5. ELİPTİK EĞRİLER

5.1. Eliptik Eğrilere Giriş

Eliptik eğriler, iki değişkenli kübik bir denklemi sağlayan noktalar kümesidir. Bu bölümde eliptik eğrilerin bazı özellikleri incelenecek ve eğri üzerindeki noktalar için bir toplama kuralı tanımlanacak öyle ki bu noktaların kümesi bir grup oluşturacak.

K bir cisim olsun. a, b, c, d, e, x ve $y \in K$ olmak üzere K cismi için eliptik eğrinin genel denklemi

$$y^2 + axy + by = x^3 + cx^2 + dx + e \quad \text{dir.}$$

Eliptik eğrinin genel denklemi afin dönüşümler kullanılarak,

eğer $char(K) = 2$ ise

$$y^2 + ay = x^3 + bx + c \quad \text{veya} \quad y^2 + xy = x^3 + ax^2 + b \ ,$$

eğer $char(K) = 3$ ise

$$y^2 = x^3 + ax^2 + bx + c$$

formundaki denkleme dönüşür.

Aynı şekilde, eğer $char(K) \neq 2, 3$ ise eliptik eğri denklemi

(5.1.1.) $$y^2 = x^3 + ax + b$$

denklemine dönüşür. (5.1.1.) denklemli eliptik eğriyi E ile gösterelim.

Esas olarak $char(K) \neq 2$, 3 olan cisimlerle ilgileneceğimizden, eliptik eğri denklemi olarak (5.1.1.) numaralı denklemi kullanacağız.

$f(x) := x^3 + ax + b$ olsun. r_1, r_2 ve r_3 $f(x) = 0$ denkleminin kökleri ise f polinomunun diskriminantı

$$\Delta(f) := (r_1 - r_2)^2(r_2 - r_3)^2(r_1 - r_3)^2 \text{ dir.}$$

f polinomunun diskriminantını katsayılar cinsinden $\Delta(f) = 4a^3 + 27b^2$ şeklinde yazabiliriz. $f(x)$ polinomunun katlı kökünün olup olmadığı polinomun diskriminantına bakılarak belirlenebilir. Eğer $\Delta(f) \neq 0$ ise f polinomunun katlı kökü yoktur.

$y^2 = f(x)$ denklemli bir eliptik eğrinin diskriminantı sıfırdan farklı ise eliptik eğri tekil olmayan (nonsingular) eliptik eğri olarak adlandırılır.

Eliptik eğri üzerindeki noktaların bir grup oluşturabilmesi için sonsuzdaki nokta olarak adlandırılacak bir noktaya daha ihtiyacımız olduğundan sonsuzdaki noktanın tanımını yapalım.

$K^3 - \{(0,0,0)\}$ kümesi üzerinde aşağıdaki şekilde tanımlanan bağıntı bir denklik bağıntısıdır.

$\forall\, (X_1, Y_1, Z_1), (X_2, Y_2, Z_2) \in K^3 - \{(0,0,0)\}$ için

$$\text{Eğer } (X_1, Y_1, Z_1) = t(X_2, Y_2, Z_2) \text{ olacak şekilde bir } t \in K \text{ varsa}$$
$$(X_1, Y_1, Z_1) \equiv (X_2, Y_2, Z_2) \text{ dir.}$$

Bu denklik bağıntısından oluşan denklik sınıflarının kümesine projektif düzlem denir ve $\mathcal{P}^2(K)$ ile gösterilir. $\mathcal{P}^2(K)$ nın elemanlarına da projektif noktalar denir ve $(X : Y : Z)$ ile gösterilir.

