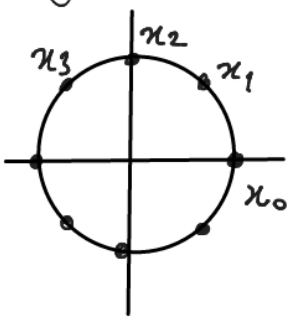
ÖRNEK. $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ cisminin ($\mathbb{Q}$ yu sabit birakan) otomorfizmalar grubunu belirleyelim.

$\sqrt[3]{2}$ nin eslenikleri : $\sqrt[3]{2},\ w\sqrt[3]{2},\ w^2\sqrt[3]{2}$ $\left(w = \frac{-1+i\sqrt{3}}{2}\right)$

$i\sqrt{3}$ ün " : $i\sqrt{3}$ ve $-i\sqrt{3}$

$$\sqrt[3]{2} \to \begin{cases} \sqrt[3]{2}, i\sqrt{3} \to \begin{cases} \sqrt[3]{2}, i\sqrt{3} \\ \sqrt[3]{2}, -i\sqrt{3} \end{cases} \\ w\sqrt[3]{2}, i\sqrt{3} \to \begin{cases} w\sqrt[3]{2}, i\sqrt{3} \\ w\sqrt[3]{2}, -i\sqrt{3} \end{cases} \\ w^2\sqrt[3]{2}, i\sqrt{3} \to \begin{cases} w^2\sqrt[3]{2}, i\sqrt{3} \\ w^2\sqrt[3]{2}, -i\sqrt{3} \end{cases} \end{cases} \cong S_3$$

ÖRNEK. $\mathbb{Q}(\sqrt[3]{2})$ nin $\mathbb{Q}$ yu sabit birakan oto. grubu $\{e\}$ dir.



ÖRNEK. $C = \mathbb{Q}(\sqrt[8]{3}, i) \Rightarrow G(C/\mathbb{Q}) = ?$

$x^8 - 3 = 0 \Rightarrow x_k = 3^{1/8} e^{i\frac{2k\pi}{4}} \quad k = 0,1,\ldots,7$

$x_0 = 3^{1/8} \quad x_1 = 3^{1/8}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) \notin C, \quad x_2 = i3^{1/8}$

$3^{1/8}$ in C içine düşen eslenikleri : $3^{1/8}, i3^{1/8}, -3^{1/8}, -i3^{1/8}$

$$3^{1/8} \to \begin{cases} 3^{1/8}, i \to \begin{cases} i \\ -i \end{cases} \\ i3^{1/8}, i \to \begin{cases} i \\ -i \end{cases} \\ -3^{1/8}, i \to \begin{cases} i \\ -i \end{cases} \\ -i3^{1/8}, i \to \begin{cases} i \\ -i \end{cases} \end{cases}$$

$$K = \{ c \in C : \forall \sigma \in G(C/\mathbb{Q}) \text{ için } \sigma(c) = c \}$$

sabit cisim $\Rightarrow K = ?$

$3^{1/2} = (3^{1/8})^4 \in C$ Aslında $3^{1/2} \in K$.

$\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{3}) \subseteq K \qquad \mathbb{Q} \neq K.$

Aslında $\underline{K = \mathbb{Q}(\sqrt{3})}$

K dan bir eleman alsak bu eleman

$1, 3^{1/8}, 3^{1/4}, 3^{1/2}, i, i3^{1/8}, i3^{1/4}$ ve $i3^{1/2}$ elemanlarının $\mathbb{Q}$ üzerindeki bir doğrusal kombinasyonudur. Burada sadece $3^{1/2}$ sabit kaldığından $K = \mathbb{Q}(\sqrt{3})$ olur

PARÇALANIŞ CİSİMLERİ

F bir cisim ve $f(x) \in F[x]$ sabit olmayan bir polinom ise $f(x)$ in bir kökünü bulunduran F nin bir E cisim genişlemesi bulunabileceğini daha önce görmüştük. Aşağıdaki teorem ile $f(x)$ in bütün köklerini içeren F nin bir cisim genişlemesi bulunabileceğini görüyoruz.

