Birebir Polinom Fonksiyonları Örtendir

Ayhan Günaydın

ayhan.gunaydin@boun.edu.tr

8 Kasım 2020

Başlık Bize Ne Anlatmaya Çalışıyor?

Polinom Fonksiyonu Nedir?

$$f : K^m \to K^n; \quad f(\vec{x}) = \big(f_1(\vec{x}), \ldots, f_n(\vec{x})\big)$$

K bir cisim, $f_1, \ldots, f_n$ m-değişkenli polinomlar.
Başlık yanlış:

$$f : K \to K^2; \quad f(x) = (x, 0)$$

Tabii ki birebir ve tabii ki örten değil.
En azından $m = n$ olsa iyi olur gibi. Ama:

$$f : \mathbb{Q} \to \mathbb{Q}; \quad f(x) = x^3$$

Birebir ama örten değil.
Demek ki hangi cisimle uğraştığımız da mühim gibi.

Doğru Önerme

Teorem (Ax-Grothendieck)

Bir $f : \mathbb{C}^n \to \mathbb{C}^n$ polinom fonksiyonu birebirse örtendir.

* Bu teorem, $\mathbb{C}$ yerine herhangi cebirsel kapalı bir cisim alındığında da doğru. Bizim bugün göreceğimiz yöntem ile o genellikte kanıtlanabiliyor.

* Ayrıca, $\mathbb{C}^n$ yerine herhangi bir cebirsel küme $V(\mathbb{C})$ alınabilir; yani verilen polinomların 0-kümesi. Bu da bizim kanıttan kolayca çıkacak.

* Bu teorem $\mathbb{C}$ yerine $\mathbb{R}$ aldığımızda da doğru. Ama bunun kanıtı bizim kanıttan hemencecik çıkmıyor.

* $\mathbb{C}$ yerine sonlu cisim alındığında sonucun doğruluğu cebirle alakası olmayan sebeplerden doğru.

$n = 1$ Durumu

$\mathbb{C}$ cebirsel kapalı. Demek ki sabit olmayan herhangi $f : \mathbb{C} \to \mathbb{C}$ polinom fonksiyonu örten.

Eğer havalı konuşmak istersek de Picard Teoremini kullanıp birebir (kompleks) analitik fonksiyonlar örtendir diyebiliriz.

$f : \mathbb{R} \to \mathbb{R}$ polinom fonksiyonu. Derecesi tekse örten. Derecesi çiftse birebir değil.

Birazcık da Mantık - Formüller

Modeller kuramı çerçevesinde çalışırken, ele alacağımız matematiksel yapı ile ilgili olarak bir *dil* sabitleriz. Dil ile ne kastettiğimizin detayına çok girmeyeceğim, keza bugün sadece $L = \{+, \cdot, -, 0, 1\}$ dilini kullanacağız.
Sonra bu dildeki formülleri belirleriz. Genelde burası en çok kafa karışıklığına sebep olan nokta oluyor. O yüzden yukarıdaki L dilindeki formüllerin neler olduğunu kısaca detaylandıralım.
Bu dildeki *terimler* polinomlar ve en basit formüller polinom eşitlikleri. Sonra polinom eşitsizlikleri geliyor. Daha sonra da $\vee$ ve $\wedge$ ile bu tür formülleri bağlıyoruz. En karmaşık olan da *niceleyiciler*: $\exists$ ve $\forall$. En kritik olan bunların sadece elemanlara uygulanabiliyor olması; yani altkümelere, fonksiyonlara vs. uygulanmıyor.

Serbest değişken içermeyen formüllere *cümle* diyoruz.

Birazcık da Mantık - Doğruluk

Şimdilik elimizde formel objeler olan formüller var. Bunların tek başlarına doğruluğu ya da yanlışlığından bahsedemeyiz. Bunun için bu dildeki *yapıları* tanıtmak lazım: Bir küme ve dildeki her sembolün bir yorumu var. Dildeki sembol $+$ diye bu sembolün yorumunun toplama olması şart değil ama genelde öyle olur. Mesela her halka bir L-yapısı.

Bir $\phi(x_1, \ldots, x_n)$ formülü verilsin. Şimdi verilen bir M yapısı ve $\vec{a} \in M^n$ için *ϕ'nin (M içinde) $\vec{a}$'daki doğruluğundan* bahsedebiliriz. Notasyon:

$$M \models \phi(\vec{a}).$$

Eğer ϕ bir cümleyse, doğruluğundan bahsetmek için bir $\vec{a}$ elemanı almaya gerek yok.

Birazcık da Mantık - Teoriler

Bir *teori* sadece bir cümleler kümesidir. Biz burada her teorinin bir modeli, yani içindeki her cümleyi doğru yapan bir yapı, olduğunu varsayacağız. Bir teorinin *tam* olması her cümle için ya o cümlenin ya da tersinin o teoride olması demek. Örneğin verilen bir M modelinin teorisi:

$$\mathrm{Th}(M) := \{\sigma : M \models \sigma\}.$$

İşin aslı her tam teori böyle. Bu yüzden de çoğu teori tam değil.

