_n}$ elemanları birbirine asallar. Demek ki öyle u, v tamsayıları var ki,

$$up_1^{k_1} + vp_2^{k_2} ... p_n^{k_n} = 1$$

olur. O zaman da,

$$\begin{aligned} m_1 &= 1m_1 = (up_1^{k_1} + vp_2^{k_2} ... p_n^{k_n})m_1 \\ &= up_1^{k_1}m_1 + vp_2^{k_2} ... p_n^{k_n}m_1 = 0 + 0 = 0 \end{aligned}$$

olur.

Şimdi de ikinci önermeyi kanıtlayalım: $m \in M$ rastgele bir eleman olsun. $0 \neq a \in R$ elemanı $am = 0$ eşitliğini sağlasın. a'yı asallarına ayıralım:

$$a = up_1^{k_1} ... p_n^{k_n}.$$

Burada u in R^* ve p_i'ler biraz önce seçtiğimiz birbirinden değişik asallar. Her $i = 1, ..., n$ için,

$$b_i = a/p_i^{k_i}$$

olsun. O zaman

$$p_i^{k_i}b_im = am = 0$$

olur, yani $b_im \in M_{p_i}$. R'nin $b_1, ..., b_n$ elemanları aralarında asaldır, yani (tersinir elemanlar dışında) ortak bölenleri olamaz. Dolayısıyla $\langle b_1, ..., b_n \rangle = R$ ve R'nin

$$1 = r_1b_1 + ... + r_nb_n$$

eşitliğini sağlayan $r_1, ..., r_n$ elemanları vardır. Demek ki,

$$\begin{aligned} m = 1m &= (r_1b_1 + ... + r_nb_n)m \\ &= r_1b_1m + ... + r_nb_nm \end{aligned}$$

eşitliği geçerlidir ve bundan da

$$m \in M_{p_1} + ... + M_{p_n}$$

çıkar. Demek ki $M = \langle M_p : p \in R, p \text{ asal} \rangle$ ve birinci kısımdan dolayı teorem kanıtlanmıştır. □

Teorem 6 ve 8'e göre sonlu eleman tarafından gerilmiş p-burulmalı halkaları sınıflandırmalıyız;

bunların tek üreteçli modüllerin direkt toplamı olduğunu kanıtlamalıyız. Daha iyisini yapacağız.

Teorem 9. *M, p-burulmalı ama derecesi sonlu olan bir modül olsun; yani bir t doğal sayısı için* $p^tM = 0$ *olsun. O zaman* $I_1, I_2, .., I_t$ *göstergeç kümeleri için,*

$$M \approx \oplus_{i=1}^{t}\left(\oplus_{I_i} R/p^iR\right)$$

izomorfizması doğrudur.

Uzun sürecek olan kanıtı t üzerine tümevarımla yapacağız. Ama önce kendi başına önemi olan birkaç önsav kanıtlayalım.

Önsav 10. $p \in R$ *asal bir eleman ve* $t > 0$ *bir doğal sayı olsun. O zaman*

$$p(R/p^tR) = \{\overline{r} \in R/p^tR : p^{t-1}\overline{r} = \overline{0}\}$$

olur.

Kanıt: ($\subseteq$) Her $\overline{r} \in R/p^tR$ için $p^{t-1}(p\overline{r}) = p^t\overline{r}\ \ \overline{0}$ olduğu için çok bariz.