TEOREM. F bir cisim, $f(x) \in F[x]$ sabit olmayan bir polinom olsun. Buna göre $f(x)$ in bütün köklerini bulunduran F nin bir cisim genişlemesi vardır.

KANIT. $\deg(f(x)) = 1$ ise F $f(x)$ in tek kökünü içerir. Dolayısıyla $\deg(f(x)) = n > 1$ ve teorem derecesi n den küçük sabit olmayan polinomlar için doğru olsun. Kronecker Teoreminden $f(x)$ bir c kökünü içeren F nin bir K genişlemesi vardır. Buna göre $K[x]$ içinde $f(x) = f_1(x)(x-c)$ olacak şekilde bir $f_1(x) \in K[x]$ vardır. $\deg(f_1(x)) = n-1 < n$ olduğundan tümevarım hipotezi gereğince $f_1(x)$ in bütün köklerini içeren K nın bir E genişlemesi vardır. Fakat $K \subseteq E$ olduğundan E, c yi de içerir ve böylece E $f(x)$ in bütün köklerini içerir. Dolayısıyla istenen kanıtlanmış olur. ☐

Tanım. F bir cisim ve $f(x) \in F[x]$, $\deg(f(x)) \geq 1$ olsun. $f(x)$ in bütün köklerini içeren F nin bir genişlemesi E olsun. Eğer $f(x)$ in bütün kökleri $c_1, \ldots, c_n \in E$ ise E nin $F(c_1, \ldots, c_n)$ alt

cismine $f(x)$ in F üzerindeki bir parçalanış cismi denir.

Yukarıdaki tanıma göre $f(x) \in F[x]$ polinomunun bir parçalanış cismi $f(x)$ in köklerini içeren F nin bir minimal genişlemesidir ve bu genişleme içinde $f(x)$ tamamı doğrusal çarpanlara ayrılabilir.

Örnek. (i) $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ polinomunun $\mathbb{Q}$ üzerindeki parçalanış cismi $\mathbb{Q}(\sqrt{2})$ cismidir.

(ii) $f(x) = x^4 - 1 \in \mathbb{Q}[x]$ polinomunun parçalanış cismi $\mathbb{Q}(i)$ dir. Gerçekten $x^4 - 1$ in tüm kökleri $\pm 1, \pm i$ $\mathbb{C}$ içinde bulunur ve bunları içeren $\mathbb{Q}$ nun en küçük genişlemesi $\mathbb{Q}(i)$ dir.

(iii) $x^3 - 2 \in \mathbb{Q}[x]$ polinomunun $\mathbb{Q}$ üzerindeki bir parçalanış cismini bulalım. $x^3 - 2$ nin tüm kökleri $\mathbb{C}$ içinde bulunabilir. Bunlar $w = \frac{-1+i\sqrt{3}}{2}$ olmak üzere $\sqrt[3]{2}$, $w\sqrt[3]{2}$ ve $w^2\sqrt[3]{2}$ dir. Dolayısıyla $x^3 - 2$ polinomunun $\mathbb{C}$ içindeki parçalanış cismi $\mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2})$ olur. Aslında $\mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ yazabiliriz.

$$w = \frac{-1+i\sqrt{3}}{2} = -\frac{1}{2} + \frac{1}{2}(i\sqrt{3}) \in \mathbb{Q}(i\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) \text{ ve}$$

$$w^2 = \frac{-1-i\sqrt{3}}{2} = -\frac{1}{2} - \frac{1}{2}(i\sqrt{3}) \in \mathbb{Q}(i\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$$

olduğundan $\mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ elde edilir. Diğer taraftan

$$w = (w\sqrt[3]{2})(\sqrt[3]{2})^{-1} \in \mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}) \text{ ve dolayısıyla}$$

$$i\sqrt{3} = \frac{-1+i\sqrt{3}}{2} - \frac{-1-i\sqrt{3}}{2} = w - w^2 \in \mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2})$$

bulunur. Böylece $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2})$ elde edilir.