Şu bir kenarda dursun:

Teorem

Verilen bir $p \geq 0$ icin karakteristiği p olan cebirsel kapalı cisimler teorisi tamdır. (Bu teoriyi ACF_p şeklinde göstereceğiz.)

Birazcık da Mantık - Kanıtlanabilirlik

Tanımlamadan sizin sezginize bırakacağım bir tanımdan bahsedeceğim: Bir teorinin bir cümleyi *kanıtlaması*. Bunu $T \vdash \sigma$ olarak gösteriyoruz. Sadece bir örnek verelim: Mesela gruplar teorisinde, 'birim eleman tektir' cümlesi kanıtlanabilir.

Sezgisel olarak makul gelecek olsa da bir sonraki teoremin ne kadar mühim olduğunu ifade etmek için yeterli kelime yok.

Teorem (Gödel Tamlık Teoremi)

Her T teorisi ve σ cümlesi için şu doğrudur:

$$T \vdash \sigma \iff T \models \sigma.$$

Sağdaki kavramı tanımlamadık: 'σ, T'nin her modelinde doğrudur' demek.

Birazcık da Mantık - Bonus: Tıkızlık Teoremi

İleride kullanmayacağız ama tamlık teoreminden hemencecik çıktığı için şunu kayda geçirelim.

Teorem (Tıkızlık Teoremi)

Bir Γ cümleler kümesinin modeli olması için gerek-yeter koşul her sonlu altkümesinin modeli olmasıdır.

Soruyu Mantığa İndirgeme

Göstermek istediğimizi bir L-cümlesi olarak yazmaya çalışalım:

$$\forall f(\forall \vec{x} \forall \vec{y}(f(\vec{x}) = f(\vec{y}) \to \vec{x} = \vec{y}) \to \forall \vec{u} \exists \vec{v}(\vec{u} = f(\vec{v}))).$$

Buradaki sorun $\forall f$ kısmı. Onun yerine 'derecesi en fazla d olan her polinom fonksiyonu için' yazabiliriz...

Bu cümleye σ_d diyelim.

Göstermek istediğimiz şu şekilde ifade edilebilir: Her $d > 0$ için

$$\mathbb{C} \models \sigma_d$$

Ya da

$$\mathrm{ACF}_0 \models \sigma_d.$$

ACF_0

ACF_0 teorisini şu şekilde ifade edebiliriz:

ACF: Cebirsel kapalı cisimler teorisi; bunu L dilinde nasıl ifade edebileceğimiz üzerine biraz düşünmek gerekli.

χ_p: Her $p > 0$ için bu tek bir cümle ve $p \neq 0$ diyor. Ya da $1 + \cdots + 1 \neq 0$.

Diyelim ki kanıtlamak istediğimiz yanlış. Yani $\mathrm{ACF}_0 \not\models \sigma_d$. Demek ki $\mathrm{ACF}_0 \models \neg\sigma_d$. Gödel Tamlık Teoremi'nden dolayı da $\mathrm{ACF}_0 \vdash \neg\sigma_d$. Bir 'kanıt' sadece sonlu adım içerdiği için ACF_0 teorisinin sadece sonlu bir kısmı bu kanıtta kullanılıyor. Yani aslında

$$\mathrm{ACF} \cup \{\chi_{p_1}, \ldots, \chi_{p_m}\} \vdash \neg\sigma_d$$

olacak şekilde $p_1, \ldots, p_m$ asalları var. Bu durumda bu asallardan daha büyük bir p asalı aldığımızda

$$\mathrm{ACF}_p \vdash \neg\sigma_d.$$

ACF_p

Demek ki karakteristiği p olan her cebirsel kapalı cisimde $\neg\sigma_d$ cümlesi doğru. Bu cümleyi yeniden insan cümlesi yaparsak:

Karakteristiği p olan her K cebirsel kapalı cismi için birebir olup örten olmayan (ve derecesi en fazla d olan) bir f polinom fonksiyonu vardır.

O zaman yolumuza $K = \overline{\mathbb{F}}_p$ alarak devam edelim. $f : \overline{\mathbb{F}}_p^n \to \overline{\mathbb{F}}_p^n$ de birebir olup örten olmayan polinom fonksiyonumuz olsun.

Bundan sonrası cebir...

Örtenliği bozan eleman $\vec{b} = (b_1, \ldots, b_n) \in \overline{\mathbb{F}}_p^n$ olsun; ayrıca f içinde gözüken katsayılar da $A \subseteq \overline{\mathbb{F}}_p$ sonlu kümesinden olsun. Son olarak da $k = \mathbb{F}_p(A \cup \{b_1, \ldots, b_n\})$ olarak tanımlayalım. İki şeye dikkat edelim:

1. k sonlu bir cisim.
2. f'nin k^n'ye kısıtlamasının görüntüsü k^n'nin içinde kalıyor. Yani

$$g = f|_{k^n} : k^n \to k^n$$

bir polinom fonksiyonu. Ve g hala birebir. Ama sonlu bir kümeden kendisine gidiyor! Demek ki örten. Demek ki $\vec{b}$, f'nin görüntü kümesinde ama aynı zaman da değil. Aradığımız çelişki de bu.