18.701 Cebir 1

2007 Güz

Mod p tamsayıların çarpım grubu

1 Abelyen bir grupta elemanların mertebesi

Bu ders notu boyunca p bir asal sayıdır.

Lemma 1.1 *Bir grubun sonlu a mertebeli bir x elemanı, k bir tamsayı ve $u = x^k$ olsun.*
(i) u elemanının mertebesi a'yı böler
(ii) Eğer k ve q çarpımları a eden iki tamsayıysa u elemanının mertebesi q eder.
(iii) $u = 1$ olması için a'nın k'yı bölmesi gerekir ve yeter. □

Teorem 1.2 *(i) Abelyen bir grubun sırasıyla a, b mertebeli x, y elemanları olsun. a ve b'nin en küçük ortak katı m olsun. O halde G grubunda m mertebeli bir z elemanı bulunur.*
(ii) G bir sonlu abelyen grup ve G'nin elemanlarının enbüyük derecesi m olsun. G'nin her elemanının derecesi m'yi böler.

Bu teoremde G'nin abelyenliğinden vazgeçilemez. Simetrik grup S_3 abelyen değildir, 2inci ve 3üncü mertebeden elemanları vardır ancak 6ncı mertebeden elemanı yoktur.

Kanıt. (ii) kısmı (i) kısmından tümevarımla çıkar. (i) kısmını kanıtlamak için şu lemmayı kullanırız:

Lemma 1.3 *İki a, b tamsayısı verilsin, ekok$(a, b) = m$ ve ebob$(a, b) = d$ olsun. O halde ekok$(a_1, b_1) = m$ ve ebob$(a, b) = 1$ olacak şekilde a ve b'nin sırasıyla a_1 ve b_1 bölenleri vardır.*

Kanıt. Eğer $d = 1$ ise $a_1 = 1$ ve $b_1 = b$ alırız. O halde $d > 1$ varsayalım ve d sayısını bölen bir p asalı seçelim. $d = pd'$, $a = pa'$ ve $b = pb'$ olsun. a, b çiftini a', b veya a, b' çiftlerinden biriyle değiştirerek ilerleyebileceğimizi gösterelim.

Hem a' hem de b, d' ile bölündüğünden ebob$(a', b) = \delta$ sayısı da d' ile bölünür. Hem a hem de b, δ ile bölündüğünden ebob$(a, b) = d$ sayısı da δ ile bölünür. Ancak $d = pd'$ ve p asal olduğundan, δ ya d' ya da d sayısına eşittir. Benzer şekilde ebob(a, b') ya d' ya da d sayısına eşittir.

Şimdi a' ve b' aynı anda d ile bölünemez. Bölünseydi a ve b aynı anda pd ile bölünürdü, ama bu ebob$(a, b) = d$ ile çelişir. d ile bölünmez olan a' olsun. O halde ebob$(a', b) = d'$ olur. $a'b = d'm$ olduğundan, ekok$(a', b) = m$ elde edilir. a ve b çifti ile a' ve b çiftinin yerini değiştirelim. Sonuçta en büyük ortak bölen küçülürken en küçük ortak kat m kalır. Tümevarımla kanıt tamamlanır. □

Şimdi Teorem 1.2(i) kısmının kanıtını bitirelim. a_1 ve b_1 lemmadaki gibi olsun, mesela $a = ra_1$, $b = sb_1$ diyelim. x ve y sayılarını sırasıyla $x_1 = x^r$ ve $y_1 = y^s$ kuvvetleriyle değiştirelim. Lemma 1.1'e göre x_1 ve y_1 sayılarının mertebesi a_1 ve b_1 olur. Böylece a ve b çiftinin aralarında asal olma durumuna indirgendik: ebob$(a, b) = 1$. Bu durumda xy çarpımının m mertebeli olduğunu göstereceğiz.

$z = xy$ sayısının mertebesi k olsun. G değişmeli olduğundan, $x^k y^k = z^k = 1$ elde ederiz. $u = x^k = y^{-k}$ olsun. O halde u elemanının mertebesi hem a hem de b sayısını

böler. a ve b aralarında asal olduğundan u elemanının mertebesi 1 olur, yani $u = 1$ buluruz. Böylece $x^k = 1$ olur, yani x'in mertebesi a, k'yı böler. Benzer şekilde b, k'yı böler. Sonuçta m, k'yı böler. Öte yandan a ve b, m'yi böldüğünden $x^m = 1$ ve $y^m = 1$ olur ve k'nın da m'yi böldüğü çıkar. Yani iddia edildiği gibi $m = k$ olur. □

2 Bir polinomun mod p'de kökleri

Bir $f(x)$ tam polinomu (katsayıları tamsayı olan polinom) verilsin verilsin ve a bir tamsayı olsun. Bölme algoritmasını $f(x)$ polinomunu $x - a$ ile bölmek için uygularsak $f(x) = (x - a)q(x) + r$ elde ederiz. Bölme algoritması $q(x)$ tam polinomu ile sonuçlandığını gösterebilirsiniz zira $x - a$ monik (başkatsayısı 1 olan) bir tam polinomdur. Üstelik, $x = a$ koyarak $r = f(a)$ eşitliği görülür. Böylece

$$f(x) - f(a) = (x - a)q(x) \tag{2.1}$$

elde ederiz.