Dolayısıyla $x^3-2 \in \mathbb{Q}[x]$ polinomunun $\mathbb{C}$ içindeki parçalanış cismi $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ cismidir.

(iv) $f(x) = x^4 - 2x^2 - 3 \in \mathbb{Q}[x]$ ise $f(x) = (x^2-3)(x^2+1)$ yazılabileceğinden $f(x)$ tüm kökleri $\pm\sqrt{3}, \pm i$ dir. Buna göre $f(x)$ in bir parçalanış cismi $\mathbb{Q}(\sqrt{3}, i)$ cismidir.

TEOREM. $\sigma : F \longrightarrow F'$ bir cisim izomorfizması, $f(x) \in F[x]$, $f^*(x) = \sigma^*(f(x))$, $f(x)$ in F üzerindeki bir parçalanış cismi K ve $f^*(x)$ in F' üzerindeki bir parçalanış cismi K' ise σ, K dan K' üzerine bir izomorfizmaya genişler.

KANIT. $\deg(f(x)) = n$ olsun. Buna göre $\deg(f^*(x)) = n$ dir. $n=1$ ise $K=F$ ve $K'=F'$ olacağından durum açıktır. $n>1$ ve teorem derecesi n den küçük polinomlar ile bunların parçalanış cisimleri için doğru olsun. $\deg(f(x)) > 1$ olduğundan $f(x)$ in $F[x]$ içinde bir indirgenemez böleni vardır. Bu bölen $p(x)$ olsun. K Fnin bir parçalanış cismi olduğundan $p(x)$ in kökleri K tarafından içerilir. $c \in K$ olmak üzere $p(c)=0$ olsun. Buna göre $p(x) = \mathrm{Min}_F(c)$ dir. $\sigma^*(p(x)) = p^*(x)$ olsun. $p^*(x) \in F'[x]$ ve $p^*(\sigma(c)) = 0$. $\sigma(c)=c'$ olsun. Bu durumda $p^*(x)$ polinomu da $F'[x]$ içinde indirgenemez olacağından $p^*(x) = \mathrm{Min}_{F'}(c')$ olur. Dolayısıyla σ

$$\overline{\sigma} : F(c) \longrightarrow F'(c')$$

şeklinde bir izomorfizmaya genişler. $f(x) = f_1(x)(x-c)$ ve $f^*(x) = f_1^*(x)(x-c')$ olsun. Dikkat edilirse K $f_1(x)$ in $F(c)$ üzerinde; K' $f_1^*(x)$ in $F'(c')$ üzerinde birer parçala-

nin cismidir. $\deg(f_1(x)) = \deg(f_1^*(x)) < \deg(f(x)) = n$ olduğundan tümevarım hipotezimiz gereğince $\overline{\sigma}$,

$$\tau : K \longrightarrow K'$$

şeklinde bir izomorfizmaya genişler. $\overline{\sigma}$ da σ nın bir genişlemesi olduğundan τ σ nın da bir genişlemesi olur.

$$\begin{array}{ccc} K & \xrightarrow{\tau} & K' \\ | & & | \\ F(c) & \xrightarrow{\overline{\sigma}} & F'(c') \\ | & & | \\ F & \xrightarrow{\sigma} & F' \end{array}$$

Böylece kanıt tamamlanmış olur. □

SONUÇ. F bir cisim ve $f(x) \in F[x]$, $\deg(f(x)) \geq 1$ olsun. $f(x)$ in F üzerindeki parçalanış cismi izomorfizma farkıyla tektir.

