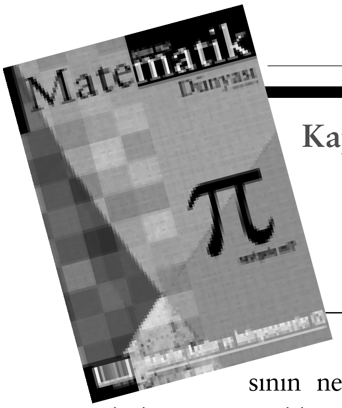


Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (2)

Tek Çarpanlama Bölgeleri ve Polinomlar

Bu yazıda, bir polinom halkasının ne zaman bir tek çarpanlama bölgesi (TÇB) olduğunu bulacağız. Tanımı anımsatalım: Tersinir ve sıfırbölen olmayan her elemanın sonlu sayıda asalın çarpımı olarak yazıldığı halkalara **tek çarpanlama halkası** (TÇH) denir. Eğer halka ayrıca bir tamlık bölgesiyse, o zaman **tek çarpanlama bölgesi**nden ya da kısaca TÇB'den sözedilir.

Tam olarak şu teoremi kanıtlayacağız.

Ana Teorem. *R bir halka olsun. $R[X]$'in bir TÇB olması için R'nin TÇB olması yeterli ve gerekli koşuldur.*

Bundan da şu sonuç çıkar:

Sonuç. $\mathbb{Z}[X_1, X_1, ..., X_n]$ *ve, eğer K bir cisimse, $K[X_1, X_1, ..., X_n]$ halkaları TÇB'dirler.*

Sayfa 31'de K bir cisimse $K[X]$'in bir TÇB olduğunu kanıtlamıştık. Bu sonucu bu yazıda kullanıp genelleştireceğiz.

Eğer $R[X]$ halkası TÇB'yse, R'nin de TÇB olması gerektiğinin kanıtı oldukça kolay. Bunu hemen şimdi yapabiliriz. Önce bir önsav.

Önsav 1. *R bir halka olsun. $R[X]$'te asal olan R'nin bir elemanı R'de de asaldır.*

Kanıt: Okura alıştırma olarak bırakılmıştır. □

Teorem 2. *Eğer $R[X]$ halkası TÇB'yse, R de TÇB'dir.*

Kanıt: Her şeyden önce $R[X]$ bir tamlık bölgesi olduğundan, R de bir tamlık bölgesidir. $r \in R$ olsun. Aynı zamanda $r \in R[X]$ olduğundan, r'yi $R[X]$'teki p asallarının sonlu çarpımı olarak yazabiliriz. Ama derecelere bakacak olursak p asallarının aslında R'de olduklarını görürüz. Yukardaki önsava göre bu p'ler R'de de asaldır. □

R'nin TÇB olduğunu kabul edip $R[X]$'in TÇB olduğunu kanıtlamak biraz daha zor.

Yazımız birbirinden bağımsız iki bölümden oluşacak.

A) Polinomlarda İndirgenemezler yazımızda, eğer K bir cisimse, $K[X]$ polinom halkasının TÇB olduğunu kanıtlamıştık. Bu sonuçtan $\mathbb{Q}[X]$ halkasının TÇB olduğu çıkar. Önce, bu sonucu kullanarak, $\mathbb{Z}[X]$ halkasının bir TÇB olduğunu kanıtlayacağız.

B) Sonra, eğer R bir TÇB'yse, yukardaki bölümdeki yöntemi kullanarak, $R[X]$ polinom halkasının da TÇB olduğunu kanıtlayacağız.

Dileyen okur A bölümünü atlayıp doğrudan B bölümüne geçebilir. Daha önce de dediğimiz gibi bu iki bölüm birbirinden bağımsızdır.