($\supseteq$) $\overline{r} \in R/p^tR$ elemanı $p^{t-1}\overline{r} = \overline{0}$ eşitliğini sağlasın. O zaman $p^{t-1}r \in p^tR$ olur, yani bir s in R için, $p^{t-1}r = p^ts$ olur. R bir bölge olduğundan, bundan, $r = ps$ çıkar, yani $\overline{r} = p\overline{s} \in p(R/p^tR)$. □

Sonuç 11. $p \in R$ *asal bir eleman ve* $t > 0$ *bir doğal sayı olsun. I bir göstergeç kümesi olsun. O zaman*

$$p(\oplus_I R/p^tR) = \{\overline{r} \in \oplus_I R/p^tR : p^{t-1}\overline{r} = \overline{0}\}$$

olur. □

Önsav 12. *M, p-burulmalı ama derecesi sonlu olan bir modül olsun; yani bir t doğal sayısı için* $p^tM = 0$ *olsun. Ayrıca* $p^{t-1}M \neq 0$ *olsun. N, M'nin*

$$\oplus_I R/p^tR$$

modülüne izomorf olan bir altmodülü olsun. O zaman bir P altmodülü için,

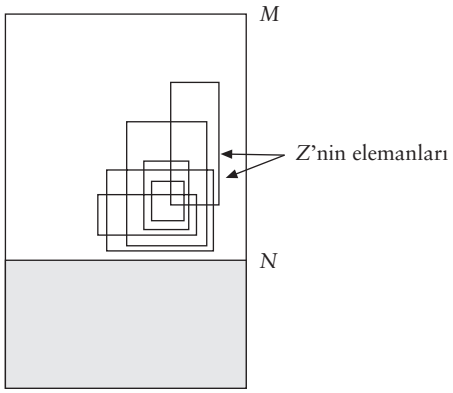
$$M = N \oplus P$$

olur.

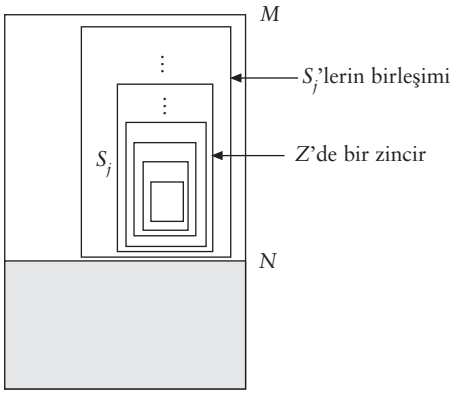
Kanıt: Zorn Önsavı'nı kullanacağız. (M sonlu sayıda eleman tarafından geriliyorsa, Zorn Önsavı'na gerek yok. Zorn Önsavı'ndan hoşlanmayan gençler bu paragrafı atlayıp bir sonraki paragrafa geçebilirler.

$$Z = \{S \leq M : S \cap N = 0\}$$

olsun. Z'yi altküme (yani altmodül) olma ilişkisiyle sıralayalım. Zorn Önsavı'nı uygulamak için Z'nin her zincirinin (yani tanımlanan sıralama için



her tamsıralı altkümesinin) Z'de bir üstsınırı olduğunu kanıtlamamız gerekiyor. Nitekim $(S_j)_{j\in J}$, Z'nin bir zinciri olsun. Yani her $j, k \in J$ için ya $S_j \leq S_k$ ya da $S_k \leq S_j$ olsun. O zaman $\cup_{j\in J} S_j$'nin bir modül olduğu ve N ile kesişmediği, dolayısıyla bu



modülün Z'de olduğu ve ayrıca her S_j'yi içerdiği, yani her S_j'den büyük olduğu bariz. Bir başka deyişle, $\cup_{j\in J} S_j$ modülü $(S_j)_{j\in J}$ zincirinin Z'de bir üstsınırıdır (aslında en küçük üstsınırıdır.) Demek ki Zorn Önsavı'nı uygulayıp Z'nin maksimal bir elemanı olduğunu buluruz. Bu maksimal elemana S diyelim.

Zorn Önsavı kısmını atlayanlar için: S'nin şu özelliği önemli: S, M'nin N ile kesişmeyen (daha doğrusu 0'da kesişen) en büyük altmodüllerinden biridir (genelllikle birden fazla vardır bu altmodüllerden), S'den büyük her altmodül N'yi 0'dan değişik bir altmodülde keser.

