18.701 Algebra I

2007 Güz

Tamsayıların Kalandaşlığı

Kalandaşlık üzerinde çok az duracağız; bu kısa özetten amacımız, konuyu kısaca gözden geçirmektir.

Bir p asalı sabitleyip, $\mathbb{Z}^+$ grubunun $p\mathbb{Z}$ altrgubunu H ile gösterelim.

• Eğer a, b iki tamsayıysa ve $a - b$ farkı p ile bölünürse *a mod p'de b'yle kalandaştır.*

Eğer a, b'yle kalandaşsa $a \equiv b$ yazılır ve gerektiğinde "mod p" ibaresi eklenir. Kalandaşlık bir denklik bağıntısıdır. Kalan sınıfları tamsayılar kümesini paylar (ayrık parçalara böler).

• Bir tamsayının kalan sınıfı $\overline{a} = a + H$ eşkümesidir.

Her kalan sınıfı $0 \leq r < p$ şeklinde tek bir r tamsayısı barındırır. Kalan sınıflarının oluşturduğu küme için kabul görmüş iki gösterim vardır:

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}.$$

• Eğer $a \equiv a'$ ve $b \equiv b'$ ise $a + b \equiv a' + b'$ $ab \equiv a'b'$ ve $-a \equiv -a'$ olur.

Buradan kalan sınıflarında çıkarma toplama ve çarpma işlemlerinin tamsayılardaki toplama ve çarpma işlemleri kullanılarak yapılabileceği çıkar:

$$\overline{a} + \overline{b} = \overline{a+b}\ ,\ -\overline{a} = \overline{-a}\ ,\ \overline{a}\overline{b} = \overline{ab}.$$

Birleşme, değişme, dağılma gibi özellikler kalan sınıfları için de geçerlidir.

Eğer $a \equiv a'$ ve $b \equiv b'$ ise $ab \equiv a'b'$ olduğunu gösterelim. Eğer $a - a'$ ve $b - b'$ farkları p asalıyla bölünürse $ab - a'b'$ farkınında p asalıyla bölüneceğini göstermeliyiz. Biraz denemeyle bulunan $ab - a'b' = (a - a')b' + a(b - b')$ eşitliğinden bu çıkar.

Şimdi kalan sınıflarını gerçekten ilginç kılan ve p sayısının asallığının elzem olduğu vakayı inceleyelim.

• $\overline{0}$ dışındaki her $\overline{a}$ kalan sınıfının çarpmaya göre tersi vardır.

Dört işlem $(+, -\times, \div)$ altında kapalı olduğundan, $\mathbb{F}_p$ bir *cisimdir*. Sıfır dışındaki kalan sınıflarının kümesi $\mathbb{F}_p^\times = \mathbb{F}_p \backslash \{\overline{0}\}$, çarpma işlemi altında $p - 1$ mertebeli bir grup oluşturur.

Sıfır dışındaki kalan sınıflarının tersinir olması *sadeleştirme* kuralının bir sonucudur:

• Eğer $\overline{a} \neq \overline{0}$ ise $\overline{a}\overline{b} = \overline{ac} \Rightarrow \overline{b} = \overline{c}$.

Kanıt. $\overline{ac}$ terimini sol tarafa geçirelim ve $\overline{d} = \overline{b} - \overline{c}$ diyelim. Bu takdirde göstermemiz gereken şey: Eğer $\overline{a} \neq \overline{0}$ ve $\overline{a}\overline{d} = 0$ ise $\overline{d} = \overline{0}$ olur. Bunu kalandaşlık cinsinden okursak, eğer a, d tamsayılarsa, $ad \equiv 0$ ve $a \not\equiv$ ise $d \equiv 0$ olur. Bir başka deyişle; eğer p, ad'yi böler ama a'yı bölmezse o zaman p, d'yi böler. Bu enbüyük ortak bölenler hakkındaki ders notunda ispatlanmıştı. □

Şimdi çarpmaya göre tersin var olduğunu gösterelim. $\overline{a}$ sıfırdan farklı bir kalan sınıfı olsun. Bu sınıfın kuvvetlerinden oluşan diziyi ele alalım:

$$\overline{a},\ \overline{a}^2,\ \overline{a}^3,\ \ldots$$

Kalan sınıfları sonlu sayıdadır ve bu yüzden dizide yineleme bulunmalıdır. Yani $\overline{a}^i = \overline{a}^j$ olacak şekilde $i < j$ pozitif tamsayıları bulunur. $\overline{a}^i$ ile sadeleştirme yaparsak $r = j - i$ olmak üzere $\overline{1} = \overline{a}^r$ elde ederiz. O halde $\overline{a}^{r-1}$ sınıfı $\overline{a}$ sınıfının tersi olur. □

• Örnek: $p = 13$ dersek $\overline{2}$'nin kuvvetleri

$$\overline{2}^1 = \overline{2}, \quad \overline{2}^2 = \overline{4}, \quad \overline{2}^3 = \overline{24} = \overline{8}, \quad \overline{2}^4 = \overline{16} = \overline{3}, \quad \overline{2}^5 = \overline{6}, \quad \overline{2}^6 = \overline{12},$$
$$\overline{2}^7 = \overline{11}, \quad \overline{2}^8 = \overline{9}, \quad \overline{2}^9 = \overline{5}, \quad \overline{2}^{10} = \overline{10}, \quad \overline{2}^{11} = \overline{7}, \quad \overline{2}^{12} = \overline{1}.$$

şeklinde yazılır ve $\overline{2}$'nin tersi $\overline{2}^{11} = \overline{7}$ elde edilir. Bunu tahminle daha kolay bulabilirdik, kuvvetleri hesaplamamın sebebi daha ilginç birşeye dikkat çekmek: $\overline{2}$ elemanının $\mathbb{F}_3^\times$ grubundaki mertebesi 12 eder. Bu grup da 12 mertebeli olduğundan, grubun devirli olduğunu ve $\overline{2}$ kalan sınıfı tarafından üretildiğini görürüz.

• Bir başka örnek: $p = 7$ dersek $\overline{2}^2 = 4$, $\overline{2}^3 = \overline{8} = \overline{1}$ elde ederiz. Mertebesi 3 olduğundan $\overline{2}$ elemanı $\mathbb{F}_7^\times$ grubunu üretmez. Öte yandan,

$$\overline{3}^1 = \overline{3}, \quad \overline{3}^2 = \overline{2}, \quad \overline{3}^3 = \overline{6}, \quad \overline{3}^4 = \overline{4}, \quad \overline{3}^5 = \overline{5}, \quad \overline{3}^6 = \overline{1}$$

olduğundan, $\mathbb{F}_7^\times$ mertebesi 6 olan bir devirli gruptur ve $\overline{3}$ sınıfı tarafından üretilir.

Aslında her p asalı için $\mathbb{F}_p^\times$ devirli bir gruptur. Bunun kanıtı, çarpımsal grup hakkındaki ders notunda bulunabilir.