A. $\mathbb{Z}[X]$ TEK ÇARPANLAMA BÖLGESİDİR

$\mathbb{Z}[X]$ halkasının 0, 1 ve –1 olmayan her elemanının indirgenemezlerin çarpımı olarak yazıldığını biliyoruz [sayfa 27, Teorem 10; bunu ayrıca bir de bir sonraki bölümde kanıtlayacağız.] Ayrıca sayfa 31'den $\mathbb{Q}[X]$ halkasının TÇB olduğunu biliyoruz, yani bu halkada her indirgenemez bir asaldır. Şimdi aynı sonucu $\mathbb{Z}[X]$ için de kanıtlamak istiyoruz, yani $\mathbb{Z}[X]$'in her indirgenemezinin bir asal olduğunu kanıtlamak istiyoruz.

Önce sık sık kullanacağımız bir sonucu ortalığa çıkaralım:

Hayat Zor!

$\mathbb{Z}/6\mathbb{Z}[X]$ halkasında

$$X(X–1) = (X–3)(X–4)$$

eşitliği geçerli olduğundan, indirgenemez olan

$$X,\ X–1,\ X–3,\ X–4$$

polinomlarının hiçbiri $\mathbb{Z}/6\mathbb{Z}[X]$ halkasında asal değildir. Dolayısıyla, $\mathbb{Z}/6\mathbb{Z}$, TÇH olmasına karşın, $\mathbb{Z}/6\mathbb{Z}[X]$, TÇH değildir. Hangi n'ler için $\mathbb{Z}/n\mathbb{Z}[X]$ bir TÇH'dir?

Önsav 3. *g ve $f \in \mathbb{Z}[X]$ olsun. g'nin katsayılarının ±1'den başka ortak böleni olmasın (yani aralarında asal olsunlar.) Eğer g, f'yi $\mathbb{Q}[X]$'te bölüyorsa, o zaman $\mathbb{Z}[X]$'te de böler. Yani eğer $h \in \mathbb{Q}[X]$ için, $f = gh$ ise, $h \in \mathbb{Z}[X]$.*

Kanıt: h'nin katsayılarının paydalarının en küçük ortak katı n ise, bir $k \in \mathbb{Z}[X]$ için $h = k/n$ yazabiliriz. Gerekirse (aslında gerekmez ya!) sadeleştirme yaparak, n'nin hiçbir asal böleninin k'nin tüm katsayılarını bölmediğini varsayabiliriz. $n = \pm 1$ eşitliğini kanıtlayacağız. Böylece h'nin $\mathbb{Z}[X]$'te olduğu anlaşılacak.

Demek ki $f = gh = gk/n$, yani $nf = gk$. Şimdi p, n'nin asal bir böleni olsun. $\mathbb{Z}$'nin p asalı $\mathbb{Z}[X]$ halkasında gk çarpımını böldüğüne göre, Gauss Önsavı'na göre (sayfa 25, Önsav 7), p, g'nin ya da ya da k'nin tüm katsayılarını böler, ki bu da bir çelişkidir. Demek ki $n = \pm 1$ olmalı ve $h = k/n = \pm k \in \mathbb{Z}[X]$. □

Teorem 4. $\mathbb{Z}[X]$'*in bir indirgenemezi* ya $\mathbb{Z}$'*nin ya da* $\mathbb{Q}[X]$'*in bir indirgenemezidir*.

Kanıt: f, $\mathbb{Z}[X]$ halkasında bir indirgenemez olsun. $g, h \in \mathbb{Q}[X]$ için, $f = gh$ olarak yazalım. Ya g'nin ya da h'nin bir sabit polinom olduğunu kanıtlayacağız.