$\mathcal{P}^2(K)$ dan herhangi bir $(X : Y : Z)$ noktasını alalım. Eğer $Z \neq 0$ ise $x := X/Z$ ve $y := Y/Z$ olmak üzere $(X : Y : Z) = (x : y : 1)$ dir. Bu durumda $\mathcal{P}^2(K)$ nın $(x : y : 1)$ şeklindeki elemanları K^2 nin elemanlarıyla 1-1 eşlenebilir. $\mathcal{P}^2(K)$ nın $(x : y : 0)$ şeklindeki noktalarına da sonsuzdaki noktalar denir. Böylece

$$\mathcal{P}^2(K) = K^2 \cup \{(x : y : 0) \mid x, y \in K\}$$

şeklinde düşünebiliriz.

Şimdi, E eliptik eğrisinin sonsuzdaki noktalarını belirleyelim. $f(x, y)$ katsayıları K cisminden alınan iki değişkenli bir polinom olmak üzere afin düzlemdeki $f(x, y) = 0$ eğrisini, $x := X/Z$ ve $y := Y/Z$ dönüşümleri ve Z nin yeterince büyük bir üssü ile çarparak $\mathcal{P}^2(K)$ de bir eğri olarak düşünebiliriz. (5.1.1.) denkleminde $x := X/Z$ ve $y := Y/Z$ dönüşümlerini yapıp denklemin her iki tarafını Z^3 ile çarparsak projektif düzlemde

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

denklemini elde ederiz. Diğer bir deyişle, $\mathcal{P}^2(K)$ projektif düzleminde

$$E^* := \{(X : Y : Z) \mid X, Y, Z \in K \text{ ve } Y^2Z = X^3 + aXZ^2 + bZ^3\} \text{ dir.}$$

$(X : Y : Z) \in E^*$ olsun. $Z = 0$ ise $X = 0$ dır. Dolayısıyla, X, Y ve Z nin her üçü birden sıfır olamayacağından $Y = 1$ dir. Yani, E^* daki sonsuzdaki nokta

sadece $(0:1:0)$ dır. $(0:1:0)$ noktasını ϑ sembolü ile gösterelim. ϑ noktasını y ekseni üzerinde ve orjinden sonsuz uzaklıktaki bir nokta olarak düşünebiliriz.

Tanım 5.1.1.

K bir cisim, $char(K) \neq 2, 3$ ve $\Delta(f) \neq 0$ olmak üzere,

$$y^2 = x^3 + ax + b \qquad , \qquad a \text{ ve } b \in K$$

denklemli E eliptik eğrisindeki $(x, y) \in K \times K$ noktaları ve sonsuzdaki noktanın oluşturduğu kümeye K cismi üzerindeki eliptik eğri denir ve $E(K)$ ile gösterilir.

Şimdi, $E(K)$ bir grup olacak şekilde $E(K)$ üzerinde bir toplama işlemi tanımlayacağız. Bu toplama işlemini daha iyi anlayabilmek için öncelikle $E(\mathbb{R})$ üzerinde tanımlayalım.

5.2. Reel Sayılar Üzerindeki Eliptik Eğriler

$\mathbb{R}$ reel sayılar olmak üzere Tanım 5.1.1.de $K = \mathbb{R}$ alalım.

Eliptik eğrideki reel noktalar üzerinde grup kuralı doğruların kübik eğriyle kesişmesi kullanılarak tanımlanır.

P,$Q \in E(\mathbb{R})$ olsun. $E(\mathbb{R})$ üzerindeki toplama kuralı şu şekilde tanımlanır :

(1) Eğer $P = \vartheta$ ise $-P := \vartheta$ ve $P+Q := Q$ olarak tanımlanır. Yani, sonsuzdaki noktayı grubun etkisiz elemanı olarak seçeceğiz.

(2) $P, Q \neq \vartheta$ olsun.