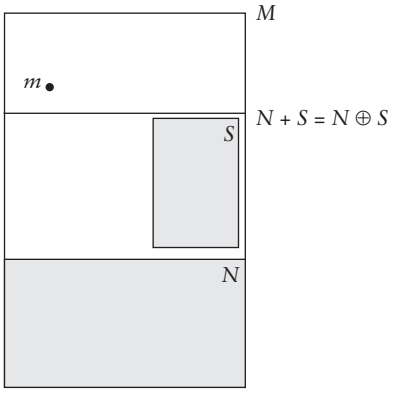
Elbette

$$\langle N, S\rangle = N + S = N \oplus S.$$

Şimdi M'nin $N + S$'ye eşit olduğunu kanıtlayalım. Tam tersine $N + S < M$ eşitsizliğini varsayıp bir çelişki elde edeceğiz.

Madem ki $N + S < M$, M'de olup da $N + S$'de olmayan bir eleman vardır. Böyle bir elemana m diyelim. Saflık derecesine varan iyimser bir günü-

müzde $\langle S, m\rangle \cap N = 0$ eşitliğini kanıtlayıp S'nin Z'de maksimalliğine karşıörnek olduğunu kanıtlamaya çalışabilirdik ama bu yanlış, çünkü eğer ola-



ğanüstü şanslı bir günümüzde değilsek, yani doğru m'yi seçmemişsek, $\langle S, m\rangle$ modülü N ile kesişir ve dolayısıyla Z'de olmaz. m'yi doğru bir m ile değiştireeceğiz.

$m \notin N + S$ ama $p^t m = 0 \in N + S$.

$$m, pm, p^2m, ..., p^tm$$

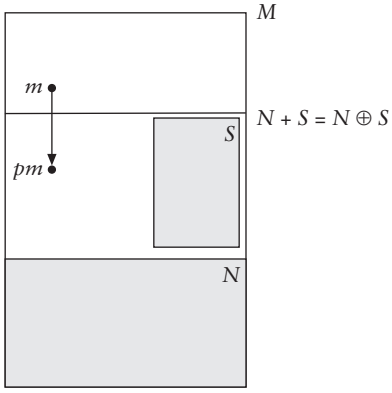
dizisine bakalım. İlk terim $N + S$'de değil ama son terim $N + S$'de. i doğal sayısı p^im'nin $N + S$'de olmadığı en büyük doğal sayı olsun. demek ki,

$$p^im \notin N + S \text{ ve } p^{i+1}m \in N + S.$$

Demek ki m elemanı yerine p^im elemanını alıp

$$m \notin N + S \text{ ve } pm \in N + S.$$

varsayımını yapabiliriz.



$n \in N$ ve $s \in S$ için,

$$pm = n + s$$

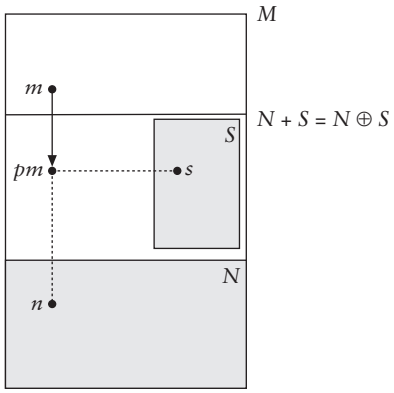
olarak yazalım. O zaman,

$$p^{t-1}n + p^{t-1}s = p^{t-1}(n + s) = p^{t-1}(pm) = p^tm = 0$$

olur, yani

$$p^{t-1}n = -p^{t-1}s \in N \cap S = 0$$

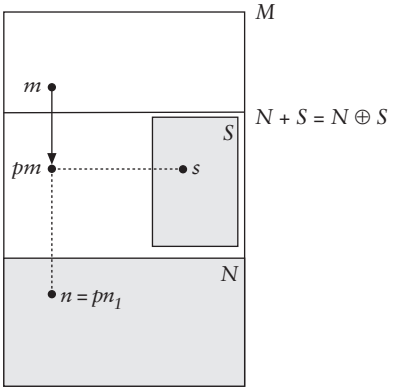
olur.