İlk olarak, g'yi kesirli bir sayıyla çarparak ve h'yi aynı sabite bölerek, g'nin $\mathbb{Z}[X]$'te olduğunu ve katsayılarının ortak böleni olmadığını varsayacağız. Bunu şöyle yapacağız: n, g'nin katsayılarının paydalarının çarpımı olsun. O zaman ng polinomu $\mathbb{Z}[X]$'tedir. $g_1 = ng$ olsun. Şimdi g_1'in katsayılarının en büyük ortak böleni m olsun. Demek ki, katsayılarının ortak böleni olmayan bir $g_2 \in \mathbb{Z}[X]$ için, $g_1 = mg_2$. Hesap yapalım:

$$f = gh = (g_1/n)h = (mg_2/n)h = g_2(mh/n).$$

$h_2 = mh/n$ yazarsak, $f = g_2h_2$ eşitliğini elde ederiz. Unutmayalım ki $g_2 \in \mathbb{Z}[X]$ ve g_2'nin katsayılarının ortak böleni yok.

Demek ki g_2, f'yi $\mathbb{Q}[X]$ halkasında bölüyor: $f = g_2h_2$. Önsav 3'e göre $h_2 \in \mathbb{Z}[X]$ olmalı. Ama f, $\mathbb{Z}[X]$ halkasında indirgenemez. Demek ki ya g_2 ya da h_2 polinomu $\mathbb{Z}[X]$'te tersinir, yani ± 1'e eşit, dolayısıyla ya g ya da h polinomu $\mathbb{Q}$'da bir sabit (ikisi de sabit olabilir). Böylece f'nin ya $\mathbb{Z}$'de olduğunu ya da $\mathbb{Q}[X]$ halkasında da indirgenemez olduğunu kanıtlamış olduk. □

Şimdi istediğimizi kanıtlayabiliriz.

Teorem 5. $\mathbb{Z}[X]$ *bir tek çarpanlama bölgesidir*.

Kanıt. Sayfa 27'deki Teorem 10'da $\mathbb{Z}[X]$'in her elemanının sonlu sayıda indirgenemezin çarpımı olduğunu söyledik. (Bu sonuç geçen sayıda kanıtlanmıştı. Aynı sonucu, bu yazının ikinci bölümünde, bu bölümden bağımsız olarak bir kez daha kanıtlayacağız.) Dolayısıyla $\mathbb{Z}[X]$'in her indirgenemezinin bir asal olduğunu kanıtlamalıyız.

$f \in \mathbb{Z}[X]$ bir indirgenemez olsun.

Eğer $f \in \mathbb{Z}$ ise, f, $\mathbb{Z}$'de bir asaldır, çünkü f'yi $\mathbb{Z}$'nin asallarının çarpımı olarak yazdığımızda, f, $\mathbb{Z}[X]$'in bir indirgenemezi olduğundan, bu asallar biri dışında hepsi $\mathbb{Z}[X]^*$ kümesinde olmalı, dolayısıyla biri dışında hepsi ± 1'dir, yani f, $\mathbb{Z}$'nin bir asalıdır. Gauss Önsav'ına göre f, $\mathbb{Z}[X]$'in de bir asalıdır.

Bundan böyle f'nin $\mathbb{Z}$'de olmadığını varsayalım. Demek ki f'nin katsayılarının ortak böleni yok (yoksa f indirgenirdi.) $g, h \in \mathbb{Z}[X]$ için, f'nin gh'yi $\mathbb{Z}[X]$'te böldüğünü varsayalım. f'nin ya g'yi ya da h'yi $\mathbb{Z}[X]$'te böldüğünü kanıtlayacağız. f, gh'yi $\mathbb{Z}[X]$'te böldüğüne göre, f, gh'yi $\mathbb{Q}[X]$'te de bölüyordur. Ama yukardaki teoreme göre f, $\mathbb{Q}[X]$'te bir indirgenemez, yani bir asal (sayfa 31). Demek ki f, ya g'yi ya da h'yi $\mathbb{Q}[X]$'te bölüyor. Diyelim f, g'yi $\mathbb{Q}[X]$'te bölüyor: $f = gk$ ve $k \in \mathbb{Q}[X]$. Önsav 3'e göre $k \in \mathbb{Z}[X]$. Ama f, $\mathbb{Z}[X]$ halkasının bir indirgenemezi. Demek ki ya $g = \pm 1$ ya da $k = \pm 1$. Birinci şıkta $gh = \pm h$ ve f, h'yi böler. İkinci şıkta $f = \pm g$ ve f, g'yi böler. □