(2a) $\forall P = (x, y) \in E(\mathbb{R})$ için $-P$ noktasını P ve ϑ noktalarından geçen doğrunun eliptik eğriyle kesiştiği 3. nokta olarak tanımlayalım (P noktasından geçen dikey doğru). Yani, $-P := (x, -y)$ dir. $-P$ noktasını

$$y^2 = x^3 + ax + b$$

denkleminde yerine yazarsak $(-y)^2 = x^3 + ax + b$ ifadesini elde ederiz. $y^2 = (-y)^2$ ve $P \in E(\mathbb{R})$ olduğundan $-P \in E(\mathbb{R})$ dir.

(2b) $P = (x_1, y_1)$ ve $Q = (x_2, y_2)$ eliptik eğri üzerindeki iki farklı nokta olsun. P ve Q noktalarından geçen l doğrusu eliptik eğriyi üçüncü bir R noktasında keser. Bu durumda, $P + Q := -R$ olarak tanımlanır (Şekil 5.1.).

(2c) $P = Q$ ise l, Eliptik eğriye P noktasındaki teğet dogrusu ve R, teğet doğrusu ve eliptik eğrinin kesiştikleri ikinci nokta olmak üzere $P + Q := -R$ olarak tanımlanır (Şekil 5.3.).

Not : $\Delta(f) = 0$ durumunda eliptik eğri üzerindeki bazı noktalar için teğet doğrusu tanımlı olmayacağından $E(\mathbb{R})$ bir grup oluşturmaz.

$E(\mathbb{R})$ tanımlanan toplama kuralına göre değişmeli bir grup oluşturur. Şimdi, toplama kuralının cebirsel formülünü elde ederken aynı anda P ve Q noktalarından geçen l doğrusunun eliptik eğriyi reel sayı olan üçüncü bir noktada daha kestiğini gösterelim.

$P = (x_1, y_1)$ ve $Q = (x_2, y_2)$ eliptik eğri üzerindeki iki farklı nokta ve $P + Q := (x_3, y_3)$ ise $-(P + Q) = (x_3, -y_3)$ dir. $-(P + Q)$ noktası P ve Q noktalarından geçen doğrunun eliptik eğriyle kesiştiği 3. nokta olarak tanımlanır. Bu iki noktadan geçen doğrunun denklemi $m = (y_2 - y_1)/(x_2 - x_1)$ olmak üzere

$$y - y_1 = m(x - x_1) \text{ dir.}$$

Doğru ve eliptik eğrinin kesiştikleri 3. noktayı ($-(P+Q)$ noktasının koordinatları) bulmak için eliptik eğri denklemindeki y değişkeni yerine doğru denklemi yazılırsa,

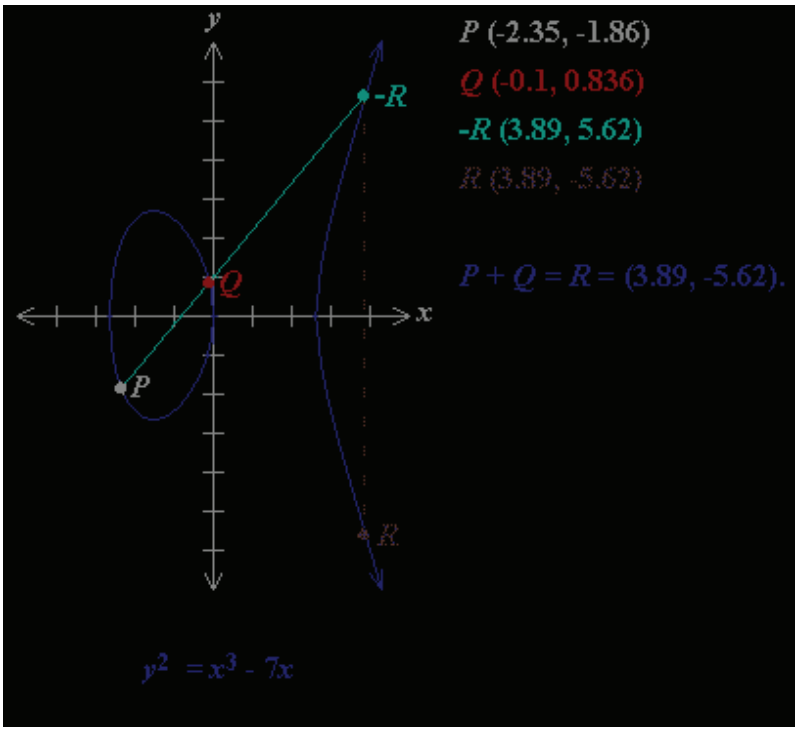
$$m^2(x-x_1)^2 + 2m(x-x_1)y_1 + y_1^2 = x^3 + ax + b$$
$$x^3 - m^2x^2 + (b_1)x + (c_1) = 0$$