KANIT. K_1 ve K_2 $f(x)$ in F üzerindeki iki parçalanış cismi olsun. Yukarıdaki teoremi $F' = F$, $K = K_1$, $K' = K_2$ ve $\sigma = I_F$ için uygularsak I_F, K_1 den K_2 üzerine bir izomorfizmaya genişler. Böylece istenen elde edilmiş olur. □

NOT: F bir cisim ve $f(x) \in F[x]$ sabit olmayan bir polinom olsun. $f(x)$ in F üzerindeki her parçalanış cismi F nin bir sonlu genişlemesidir.

SONLU CİSİMLER

F bir cisim ve F nin karakteristiği n olsun. $n=0$ yada p bir asal sayı olmak üzere $n=p$ dir. Her $m,n\in\mathbb{Z}$ için

$$m.1_F + n.1_F = (m+n).1_F \text{ ve } (m.1_F)(n.1_F) = (mn).1_F$$

olduğundan

$$\varphi : \mathbb{Z} \longrightarrow F$$
$$z \longmapsto z.1_F$$

eşlemesi bir halka homomorfizmasıdır ve $\text{Çek}(\varphi) = n\mathbb{Z}$ dir. Eğer $n=0$ ise F nin $\mathbb{Z}$ ye izomorf bir althalkası olur ki bu durum da F nin $\mathbb{Q}$ ya izomorf bir altcismi olur. Eğer $n=p$ ise F nin $\mathbb{Z}/p\mathbb{Z}$ ye izomorf bir altcismi vardır. $n=0$ ise $\mathbb{Q}$ ya, $n=p$ ise $\mathbb{Z}/p\mathbb{Z}$ ye izomorf altcismine F nin <u>asal altcismi</u> denir. F nin asal altcismini $\Delta(F)$ ile gösterelim. Bu durumda

$$\Delta(F) \cong \begin{cases} \mathbb{Q}, & n=0 \text{ ise} \\ \mathbb{Z}/p\mathbb{Z}, & n=p \text{ ise} \end{cases}$$

yazılabilir. $n=p$ olduğu durumda $\Delta(F) = \{0.1_F, 1.1_F, \ldots, (p-1).1_F\}$ dir. Ayrıca eğer F bir sonlu cisim ise gruplardaki Lagrange teoremini $(F,+)$ abelyan grubuna uygulayarak F nin karakteristiğinin sıfırdan farklı, yani bir asal sayı olacağını söyleyebiliriz.

TEOREM. F bir sonlu cisim ve $\text{kar}(F)=p$ olsun. O zaman bir $n\geq 1$ tamsayısı için $|F| = p^n$ dir.

KANIT. F, $\Delta(F)$ üzerinde bir vektör uzayı olduğundan $[F:\Delta(F)]=n$

olacak şekilde bir $n \geq 1$ tamsayısı vardır. F nin $\Delta(F)$-bazı $\{v_1, v_2, \ldots, v_n\}$ olsun. O zaman her $u \in F$ için

$$u = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n$$

olacak şekilde tek türlü belirli $(c_1, \ldots, c_n) \in \Delta(F)^n$ sıralı n-lisi vardır. Dolayısıyla

$$\begin{aligned} \Delta(F)^n &\longrightarrow F \\ (c_1, \ldots, c_n) &\longmapsto c_1 v_1 + \cdots + c_n v_n \end{aligned}$$

eşlemesi bir birebir eşlemedir. Ayrıca $\Delta(F) \cong \mathbb{Z}_p$ olduğundan $|\Delta(F)| = p$ ve böylece $|F| = |\Delta(F)^n| = p^n$ bulunur. ☒

TEOREM. F bir cisim olsun. O zaman $F^* = F \setminus \{0_F\}$ çarpımsal grubunun her sonlu altgrubu devirlidir.