B. $R[X]$ TEK ÇARPANLAMA BÖLGESİDİR

Bu bölümde, R bir TÇB'yse, $R[X]$'in de bir TÇB olduğunu kanıtlayacağız. Yani R'nin sıfır ve tersinir olmayan her elemanının R'nin sonlu sayıda asalının çarpımı olarak yazıldığını varsayıp aynı şeyin $R[X]$ için de geçerli olduğunu kanıtlayacağız.

Sayfa 25, Önsav 7'ye göre R'nin bir asalı (ya da indirgenemezi, aynı şey), $R[X]$'te de bir asaldır (dolayısıyla indirgenemezdir.) Dolayısıyla $R[X]$'in bir sabit polinomunu R'de asallarının çarpımı olarak yazarsak, böylece o sabit polinomu $R[X]$'te asalların çarpımı olarak yazmış oluruz. Dolayısıyla sorun, $R[X]$'in sabit olmayan polinomlarını asalların çarpımı olarak yazabilmekte. Bunu yapabilmek için R'nin bölüm cismine (bknz. sayfa 43-46) geçeceğiz. Yukarda $\mathbb{Z}$ için $\mathbb{Q}$'nün oynadığı rolü, bu bölümde R için R'nin bölüm cismi oynayacak.

K, R halkasının bölüm cismi olsun. Bölüm cisimlerini anımsatalım:

$$K = \{r/s : r, s \in R, s \neq 0\}$$

dir. K kümesinde,

$$r/s = t/u \text{ ancak ve ancak } ru = st \text{ ise}$$

eşitlik kuralı kabul edilir ve toplama ve çarpma işlemleri olabilecek en doğal ve okurun tahmin ettiği şekilde tanımlanır. Bütün bunlar sayfa 43-46'da ayrıntılarıyla matematiksel olarak açıklanmıştı.

K bir cisim olduğundan, $K[X]$'in bir TÇB olduğunu biliyoruz, yani $K[X]$'in her elemanı sonlu sayıda asalın çarpımı olarak yazılır. $R[X]$ de $K[X]$'in bir althalkası olduğundan, $R[X]$'in R'de olmayan her elemanı $K[X]$'in asallarının/indirgenemezlerinin çarpımı olarak yazılır. Dolayısıyla $K[X]$'in asallarının R ve $R[X]$'in elemanları cinsinden nasıl yazıldıklarını bulmalıyız. Bunu Önsav 8'de yapacağız.

Aynen, yukarda $\mathbb{Z}[X]$ ve $\mathbb{Q}[X]$ için yaptığımızı yapacağız, tek farkla ki $\mathbb{Z}$'nin yerini R, $\mathbb{Q}$'nün yerini de K alacak. Önümüze çıkabilecek bir zorluk şu olabilir: $\mathbb{Z}$ için tanımladığımız ve yukarda kullandığımız bir kavramı daha R için tanımlamamış olabiliriz. Nitekim Teorem 4'te $\mathbb{Z}$'nin elemanlarının en büyük ortak böleninden sözetmişiz. Böyle bir kavramı daha herhangi bir TÇB için tanımlamadık. Bu tür eksiklikleri de giderdik mi sorun kalmayacak. Yalnız dikkat edilmesi bir nokta, $\mathbb{Z}$ ve $K[X]$ için doğru olan Bezout Önsavı'nın, ne yazık ki R ya da $R[X]$ halkaları için doğru olmayabileceğidir.