Not : b_1 ve c_1 a, b, m, x_1 ve y_1 terimlerini içeren ifadelerdir.

Sonuç olarak, kökleri x_1, x_2 ve x_3 olan kübik bir denklem elde edilir. x^2 li terimin katsayısı $-(x_1+x_2+x_3)$ olacağından

$$x_1 + x_2 + x_3 = m^2 \quad \text{yani,} \quad x_3 = m^2 - x_1 - x_2 \text{ dir.}$$

Doğru denkleminden $y_3 = -(m(x_3 - x_1) + y_1)$ olarak bulunur. Böylece $P+Q$ toplamının koordinatları (x_3, y_3) noktasıdır (Şekil 5.2.1).



Şekil 5.2.1. $P \neq Q$ için $P + Q = R$ toplamının geometrik gösterimi

$P = Q$ durumunda eliptik eğri üzerindeki 2. kesişme noktasını bulmak için $P = (x_1, y_1)$ noktasında eliptik eğriye teğet doğrusu çizilir. Teğet doğrusunun eğimi türevle de bulunabilir :

$$2y\frac{dy}{dx} = 3x^2 + a$$

yani, teğet doğrusunun P noktasındaki eğimi :

$$m = \frac{3x_1^2+a}{2y_1} \qquad \text{dir.}$$

$y_1 \neq 0$ kabul edilip, teğet doğrusu ve eliptik eğri ortak çözülürse:

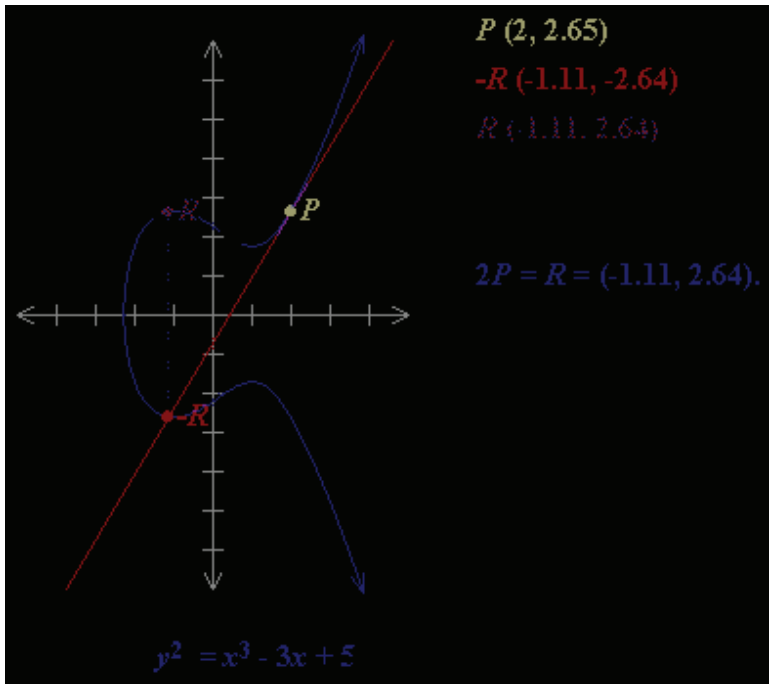
$$x^3 - m^2x^2 + b_1x + c_1 = 0$$

denklemi elde edilir. Bu denklem x_1 noktasında çift kat köke sahiptir. Eğer (x_3, y_3) noktası eliptik eğri ve teğet doğrusunun 2. kesişme noktası ise x^2 li terimin katsayısı $-(2x_1 + x_3)$ olmalıdır. Böylece,