KANIT. G, F^* ın bir sonlu altgrubu ve $|G| = n$ olsun. $n = 1$ ise $G = \{1_F\}$ devirlidir. $n > 1$ olsun. G nin en büyük olan bir elemanı a ve a nın mertebesi $o(a) = m$ olsun. Eğer $m = n$ ise $G = \langle a \rangle$ dır. Mümkünse $m < n$ olsun. Her $c \in \langle a \rangle$ için $c^m = 1_F$ olduğundan $\langle a \rangle$ nın elemanları $x^m - 1_F \in F[x]$ polinomunun m farklı kökünü oluşturur. Bu polinomun F içinde en çok m tane kökü olacağından bütün kökler $\langle a \rangle$ nın elemanlarıdır. Şimdi $b \in G \setminus \langle a \rangle$ ve $o(b) = s$ olsun. $b^m \neq 1_F$ olduğundan $s \nmid m$ ve $s < m$ dir. $d = (m, s)$ olsun. O zaman $d < m$ ve $d < s$ dir. Ayrıca $o(a^d) = \frac{m}{d}$ ve $o(b^d) = \frac{s}{d}$ dir. Üstelik $\left(\frac{m}{d}, \frac{s}{d}\right) = 1$ olduğundan $o((ab)^d) = o(a^d b^d) = \left(\frac{m}{d}\right)\left(\frac{s}{d}\right)$ olur. Buradan $o(ab) = d \frac{m}{d} \frac{s}{d} = m \frac{s}{d} > m$ bulunur. Bu ise bir çelişkidir. Dolayısıyla

$G = \langle a \rangle$ dır.

Alternatif olacak aşağıdaki kanıtı da verebiliriz.

G nin tüm elemanlarının mertebelerinin en küçük ortak katı m olsun. m nin, $p_1^{t_1} \dots p_k^{t_k}$ şeklinde asal çarpanlarına ayrıldığını varsayalım. m nin seçiminden dolayı $p_1^{t_1} \mid o(g)$ olacak şekilde bir $g \in G$ vardır. $g_1 = g^{m/p_1^{t_1}}$ olsun. $o(g_1) = p_1^{t_1}$ olduğunu gösterelim. $g_1^{p_1^{t_1}} = g^m = 1_F$ olduğundan $o(g_1) \mid p_1^{t_1}$ dir. Buna göre $o(g_1) = p_1^s$ olacak şekilde bir $s \leq t_1$ tamsayısı vardır. $1_F = g_1^{p_1^s} = g^{\frac{m}{p_1^{t_1}} \cdot p_1^s}$ olduğundan $o(g) = m \mid m \cdot p_1^{s-t_1}$ ve böylece $p_1^{s-t_1} \in \mathbb{Z}$ yani $s = t_1$ bulunur. Dolayısıyla $o(g_1) = p_1^{t_1}$. Benzer şekilde her $i = 1, \dots, k$ için $o(g_i) = p_i^{t_i}$ olacak şekilde $g_i \in G$ vardır. $a = g_1 \dots g_k$ olsun. $o(a) = o(g_1 \dots g_k) = p_1^{t_1} \dots p_k^{t_k} = m$ olur. Böylece $m \mid |G|$ yani $m \leq |G|$ olur. Öte yandan G nin her elemanı $x^m - 1_F$ polinomunun bir köküdür (m nin seçiminden dolayı). Bu polinomun F içinde en fazla m tane kökü olacağı için $|G| \leq m$ bulunur. Böylece $|G| = m$ ve $G = \langle a \rangle$ elde edilir.

□

SONUÇ. Bir sonlu cismin her sonlu genişlemesi bir basit genişlemedir.

KANIT. F bir sonlu cisim ve E, F nin bir sonlu genişlemesi olsun. $[E:F] = n$ olsun. F sonlu olduğundan $|E| = |F|^n$ dir. Dolayısıyla E sonludur. Buradan $E^* = \langle a \rangle$ olacak şekilde bir $a \in E^*$ bulunur. Şimdi $E = E^* \cup \{0\} = \langle a \rangle \cup \{0\} \subseteq F(a)$ olduğundan $E = F(a)$ olur.

□

TEOREM. F, p^n elemanlı bir cisim ise $x^{p^n} - x \in \Delta(F)[x]$ polinomunun $\Delta(F)$ üzerindeki bir parçalanış cismidir. Ayrıca p^n elemanlı herhangi iki cisim birbirine izomorftur.