R'nin iki elemanının "en büyük ortak böleni" kavramını tanımlayalım. a ve b, R'nin 0 olmayan iki elemanı olsun. Eğer a ya da b, R'de tersinirse, ebob(a, b)'yi R^* kümesi olarak tanımlayalım. Eğer a ya da b tersinir değillerse, a'yı ve b'yi asallarının çarpımı olarak yazalım:

$$a = p_1^{n_1} \dots p_k^{n_k},$$
$$b = p_1^{m_1} \dots p_k^{m_k}.$$

Burada n_i ve m_i'ler doğal sayılar. Eğer, örneğin p_1, a'yı bölmüyorsa, $n_1 = 0$. Şimdi ebob(a, b)'yi şöyle tanımlayalım:

$$\text{ebob}\,(a,b) = p_1^{\min(n_1, m_1)} \dots p_k^{\min(n_k, m_k)} R^*.$$

Tanıma biraz aykırı kaçsa da ebob(a, b)'nin herhangi bir elemanını gene ebob(a, b) olarak yazacağız. Umarız bu bir karışıklığa neden olmaz. Örneğin, ebob(8, 12) = ±4 olmasına karşın, çoğu zaman, ebob(8, 12)'yi 4 kabul ederiz.

Tanımdan hemen görüleceği üzere, ebob(a, b) (aslında ebob(a, b)'nin her elemanı) elbette hem a'yı hem de b'yi böler. Ayrıca R'nin hiçbir asalı hem a/ebob(a, b)'yi hem de b/ebob(a, b)'yi bölmez, yani a/ebob(a, b)'yle b/ebob(a, b)'nin ebob'u 1'dir (yani R^*'dır.)

Eğer $b \neq 0$ ise, ebob(0, b) = b olarak tanımlanır. ebob(0, 0) tanımlanmaz.

Eğer ebob(a, b) = 1 (yani R^* ise), a ve b'nin ortak böleninin olmadığını söyleyeceğiz ve a ve b'ye **aralarında asal** diyeceğiz. Örneğin, a ya da $b \neq 0$ ise a/ebob(a, b)'yle b/ebob(a, b) elemanı aralarında asaldır.

Elbette, ikiden fazla elemanın da ebob'unu tanımlayabiliriz.

Bu tanımdan sonra, Önsav 3'ü genelleştirebiliriz:

Önsav 6. *g ve $f \in R[X]$ olsun. Ayrıca g'nin katsayılarının ortak böleninin olmadığını varsayalım. Eğer g, f'yi $K[X]$'te bölüyorsa, o zaman $R[X]$'te de böler. Yani eğer $h \in K[X]$ için, $f = gh$ doğruysa, $h \in R[X]$'tir.*

Kanıt: h'nin katsayılarının paydalarının çarpımı n ise, bir $k \in R[X]$ için $h = k/n$ yazabiliriz. Gerekirse sadeleştirme yaparak, n'nin hiçbir asal böleninin k'nin tüm katsayılarını bölmediğini varsayabiliriz. $n \in R^*$ ilişkisini kanıtlayacağız.

Demek ki $f = gh = gk/n$, yani $nf = gk$. Şimdi p, n'nin asal bir böleni olsun. R'nin p asalı $R[X]$ halkasında gk çarpımını böldüğünden, Gauss Önsavı'na göre (sayfa 25, Önsav 7), p, g'nin ya da ya da k'nin tüm katsayılarını böler, ki bu da bir çelişkidir. Demek ki $n \in R^*$ olmalı ve $h = k/n \in R[X]$. □

Teorem 7. *$R[X]$'in bir indirgenemezi* ya *R'dedir ya da $K[X]$'in de bir indirgenemezidir.*

Kanıt: f, $R[X]$ halkasının R'de olmayan bir indirgenemezi olsun. $g, h \in K[X]$ için, $f = gh$ olarak yazalım. Ya g'nin ya da h'nin bir sabit polinom olduğunu kanıtlayacağız.