Netice 2.2 *$f(x)$ bir tam polinom ve a bir tamsayı olsun. (2.1) eşitliğini sağlayan yegane $q(x)$ tam polinomu vardır.* □

Netice 2.3 *$f(x)$ bir tam polinom ve a, a' iki tamsayı olsun. Eğer $a \equiv a' \pmod p$ ise, $f(a) \equiv f(a') \pmod p$ olur.*

Kanıt. Formül (2.1) içinde $x = a'$ koyarak görülür. □

Netice (2.3) bir $f(x)$ tam polinomunun mod p'de köklerinden sözetmemize izin verir. Eğer $f(a) \equiv 0 \pmod p$ ise a tamsayısının mod p denklik sınıfı $\overline{a}$, *f(x)'in mod p'de bir köküdür* denir. Bu durumda, eğer $a \equiv a' \pmod p$ ise $f(a') \equiv 0$ eşitiği de geçerlidir.

Lemma 2.4 *Bir $f(x)$ tam polinomunun derecesi d olsun. $f(x)$'in (mod p) kökü olan denklik sınıflarından en çok d adet vardır.*

Polinomların gelişigüzel bir cisimdeki köklerinin adedi için Lemma 2.4'e benzer bir sonuç geçerlidir ancak sunumu yeni terminoloji gerektirdiğinden bunu erteliyoruz.

Kanıt. d üzerinde tümevarım uygulayalım. a, b iki tamsayı olsun ve $\overline{a}, \overline{b}$ denklik sınıfları $f(x)$'in (mod p) kökleri olsun. $a \not\equiv b (\mathrm{mod} p)$ varsayalım. (2.1)'de $x = b$ koyarak $f(b) - f(a) = (b - a)q(b)$ elde edelim. $f(b) \equiv 0$ ve $f(a) \equiv 0$, ama $b - a \not\equiv 0$ olduğundan $q(b) \not\equiv 0$ çıkar. Yani $\overline{b}$ denklik sınıfı $q(x)$ polinomunun mod p köküdür. Bu $\overline{a}$'dan farklı tüm mod p kökler için doğrudur.

$q(x)$'in derecesi $d - 1$ olduğundan, tümevarım hipotezine göre mod p'de ençok $d - 1$ adet kökü vardır. Yani $f(x)$'in mod p'de $\overline{a}$'dan farklı ençok $d - 1$ adet kökü vardır, ve $\overline{a}$'yı da sayarsak toplam ençok d adet kökü vardır. □

3 Çarpımsal grubun yapısı

Teorem 3.1 *Asal bir p tamsayısı olsun. Sıfır dışındaki mod p denklik sınıflarının $F^\times$ çarpımsal grubu $p-1$ mertebeli bir devirli gruptur.*

Bu grubun bir üretecine *ilkel eleman* denir.

Örnekler 3.2. $p = 7$ içim sıfır dışındaki altı denklik sınıfı: $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$ olur. $x = \overline{3}$ için

$$x^0 = \overline{1},\ x^1 = \overline{3},\ x^2 = \overline{2},\ x^3 = \overline{6},\ x^4 = \overline{4},\ \text{ ve } x^5\overline{5},$$

olduğundan x bir ilkel elemandır ve $F^\times$ mertebesi 6 olan devirsel gruptur.

$p = 11$ için sıfır dışında on denklik sınıfı vardır. $x = \overline{2}$ için

$$x^0 = \overline{1},\ x^1 = \overline{2},\ x^2 = \overline{4},\ x^3 = \overline{8},\ x^4 = \overline{5},\ x^5 = \overline{10},\ x^6 = \overline{9},\ x^7 = \overline{7},\ x^8 = \overline{3},\ \text{ ve } x^9 = \overline{6}$$

olduğundan x bir ilkel elemandır ve $F^\times$ mertebesi 10 olan devirsel gruptur.

Teorem 3.1'in kanıtı. $F^\times$ grubunun elemanlarının enbüyük mertebesi m olsun. Teorem 1.2 bize $F^\times$ içindeki her $\overline{a}$ elemanının mertebesinin m'yi böldüğünü söyler, yani $\overline{a}^m = 1$ olur. Üstelik, m bir elemanın mertebesi olduğundan, $F^\times$ grubunun mertebesini de böler.

Şimdi yapılacak önemli bir gözlem var: Eğer $\overline{a}$ gelişigüzel bir $F^\times$ elemanıysa, $\overline{a}^m = 1$ eşitliği yüzünden $\overline{a}$, $x^m - 1$ polinomunun bir mod p köküdür (!). Lemma 2.4 bize $x^m - 1$ polinomunun ençok m adet mod p kökü olduğunu söyler. Yani $F^\times$ grubunda ençok m eleman olabilir: $p - 1 \leq m$. Ancak m'nin $p-1$'i böldüğünü görmüştük. Buradan $m = p - 1$ çıkar. $F^\times$ grubu m mertebeli bir eleman içerdiğinden, devirli bir gruptur.□

Hangi elemanların ilkel eleman olduğuna karar vermenin kolay bir yolunun bu kanıtta verilmediğini kaydedelim. Genel bir p asalı için, bu zor bir sorudur.