$\mathbb{Q}[\sqrt{d}]$'nin Çıkarma ve Kare Alma Altında Kapalı Altkümeleri

Serhat Doğan* / *kelaker@gmail.com*

Bu yazıda aşağıdaki teoremi kanıtlayacağız:

Teorem. $\mathbb{Q}[\sqrt{d}]$ *kümesinin bir altkümesi çıkarma ve kare alma altında kapalıysa çarpma altında da kapalıdır.*

Önce kolay bir önsav:

Önsav. *Eğer* $A \subseteq \mathbb{R}$, *çıkarma ve kare altında kapalıysa, o zaman her* $\alpha, \beta \in A$ *için,* $\alpha + \beta \in A$ *ve* $2\alpha\beta \in A$. *Dolayısıyla her* $n \in \mathbb{Z}$ için $n\alpha \in A$.

Kanıt: $0 = \alpha - \alpha \in A$ olduğundan, $-\beta = 0 - \beta \in A$. Dolayısıyla $\alpha + \beta = \alpha - (-\beta) \in A$. Bundan da $2\alpha\beta = (\alpha + \beta)^2 - \alpha^2 - \beta^2 \in A$ çıkar. Eğer $n > 0$ ise, $n\alpha = \alpha + ... + \alpha$ olduğundan, $n\alpha \in A$. Buradan, her $n \in \mathbb{Z}$ için, $n\alpha \in A$ çıkar. □

Teoremin Kanıtı. Eğer d bir tamkareyse o zaman $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}$'dir ve bu durumda kanıt bir önceki yazıda verildi. Bundan böyle d'nin bir tamkare olmadığını varsayalım.

$A \subseteq \mathbb{Q}[\sqrt{d}]$ çıkarma ve kare alma altında kapalı bir küme olsun. $\alpha, \beta \in A$ olsun. $\alpha\beta$'nın da A'da olduğunu kanıtlayacağız. Önsav'dan dolayı α^2, β^2, $2\alpha\beta \in A$.

Kanıtımız iki adımdan oluşacak: İlki bu iki sayıdan birinin kesirli olduğu, diğeriyse ikisinin de kesirli olmadığı durum.

Birinci Şık. Eğer α ya da β Kesirliyse. α'nın kesirli olduğunu varsayabiliriz. Birbirine asal p ve q tamsayıları için $\alpha = p/q$ yazalım.

Eğer q Tekse. p bir tamsayı olduğundan, $p\beta \in A$. Ama $p\beta = q\alpha\beta$. Demek ki $q\alpha\beta \in A$. Şimdi, q tek olduğundan, $q\alpha\beta$'dan yeterince $2\alpha\beta$ çıkararak $\alpha\beta$'nın A'da olduğunu görürüz.

Eğer q Çiftse. O zaman p bir tek sayıdır ve bir r tamsayısı için $q = 2r$ yazabiliriz. $\alpha \in A$ olduğundan, $\alpha^2 \in A$ ve Önsav'dan dolayı $2\alpha^2\beta \in A$, ve dolayısıyla $r(2\alpha^2\beta) \in A$. Ama $r(2\alpha^2\beta) = 2r\alpha^2\beta = 2r\alpha(\alpha\beta) = p\alpha\beta$. Demek ki $p\alpha\beta \in A$. Burada p tek sayı olduğundan, $p\alpha\beta$'dan yeterinde $2\alpha\beta$ çıkararak $\alpha\beta \in A$ elde ederiz.

İkinci Şık: Eğer α ve β Kesirli Değilse. Bu durumda bir önsava daha ihtiyacımız var:

Önsav. *Eğer* $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$ *kesirli değillerse, o zaman aralarında asal olan öyle* x *ve* y *tamsayıları vardır ki,* $\alpha x + \beta y \in \mathbb{Q}$.

Kanıt: $\alpha = u_1 + u\sqrt{d}$ ve $\beta = v_1 + v\sqrt{d}$ olsun. Burada, $u, u_1, v, v_1 \in \mathbb{Q}$. Birbirine asal olan ve $ux + vy = 0$ eşitliğini sağlayan x ve y tamsayılarını bulmak istiyoruz. u_1, u_2, v_1, v_2 tamsayıları için, $u = u_1/u_2$ ve $v = v_1/v_2$ yazalım. Ayrıca u_1'le u_2'nin ve v_1'le v_2'nin birbirlerine asal olduklarını varsayalım. $\text{ebob}(u_1, v_1) = w_1$ ve $\text{ebob}(u_2, v_2) = w_2$ olsun. $u_1 = w_1r_1$, $v_1 = w_1s_1$, $u_2 = w_2r_2$, $v_2 = w_2s_2$ olsun. Burada, r_i'le s_i birbirlerine asaldır. Ayrıca, u_1'le u_2 ve v_1'le v_2 birbirlerine asal olduklarından r_1'le r_2 ve s_1'le s_2 birbirlerine asaldır. Şimdi $x = r_2s_1$ ve $y = -r_1s_2$ olsun. Söylediklerimizden x'le y'nin birbirlerine asal oldukları çıkar. Şimdi,

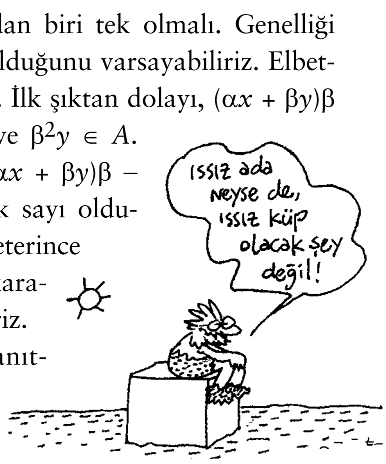
$$ux + vy = \frac{u_1}{u_2}x + \frac{v_1}{v_2}y = \frac{w_1r_1}{w_2r_2}x + \frac{w_1s_1}{w_2s_2}y$$

$$= \frac{w_1r_1}{w_2r_2}r_2s_1 + \frac{w_1s_1}{w_2s_2}(-r_1s_2) = \frac{w_1r_1s_1}{w_2} - \frac{w_1r_1s_1}{w_2} = 0.$$

Böylece önsavımız kanıtlanmış oldu. □

Önsavdaki gibi x ve y sayıları alalım. O zaman $\alpha x + \beta y \in \mathbb{Q} \cap A$. Birbirlerine asal olduklarından x ya da y sayılarından biri tek olmalı. Genelliği bozmadan x'in tek olduğunu varsayabiliriz. Elbette $\alpha x + \beta y \in \mathbb{Q} \cap A$. İlk şıktan dolayı, $(\alpha x + \beta y)\beta \in A$. Ama $\beta^2 \in A$ ve $\beta^2 y \in A$. Dolayısıyla $x\alpha\beta = (\alpha x + \beta y)\beta - \beta^2 y \in A$. Ama x tek sayı olduğundan, $x\alpha\beta$'dan yeterince A'da olan $2\alpha\beta$'yı çıkararak $\alpha\beta \in A$ elde ederiz.

Teoremimiz kanıtlanmıştır. ♠



* Bilkent Üniversitesi Matematik Bölümü 3. sınıf öğrencisi.