KANIT. $f(x) = x^{p^n} - x$ olsun. F sonlu olduğundan $F^* = \langle a \rangle$ olacak şekilde $0_F \neq a \in F$ vardır. Ayrıca $|F^*| = p^n - 1$ olduğundan $a^{p^n-1} = 1_F$; yani $a^{p^n} = a$ dır. O zaman her $1 \leq i \leq p^n$ için $(a^i)^{p^n} = (a^{p^n})^i = a^i$ olduğundan F nin her elemanı $f(x)$ in bir köküdür. Böylece $f(x)$ in F içinde p^n kökü vardır. $f(x)$ in köklerinin sayısı $\leq p^n$ olduğundan F $x^{p^n} - x$ polinomunun köklerinden ibarettir. Dolayısıyla F $x^{p^n} - x$ polinomunun $\Delta(F)$ üzerindeki bir parçalanış cismidir.

Şimdi p^n elemanlı başka bir cisim E olsun. Kanıtın ilk kısmından dolayı E $x^{p^n} - x$ polinomunun $\Delta(E)$ üzerindeki parçalanış cismidir. Diğer taraftan $\Delta(F) \cong \mathbb{Z}_p$ ve $\Delta(E) \cong \mathbb{Z}_p$ olduğundan $\Delta(F)$ den $\Delta(E)$ ye bir cisim izomorfizması tanımlanabilir. Bu izomorfizmaya σ dersek, $\sigma^*(x^{p^n} - x) = x^{p^n} - x$ olduğundan σ F den E ye bir izomorfizmaya genişler. □

NOT: Bundan sonra aksi belirtilmedikce p^n elemanlı bir cismin daima $\mathbb{Z}_p$ yi içerdiği varsayılacaktır.

F bir cisim ve $f(x) \in F[x]$ olsun. $f(x) = \sum_{i=0}^{n} a_i x^i$ ise $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$ şeklinde tanımlanan polinoma $f(x)$ in türevi denir.

LEMMA. F bir cisim, $f(x) \in F[x]$, $\deg(f(x)) \geq 1$ olsun. $f(x)$ in F nin bir cisim genişlemesi içindeki bir kökü u olsun. u nun çok katlı kök olması için gerek ve yeter şart $f'(x)$ in bir kökü olmasıdır.

KANIT. $f(x)$ in $u$yu içeren bir parçalanma cismi K olsun. Kabul edelim ki u, $f(x)$ in çokkatlı bir kökü olsun. O zaman

$$f(x) = (x-u)^s g(x)$$

olacak şekilde $g(x) \in K[x]$ ve $s \geq 2$ tamsayısı vardır. iki tarafın türevi alınırsa $f'(x) = s(x-u)^{s-1} g(x) + (x-u)^s g(x)$ olacağından $f'(u) = 0$ bulunur.

Karşıt olarak u, $f(x)$ ve $f'(x)$ in ortak kökü olsun. İlk halde olduğu gibi $f(x) = (x-u)h(x)$ olacak şekilde $h(x) \in K[x]$ vardır.

$\Rightarrow \quad f'(x) = h(x) + (x-u)h'(x) \Rightarrow 0_F = f'(u) = h(u) \Rightarrow x-u \mid h(x)$

$\Rightarrow (x-u)^2 \mid f(x) \Rightarrow u$ en az iki katlıdır. ☐

LEMMA F bir cisim ve $\text{kar}(F) = p \neq 0$ ise o zaman her $a, b \in F$ ve $n \geq 0$ tamsayısı için $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ dir.

