18.701 Cebir 1

2007 Güz

Enbüyük Ortak Bölen ve Enküçük Ortak Kat

a ve b iki tamsayı olsun. $a|b$ gösterimi a, b'yi böler anlamına gelir, yani bir r tamsayısı için $b = ra$ olur.

Eğer a bir pozitif tamsayıysa, $\mathbb{Z}a$ gösterimi a sayısının tam katı olan tamsayılar kümesini göstermek için kullanılır; bu kümeyi aynı zamanda a ile bölünen tamsayılar kümesi diye tasvir etmek de mümkündür. $\mathbb{Z}^+$ toplamsal grubunun altgrupları hakkındaki esas teoreme göre $\mathbb{Z}a$ bir altgruptur, ve $\mathbb{Z}^+$ grubunun bariz altgrubu dışındaki her altgrubu yegane bir $a > 0$ için $\mathbb{Z}a$ grubuna eşittir. Üztelik, a bu altgrubun içindeki enküçük pozitif tamsayıdır.

İki pozitif tamsayı a ve b verildiğinde, $\mathbb{Z}a$ ve$\mathbb{Z}b$ altgruplarını kullanarak iki altgrup daha üretebiliriz: *toplam* ve *kesişim*. $\mathbb{Z}a + \mathbb{Z}b$ toplamı $\alpha \in \mathbb{Z}a$ ve $\beta \in \mathbb{Z}$ olmak üzere $\alpha + \beta$ şeklinde yazılan tüm tamsayıların kümesidir. :

$$\mathbb{Z}a + \mathbb{Z}b = \{c \,|\, c = ra + sb \ (r, s \in \mathbb{Z})\} \tag{1}$$

Lemma 1 *(i) $\mathbb{Z}a + \mathbb{Z}b$ ve $\mathbb{Z}a \cap \mathbb{Z}b$ kümeleri $\mathbb{Z}^+$ grubunun altgruplarıdır ve ikisi de $\{0\}$ altgrubu değildir*
(ii) Toplam ve kesişimi üreten d, m pozitif tamsayıları vardır: $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$ ve $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$

Kanıt. (i) şıkkını alıştırma olarak bırakıyoruz. (ii) şıkkı (i)'den çıkar çünkü $\{0\}$ dışındaki her altgrup bir c için $\mathbb{Z}c$ biçimindedir.

$\mathbb{Z}a + \mathbb{Z}b$ altgrubunun üretecine *a ile b'nin enbüyük ortan böleni* ve $\mathbb{Z}a \cap \mathbb{Z}b$ altgrubunun üretecine *a ile b'nin enküçük ortak katı* denir. Bu tamsayılar a ve b tarafından tek bir şekilde belirlenirler ve izleyen önermedeki (i) ve (ii) özellikleriyle karakterize edilirler.

Önerme 2 *a, b, d, m yukarıdaki gibi olsun.*
(i) $a|m$ ve $b|m$. Eğer x tamsayısı için hem $a|x$ hem de $b|x$ ise $x|m$ olur.
(ii) $d|a$ ve $d|b$. Eğer x tamsayısı için hem $x|a$ hem de $x|b$ ise $d|x$ olur.
(iii) $d = ra + sb$ olacak şekilde r ve s tamsayıları vardır.

Kanıt. (i) $m \in \mathbb{Z}a$ olduğundan a, m'yi böler. Benzer şekilde b, m'yi böler. Şimdi $a|x$ ve $b|x$ varsayalım. O takdirde x kesişim kümesi $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$'nin elemanıdır, yani $x \in \mathbb{Z}m \Rightarrow x|m$.
(iii) d sayısı $\mathbb{Z}d$ altgrubunun elemanı ve $\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b$ olduğu için bu şık doğrudur.
(ii) $a = 1a + 0b$ eşitliğinden $a \in \mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$ elde edilir, dolayısıyla $d|a$ bulunur. Benzer şekilde, $d|b$ bulunur. O halde (iii) şıkkındaki gibi $d = ra + sb$ olur. Eğer $x|a$ ve $x|b$ ise $x|ra + sb = d$ elde edilir. □

Not 5. Enbüyük ortak bölenin a ve b'nin doğrusal bileşimi olarak yazılabilmesi çok kuvvetli bir alettir ve gördüğümüz gibi (ii) özelliği bu özellikten çıkar. Enbüyük ortak bölen karşımıza çıktığında hemen (iii) şıkkını uygulayıp ne çıktığına bakmalıdır. Aşağıda sunduğumuz Önerme 7 ve 8'de bu aletin kullanımına iki örnek vereceğiz.