$N \approx \oplus_I R/p^tR$ izomorfisini anımsayıp, Sonuç 11'i uygulayalım: Öyle bir $n_1 \in N$ vardır ki,

$$n = pn_1$$

olur. Demek ki,



$$pm = n + s = pn_1 + s$$

ve

$$p(m - n_1) = pm - pn_1 = pm - n = s \in S.$$

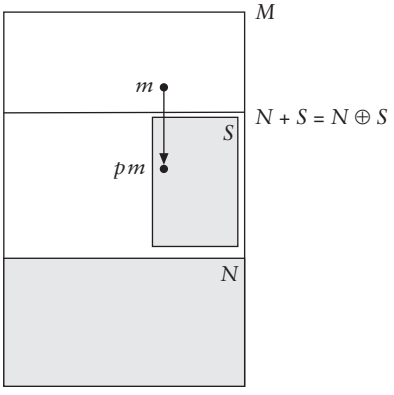
Şimdi,

$$m - n_1 \notin N + S \text{ ve } p(m - n_1) \in S$$

oldu. Artık m yerine $m - n_1$ alıp,

$$m \notin N + S \text{ ve } pm \in S$$

varsayımlarını yapabiliriz.



Yukarda kullandığımız n ve s elemanlarını unutalım. Mutlu sona bir adımcık kaldı:

Şimdi $\langle S, m\rangle \cap N = 0$ eşitliğini kanıtlayacağız ve bu da S'nin maksimalliğiyle çelişecek.

$\langle S, m\rangle \cap N$ kesişiminden herhangi bir n elemanı alalım. Bu elemanı, $s \in S$ ve $r \in R$ için,

$$n = s + rm \in \langle S, m\rangle \cap N$$

olarak yazabiliriz. Demek ki

$$rm = n - s \in N + S.$$

r, p'ye asal olamaz, çünkü aksi halde,

$$pm \in S \leq N + S$$

olduğundan, $m \in N + S$ olurdu. (Neden?) Demek ki p, r'yi bölüyor; diyelim $u \in R$ için, $r = pu$. O zaman,

$$rm = (pu)m = u(pm) \in S$$

olur ve buradan da

$$n = s + rm \in S \cap N = 0$$

çıkar. Önsav 12'yi kanıtladık. □

Teorem 9'un Kanıtı: t üzerine tümevarımla kanıtlayacağız.

Birinci Adım: Önce M'nin,

$$\oplus_I R/p^tR$$

modülüne izomorf en büyük altmodülünü bulacağız. Bunun için Zorn Önsavı'nı dikkatlice kullanacağız. (Eğer M sonlu eleman tarafından geriliyorsa, Zorn Önsavı'na ihtiyaç yok.)

$$\begin{aligned} Z = \{(m_i)_{i\in\alpha} :\ & \alpha \text{ bir ordinal,} \\ & \text{her } i \in \alpha \text{ için } m_i \in M, \\ & \langle m_i : i \in \alpha\rangle = \oplus_{i\in\alpha} Rm_i, \\ & Rm_i \approx R/p^tR\}. \end{aligned}$$

Z'yi şöyle sıralayalım: $(m_i)_{i\in\alpha}$ ve $(n_i)_{i\in\beta}$, Z'nin iki elemanıysa, $(m_i)_{i\in\alpha} \leq (n_i)_{i\in\beta}$ koşulu şu anlama gelsin: α, β'nın bir başlangıç dilimidir ve her $i \in \alpha$ için $m_i = n_i$ olur.

Zorn Önsavı'nı kullanmak için, Z'nin her zincirinin Z'de bir üstsınırı olduğunu kanıtlayalım.