KANIT. Binom açılımı yapılırsa

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \ldots + \binom{p}{r} a^{p-r}b^r + \ldots + \binom{p}{p-1} ab^{p-1} + b^p$$

olduğu görülür. Ayrıca kolayca görülebilir ki her $1 \leq r \leq p-1$ için

$\binom{p}{r}$ tamsayısı p tarafından bölünür. $Kar(F)=p$ olduğundan binom açılımındaki tüm ara terimler sıfır olur ve böylece

$$(a+b)^p = a^p + b^p$$

bulunur. Tümevarım ile herhangi bir $n \geq 0$ tamsayısı için

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

elde edilir. ☒

TEOREM. Her p asal sayısı ve her $n \geq 1$ için p^n elemanlı bir cisim vardır.

KANIT. $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ olsun. $\mathbb{Z}_p$ üzerinde $f(x)$ in bir parçalanış cismi vardır. Bu cisim K olsun. $f(x)$ in K içindeki bütün köklerinin kümesi S olsun.

$$f'(x) = \overline{p^n} x^{p^n-1} - \overline{1} = -\overline{1}$$

olduğundan $f'(x)$ in hiç kökü yoktur. Dolayısıyla $f(x)$ in her kökü basit (tek katlı) köktür. Buna göre $|S| = p^n$ dir.

Şimdi S nin cisim olduğunu gösterelim. $|S| \geq 2$ olduğu açıktır. $a, b \in S$ olsun. Buna göre $a-b$, ab ve $b \neq \overline{0}$ iken $b^{-1} \in S$ olduğunu göstermek yeter. a, b, $f(x)$ in kökleri olduğundan $a^{p^n} = a$ ve $b^{p^n} = b$ dir.

$$(a-b)^{p^n} = a^{p^n} - b^{p^n} = a-b$$

ve

$$(ab)^{p^n} = a^{p^n} b^{p^n} = ab$$

olduğundan $a-b, ab \in S$ dir. Ayrıca $b \neq \overline{0}$ iken $(b^{-1})^{p^n} = (b^{p^n})^{-1} = b^{-1}$ olduğundan $b^{-1} \in S$ bulunur. Dolayısıyla S bir cisimdir. ☒

Genelde $\mathbb{Z}_p$ yi içeren p^n elemanlı bir cisim $GF(p^n)$ ile gösterilir ve bu cisme p^n elemanlı Galois cismi denir.

TEOREM. F bir sonlu cisim olsun. Her $n \geq 1$ için $F[x]$ içinde derecesi n olan bir indirgenmez polinom vardır.

KANIT. $Kar(F) = p$ ve $F = GF(p^r)$ olsun. Ayrıca $f(x) = x^{p^{rn}} - x \in \mathbb{Z}_p[x]$ olsun. $\mathbb{Z}_p \leq F$ olduğundan $f(x) \in F[x]$ tir. $f(x)$ in F üzerindeki parçalanma cismi K ve $f(x)$ in K içindeki köklerinin kümesi S olsun. Yukarıdaki teoremin kanıtında olduğu gibi S, K nın bir altcismi ve $|S| = p^{nr}$ dir. Öte yandan $\mathbb{Z}_p$, K nın asal cismi olduğundan S nin bir altcismidir. Ayrıca $f(x) \in \mathbb{Z}_p[x]$ olduğundan hem K hem de S, K içinde $f(x)$ in $\mathbb{Z}_p$ üzerindeki parçalanma cisimleridir. Buradan $K = S$ bulunur. Özel olarak $|K| = p^{rn}$ dir. Şimdi $F \leq K$ ve $|F| = p^r$ olduğundan $[K : F] = n$ dir. Ayrıca K, F üzerinde bir basit genişleme olacağından $K = F(u)$ olacak şekilde $u \in K$ vardır. Buna göre u nun F üzerindeki minimal polinomu F üzerinde derecesi n olan bir indirgenmez polinomdur. ☒

SONUÇ. $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ polinomu $\mathbb{Z}_p[x]$ içinde birbirinden farklı monik indirgenmez polinomların çarpımıdır. Ayrıca bir indirgenmez polinomun $f(x)$ i bölmesi için gerek ve yeter şart derecesinin n yi bölmesidir.

KANIT. $f'(x) = -\bar{1}$ olduğundan $f(x)$ in her kökü tek katlıdır, dolayısıyla birbirinden farklı monik indirgenmez polinomların çarpımıdır.