İlk olarak, g'yi K'den bir elemanla çarparak ve h'yi aynı elemana bölerek, g'nin $R[X]$'te olduğunu

Bézout Önsavı

Bézout Önsavı, her TÇB, örneğin $\mathbb{Z}[X]$ polinom halkasında doğru değildir: 2 ve X, $\mathbb{Z}[X]$'te birbirine asaldır, ama $\mathbb{Z}[X]$'te $2g + Xh = 1$ eşitliğini sağlayan g ve h polinomları yoktur.

Bézout Önsavı, $K[X, Y]$ tek çarpanlama bölgesinde de doğru değildir: $Xg + Yh = 1$ eşitliğini sağlayan g ve $h \in K[X, Y]$ yoktur. Olsaydı, her iki tarafı da $X = Y = 0$'da değerlendirip $0 = 1$ bulurduk.

Ama eğer K bir cisimse, Bézout Önsavı $K[X]$'te geçerlidir. Bunu sayfa 30 ve 42'de iki kez kanıtlamıştık.

ve katsayılarının ortak böleni olmadığını varsayacağız. Bunu şöyle yapacağız: n, g'nin katsayılarının paydalarının çarpımı olsun. O zaman $ng \in R[X]$. $g_1 = ng$ olsun. Şimdi g_1'in katsayılarının en büyük ortak bölemi m olsun. Demek ki, katsayılarının ortak böleni ancak R^*'da olabilen (yani aralarında asal olan) bir $g_2 \in R[X]$ için, $g_1 = mg_2$. Hesap yapalım:

$$f = gh = (g_1/n)h = (mg_2/n)h = g_2(mh/n).$$

$h_2 = mh/n$ yazarsak, $f = g_2h_2$ eşitliğini elde ederiz. Ayrıca $g_2 \in R[X]$ ve g_2'nin katsayılarının ortak böleni yok.

Demek ki g_2, f'yi $K[X]$ halkasında bölüyor: $f = g_2h_2$. Önsav 6'ya göre $h_2 \in R[X]$ olmalı. Ama f, $R[X]$ halkasında indirgenemez. Demek ki ya g_2 ya da h_2 polinomu $R[X]$'te tersinir, yani R^* kümesinde, dolayısıyla ya g ya da h polinomu K'da bir sabit. Böylece f'nin $K[X]$ halkasında da indirgenemez olduğunu kanıtlamış olduk. □

Önsav 8. *$K[X]$'in her indirgenemezi, bir $g \in R[X]$ indirgenemezi ve bir $\alpha \in K^*$ için αg biçiminde yazılır.*

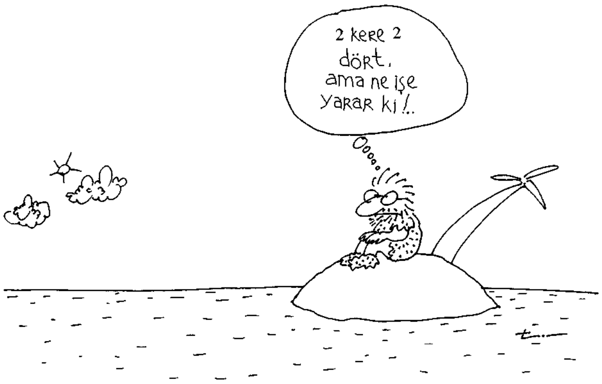
Kanıt: f, $K[X]$'in bir indirgenemezi olsun. Birçok kez yaptığımız gibi, bir $\alpha \in K^*$ ve katsayılarının ortak böleni olmayan bir $g \in R[X]$ için $f = \alpha g$ yazabiliriz. g'nin $R[X]$'te indirgenemez olduğunu savlıyoruz: $h, k \in R[X]$ için $g = hk$ olsun. O zaman $f = \alpha g = \alpha hk$ ve f, $K[X]$'te indirgenemez olduğundan, ya h ya da $k \in R[X] \cap K^* = R^*$. □

Şimdi artık istediğimizi kanıtlayabiliriz.