$$2x_1 + x_3 = -(-m^2) \quad \text{veya} \quad x_3 = m^2 - 2x_1 \text{ dir.}$$

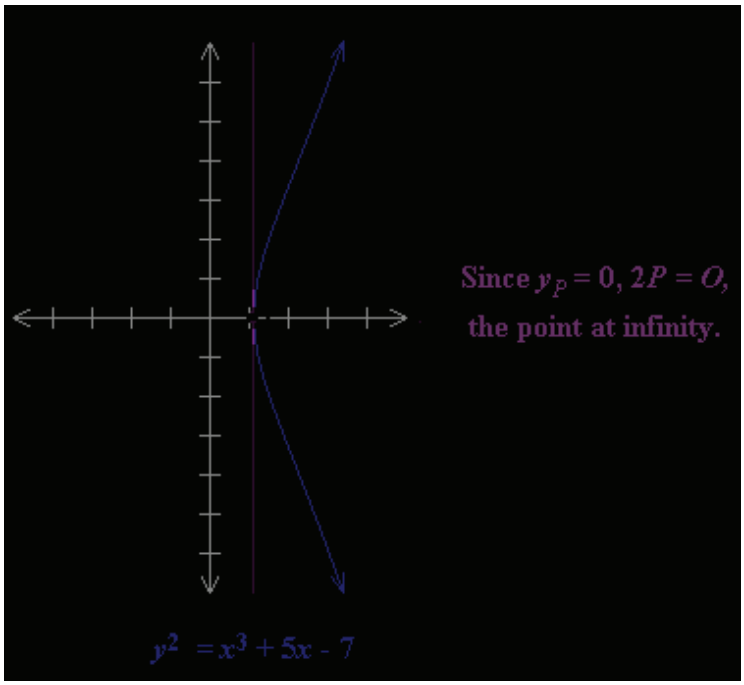
$y_3 = -(m(x_3 - x_1) + y_1)$ koordinatı doğru denkleminden bulunabilir.

Sonuç olarak, $P + P = 2P = (x_3, y_3)$ dür. (Şekil 5.2.2).



Şekil 5.2.2. $P = Q$ için $P + Q = R$ toplamının geometrik gösterimi

$y_1 = 0$ olduğunda ise teğet doğrusu dikey olur. Bu durumda 3. kesişme noktası sonsuzdaki noktadır (Şekil 5.2.3.).



Şekil 5.2.3. $P = Q$ ve $y_1 = 0$ için $P + Q = R$ toplamının geometrik gösterimi

Tanımladığımız toplama işlemini özetlersek :

$P = (x_1, y_1)$ ve $Q = (x_2, y_2)$ sonsuzdaki noktadan farklı eliptik eğri üzerindeki herhangi iki nokta olsun:

(1) Eğer $x_1 = x_2$ ve $y_1 = y_2 = 0$ ise $P + Q := \vartheta$

(2) Eğer $x_1 = x_2$ ve $y_1 \neq y_2$ ise $P + Q := \vartheta$

(3) Diğer durumlarda, $P + Q = (x_3, y_3)$ olsun.

Eğer $P = Q$ ise

$$m := \frac{(y_2 - y_1)}{(x_2 - x_1)}$$

aksi halde;

$$m := \frac{\left(3x_1^2+a\right)}{(2y_1)}$$

olmak üzere

$$x_3 := (m^2 - x_1 - x_2\,) \qquad \text{ve} \qquad y_3 := (m(x_1 - x_3) - y_1) \text{ dir.}$$