Gösterim 7. Kısaltmaları sevmem, ancak "a ve b'nin enbüyük ortan bölenü" ve "a ve b'nin en küçük ortak katı" ifadeleri sırasıyla ebob(a, b) ve ekok(a, b) biçiminde kısaltılmayı gerektirecek kadar hantallar.

Önerme 8 *a, b pozitif tamsayıları verilsin. Eğer $d = ebob(a, b)$ ve $m = ekok(a, b)$ ise $dm = ab$ olur.*

Kanıt. dm ve ab pozitif tamsayılar olduğundan ab'nin dm'yi böldüğünü ve dm'nin ab'yi böldüğünü göstermek yeterli olur. $d = ra + sb$ yazalım:

$$dm = ram + sbm.$$

m hem a hem b'nin katı olduğundan, bu denklemin sağındaki her iki terim de ab ile bölünür. Öyleyse sol taraf da bölünür ve $ab|dm$ buluruz.

Şimdi, d hem a hem de b'yi böldüğünden $a' = a/d$ ve $b' = b/d$ oranları tamsayılardır. $m' = ab/d = a'b = ab'$ dersek m' hem a hem b ile bölünür, yani $m|m'$ çıkar. Bunu d ile çarparak $dm|ab$ elde ederiz. □

Önerme 9 *a, b iki pozitif tamsayı ve p bir asal olsun. Eğer p asalı ab çarpımını bölerse, p ya a'yı ya da b'yi böler.*

Kanıt. Bir "veyalı" önermeyi doğrudan ispatlamaya çalışmak biraz garip, bu nedenle simetriyi kıralım. p asalının ab çarpımını böldüğünü ancak a'yı bölmediğini varsayıp b'yi böldüğünü gösterelim. Bu önermeyi kanıtlamak için yeterli olur.

a ve p'nin en büyük ortak böleni δ nedir? p'nin pozitif bölenleri sadece 1 ve p'dir. Yani $\delta = 1$ veya $\delta = p$ olabilir. Ancak δ aynı zamanda a'ı da böler ve varsayımımıza göre p asalı a'yı bölmez. Dolayısıyla $\delta = 1$ olmalı. Önerme 4(iii)'den $ra + sp = \delta = 1$ olacak şekilde r, s tamsayıları bulunur. Bu eşitliğin her iki tarafını da b ile çarparak $bra + bsp = b$ elde edilir. Eşitliğin sol tarafındaki her iki terim de p ile bölünür, ve iddia edildiği gibi b de p ile bölünür. □

Enbüyük ortak bölen ve enküçük ortak kat a ve b'nin asal çarpanlarına ayrışımından bulunabilir. $p_1, \ldots, p_k$ asallar ve $r_i, s_i \geq 0$ için $a = p_1^{r_1} \cdots p_k^{r_k}$ ve $b = p_1^{s_1} \cdots p_k^{s_k}$ olsun. max_i ve min_i ile r_i ve s_i sayılarının büyüğünü ve küçüğünü gösterelim (eşit olabilirler). İzleyen önermenin kanıtı bir alıştırmadır:

Önerme 10 *Yukarıdaki gösterimler altında $ebob(a, b) = p_1^{min_1} \cdots p_k^{min_k}$ ve $ekok(a, b) = p_1^{max_1} \cdots p_k^{max_k}$ olur.* □

Alıştırmalar.

1. $d = ra + sb$ sayısı Önerme 4(iii)'deki gibiyse, $d = r_1 a + s_1 b$ şeklindeki tüm r_a, s_1 tamsayılarını tasvir edin.

2. a, b pozitif tamsayıları verilsin ve $d = \text{ebob}(a, b)$, $m = \text{ekok}(a, b)$ olsun. p bir asal olsun ve $a' = a$, $b' = bp$, $d' = \text{ebob}(a', b')$, $m' = \text{ekok}(a', b')$ olsun. Bu takdirde ya $d' = d$ ve $m' = mp$ ya da $d' = dp$ ve $m' = m$ olabileceğini gösterin. Her bir ihtimalin hangi şartlarda gerçekleştiğini açıklayın.

3. a, b, c pozitif tamsayıları verilsin ve $a' = ac$ ve $b' = bc$ olsun. Bir önceki alıştırmadaki gösterimle $d' = dc$ ve $m' = mc$ olduğunu gösterin.

4. Önerme 9'u kanıtlayın.