Teorem 9. *$R[X]$ bir tek çarpanlama bölgesidir.*

Kanıt. Önce $R[X]$'in 0 ya da tersinir olmayan, yani $\{0\} \cup R^*$'da olmayan her elemanının $R[X]$'in sonlu sayıda indirgenemezinin çarpımı olarak yazıldığını kanıtlayacağız. f, böyle bir polinom olsun.

Eğer $f \in R$ ise kanıt oldukça kolay: Sayfa 25, Önsav 7'ye göre R'nin bir asalı (ya da indirgenemezi, aynı şey), $R[X]$'te de bir asaldır. Dolayısıyla f'yi R'de asallarının çarpımı olarak yazarsak, f'yi $R[X]$'in asallarının çarpımı olarak yazmış oluruz.



Şimdi $f \notin R$ olsun. f, $K[X]$'te olduğundan, f, $K[X]$'in sonlu sayıda indirgenemezinin çarpımı olarak yazılabilir. Önsav 8'e göre, $K[X]$'in bu indirgenemezleri, K'nin bir elemanı ve $R[X]$'in bir indirgenemezinin çarpımı olarak yazılabilir. Demek ki $\alpha \in K^*$ ve $R[X]$'in derecesi 0'dan büyük $f_1, ..., f_k$ indirgenemezleri için, $f = \alpha f_1 ... f_k$. Birbirine asal b ve $c \in R$ için $\alpha = b/c$ yazarsak, $cf = bf_1 ... f_k$ eşitliğini buluruz. c'yi bölen bir asal, $R[X]$'te de asal olduğundan [Gauss Önsavı, sayfa 25, Önsav 7], aynı asal f_i'lerden birini bölmeli (b'yi bölemez), ama bu, f_i'nin $R[X]$'te indirgenemez olmasıyla ve derecesinin en az 1 olmasıyla çelişir. Demek ki c tersinir. c'yi c^{-1} olarak sağ tarafa aktararak,

$$f = c^{-1}bf_1 ... f_k$$

eşitliğini elde ederiz. Şimdi b'yi R'de asallarına ayırarak, Gauss Önsavı sayesinde, f'yi $R[X]$'teki indirgenemezlerinin çarpımı olarak yazmış oluruz.

$R[X]$'in her indirgenemezinin bir asal olduğunu kanıtlamak kaldı. $f \in R[X]$ bir indirgenemez olsun.

Eğer $f \in R$ ise, $R[X]$'in bir indirgenemezi olan f, R'de bir asaldır, çünkü f'yi R'nin asallarının çarpımı olarak yazdığımızda, bu asallar $R[X]$'in de birer asalıdır (Gauss Önsavı), dolayısıyla biri dışında hepsi tersinirdir, yani f, R'nin bir asalıdır. Önsav 1'e göre f, $R[X]$'in de bir asalıdır.

Bundan böyle f'nin R'de olmadığını varsayalım. Demek ki f'nin katsayılarının ortak böleni yok (yoksa f indirgenirdi.) $g, h \in R[X]$ için, f'nin gh'yi $R[X]$'te böldüğünü varsayalım. f'nin ya g'yi ya da h'yi $R[X]$'te böldüğünü kanıtlayacağız. f, gh'yi $R[X]$'te böldüğüne göre, f, gh'yi $K[X]$'te de bölüyordur. Ama Teorem 7'ye göre, f, $K[X]$'te bir indirgenemez, yani bir asal (sayfa 31). Demek ki f, ya g'yi ya da h'yi $K[X]$'te bölüyor. Diyelim f, g'yi $K[X]$'te bölüyor: $f = gk$ ve $k \in K[X]$. Önsav 6'ya göre $k \in R[X]$. Ama f, $R[X]$ halkasının bir indirgenemezi. Bundan ve $f = gk$ eşitliğinden, ya g'nin ya da k'nin R^*'da olduğu çıkar. Birinci şıkta f, gh'yi böldüğünden, h'yi de böler. İkinci şıkta f, gk'ye eşit olduğundan, g'yi böler. ♥