$((m_{j,i})_{i\in\alpha(j)})_{j\in J}$ Z'den bir zincir olsun. O zaman, kolayca görülebileceği üzere,

$$\cup_{j\in J} (m_{j,i})_{i\in\alpha(j)},$$

Z'nin bir elemanıdır ve zincirin bir üstsınırıdır (aslında en küçük üstsınırıdır.)

Demek ki Z'ye Zorn Önsavı'nı uygulayabiliriz. $(m_i)_{i\in\alpha}$, Z'nin bir maksimal elemanı olsun.

$N = \langle m_i : i \in \alpha\rangle = \oplus_{i\in\alpha} Rm_i \approx \oplus_{i\in\alpha} R/p^tR\}$ olsun.

Alıştırma. M sonlu eleman tarafından gerilmişse, birinci adımı Zorn Önsavı'nı kullanmadan kanıtlayın.

Bir önceki Önsava göre, $N \oplus S = M$ eşitliğini sağlayan bir $S \leq M$ vardır.

İkinci Adım: $p^{t-1}S = 0$.

Eğer S'de $p^ts = 0$ eşitliğini sağlayan ama $p^{t-1}s = 0$ eşitliğini sağlamayan bir eleman varsa, o zaman, $(m_i)_{i\in\alpha}$ ailesinin en sonuna s elemanını ekleyerek, $(m_i)_{i\in\alpha}$ ailesinin Z'nin maksimal bir elemanı olduğuyla çelişiriz. Demek ki $p^{t-1}S = 0$.

Şimdi S'ye tümevarım varsayımını uygularsak, Teorem 9 kanıtlanmış olur. □□

Artık Teorem 1'i kanıtlayabiliriz.

Teorem 1'in Kanıtı. M, sonlu sayıda eleman tarafından gerilmiş bir R-modül olsun. T, M'nin burulmalı elemanlardan oluşan altmodülü olsun. Teorem 6'ya göre, özgür bir F altmodülü için,

$$M = T \oplus F$$

olur. Sonuç 4'e göre T ve F sonlu sayıda eleman tarafından (en fazla M'yi geren eleman kadar elemanla) gerilmişlerdir. Demek ki,

$$F \approx R \times \ldots \times R.$$

Teorem 8'e göre,

$$T = \oplus_{p \text{ asal}} M_p.$$

T sonlu eleman tarafından gerildiğinden, sadece sonlu tane p asalı için $M_p \neq 0$'dır. Demek ki, sonlu sayıda $p_1, \ldots, p_k$ asalı için

$$T = \oplus_{i=1}^{k} M_{p_i}.$$

Sonuç 4'e göre her M_{p_i} sonlu eleman tarafından gerilmiştir, diyelim $x_1, \ldots, x_r$ tarafından. Her $j = 1, \ldots, r$ için, k_j doğal sayısı $p_i^{k_j}x_j = 0$ eşitliğini sağlıyorsa, o zaman $k = \max\{p_1^{k_1}, \ldots, p_1^{k_r}\}$ için $p_i^k x_j = 0$ ve dolayısıyla $p_i^k M_{p_i} = 0$ eşitliği sağlanır. Demek ki Teorem 9'un varsayımları sağlanmıştır ve

$$M_{p_i} \approx \oplus_{j=1}^{t(p_i)} \left(\oplus_{I_{p_i,j}} R/p_i^j R \right)$$

eşitliği belli bir $t(p_i)$ doğal sayısı ve $I_{p_i,j}$ göstergeç kümeleri için sağlanır. Nihai sonuç,

$$\begin{aligned} M \approx T \oplus F &\approx \left(\oplus_{i=1}^{k} M_{p_i} \right) \oplus \left(R \times \ldots \times R \right) \\ &\approx \oplus_{i=1}^{k} \left(\oplus_{j=1}^{t(p_i)} \left(\oplus_{I_{p_i,j}} R/p_i^j R \right) \right) \oplus \left(R \times \ldots \times R \right) \end{aligned}$$

olur. □