Şimdi $p(x) \in \mathbb{Z}_p[x]$ irreg ve $\deg(p(x)) = d$ olsun. $f(x)$ in $\mathbb{Z}_p$ üzerindeki parçalanış cismi K olsun. Daha önce görüldüğü gibi K, $f(x)$ in bütün köklerinin kümesidir ve $|K| = p^n$ dir. Dolayısıyla $[K : \mathbb{Z}_p] = n$ dir. Önce $p(x) \mid f(x)$ olsun. K $f(x)$ in bütün kökleri olduğundan $p(u) = \bar{0}$ olacak şekilde bir $u \in K$ vardır. Bu durumda $[\mathbb{Z}_p(u) : \mathbb{Z}_p] = d$ dir. Aynı zamanda

$$n = [K : \mathbb{Z}_p] = [K : \mathbb{Z}_p(u)] \cdot [\mathbb{Z}_p(u) : \mathbb{Z}_p]$$
$$= [K : \mathbb{Z}_p(u)] \cdot d$$

olduğundan $d \mid n$ dir.

Karşıt olarak $d \mid n$ olsun. $p(x) \in \mathbb{Z}_p[x] \subseteq K[x]$ olduğundan $p(x) \in K[x]$ tir. Şimdi $p(x)$ in K üzerinde bir parçalanma cismi L ve $p(x)$ in L içindeki bir kökü v olsun. Eğer $v \in K$ ise $f(v) = \bar{0}$ ve o zaman $p(x) \mid f(x)$ tir. Mümkünse $v \notin K$ olsun. $\mathbb{Z}_p \leq K$ olduğundan $\mathbb{Z}_p(v) \leq K(v)$ dir. Ayrıca $[\mathbb{Z}_p(v) : \mathbb{Z}_p] = d$ olduğundan $|\mathbb{Z}_p(v)| = p^d$ ve $|\mathbb{Z}_p(v)^*| = p^d - 1$ dir. Buradan $v \neq 0$ olduğundan $v^{p^d - 1} = 1$ ve böylece v, $x^{p^d - 1} - 1$ polinomunun bir köküdür. Öte yandan $d \mid n$ olduğundan $p^d - 1 \mid p^n - 1$ ve buradan $x^{p^d - 1} - 1 \mid x^{p^n - 1} - 1$ olur. Dolayısıyla $v^{p^n - 1} = 1$ ve buradan $v^{p^n} = v$ bulunur. Böylece v, $f(x)$ in L içindeki bir köküdür ve bu durumda $v \in K$ olur ki, bu da bir çelişkidir. Böylece kanıt tamamlanmış olur. ∎

ÖRNEK. $\mathbb{Z}_2[x]$ içindeki derecesi ≤ 3 olan bütün polinomlar

x, $x+\bar{1}$

$x^2+x+\bar{1}$

$x^3+x+\bar{1}$, $x^3+x^2+\bar{1}$

polinomlarıdır.

$x^4-x = x(x+\bar{1})(x^2+x+\bar{1})$

$x^8-x = x(x+\bar{1})(x^3+x+\bar{1})(x^3+x^2+\bar{1})$

yazılabilir.

$F = \dfrac{\mathbb{Z}_2[x]}{\langle x^3+x+\bar{1}\rangle} \Rightarrow F$ 8 elemanlı bir cisim

Genel olarak p^n elemanlı bir cisim bulmak için $\deg(p(x))=n$ o.ş. $p(x)\in\mathbb{Z}_p[x]$ indirgenemez polinom bulup $\mathbb{Z}_p[x]/\langle p(x)\rangle$ bölümüne geçmek gerekir.

$F = \mathbb{Z}_3[x]/\langle x^2+\bar{1}\rangle \Rightarrow |F|=9$

$F = \mathbb{Z}_2[x]/\langle x^4+x^3+1\rangle \Rightarrow |F|=16.$