# Derse Ek:

$f$, $\mathbb{Q}$ üzerinde derecesi $n$ olan indirgenemez bir polinom olsun.

$$\varphi : G(\mathbb{Q}(f)/\mathbb{Q}) \longrightarrow Perm(\{\alpha_1 \dots \alpha_n\}) \text{ 'yi}$$
$$\sigma \longmapsto \sigma|_{\{\alpha_1 \dots \alpha_n\}}$$

düşünelim. Burada $\mathbb{Q}(f)$, $f$'nin parçalanış cismini, $\alpha_1 \dots \alpha_n$"de $f$'nin köklerini göstersin. Son dersteki ilk teoremden $\mathbb{Q}(f)/\mathbb{Q}$'nun bir Galois genişlemesi olduğunu biliyoruz. O zaman $[\mathbb{Q}(f):\mathbb{Q}] = |G(\mathbb{Q}(f)/\mathbb{Q})|$'dir. Derste $\varphi$'nin iyi tanımlılığı, 1-1'liği tartışılmıştı. $\varphi$'nin bir homomorf olduğu da açıktır. O zaman eğer $[\mathbb{Q}(f):\mathbb{Q}] = |Per(\{\alpha_1 \dots \alpha_n\})| = |S_n| = n!$ ise $\varphi$ örtendir (bu teoremi grup teorisinden hatırla!). Böylelikle, eğer $[\mathbb{Q}(f):\mathbb{Q}] = n!$ ise, $\varphi$ bir izomorfizmadır. Derste Van der Waerden'in bir teoreminden $[\mathbb{Q}(f):\mathbb{Q}] = n!$ olma durumuyla ~~genişçe yüksek~~ neredeyse her zaman karşılaştığımızı (olasılık 1) söylemiştik. Fakat olasılığın 1 olması bu durumun $[\mathbb{Q}(f):\mathbb{Q}] = n!$ olmadığı durumlarla hiç karşılaşmayacağımız anlamına gelmez. Aşağıdaki örnek mesela $[\mathbb{Q}(f):\mathbb{Q}] \neq n!$ olduğu bir durum verecek:

**Örnek:** $f(x) = x^5 - 2 \in \mathbb{Q}[x]$, $\mathbb{Q}(f) = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$'dir.

Burada $\zeta_5 = e^{\frac{2\pi i}{5}}$ (yani $\zeta_5$, 1'in 5'inci dereceden ilkel köküdür. yani $\zeta_5$, $x^5 - 1 = 0$'ın köküdür fakat $\zeta_5 \neq 1$'dir).

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(f) = \mathbb{Q}(\sqrt[5]{2}, \zeta_5) \arrow[dl, no head] \arrow[dr, no head] & \\ \mathbb{Q}(\zeta_5) \arrow[dr, no head, "m"'] & & \mathbb{Q}(\sqrt[5]{2}) \arrow[dl, no head, "n"] \\ & \mathbb{Q} & \end{tikzcd}$$

$f$, $\mathbb{Q}$ üzerinde Eisenstein teoreminden indirgenemezdir, yani $n = 5$'dir. $\zeta_5$, $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) = 0$'ın kökü ve $\zeta_5 \neq 1$ olduğundan, $\zeta_5$,

$g(x) = x^4 + x^3 + x^2 + x + 1$'in bir köküdür. Fakat derste gördüğümüz üzere $g$, $\mathbb{Q}$ üzerinde indirgenemezdir. Yani $m=4$'dür. Başka bir teoremden (derste gördüğümüz), $(m,n)=(4,5)=1$ olduğundan, $[\mathbb{Q}(f):\mathbb{Q}]=4\cdot 5 = 20$'dir. $20 \neq 5! = 120$ olduğundan bu örnek bize $[\mathbb{Q}(f):\mathbb{Q}]=n!$ olmayan bir durumu verir. Fakat bunun Van der Waerden'in sonucu ile çelişmediğini söyleyelim. O, herzaman $[\mathbb{Q}(f):\mathbb{Q}]=n!$ olduğunu değil, böyle olma olasılığının neredeyse her zaman olduğunu söylemiştir, yani az da olsa $\mathbb{Q}$'in sağlamadığı durumlar vardır.

Derste ayrıca şu teorem ve sonucunu yapmıştık:

Teorem: $S_n$ $(n \geq 5)$ çözümlenebilir (solvable) değildir.

Sonuç: $f$, $\mathbb{Q}$ üzerinde derecesi $n \geq 5$ olan indirgenemez bir polinom olsun ve $[\mathbb{Q}(f):\mathbb{Q}]=n!$ $\left(|G(\mathbb{Q}(f)/\mathbb{Q})|=n!\right)$ olsun. Böylece, $f$'nin kökleri ard arda kök alarak elde edilemez.

Bu sonuç bize, eğer $G := G(\mathbb{Q}(f)/\mathbb{Q}) \cong S_n$ ve $n \geq 5$ ise, $f$'nin köklerinin ard arda kök alarak elde edilemeyeceğini gösterir. Ama Van der Waerden'in sonucuna göre $G \cong S_n$ olma durumu olasılığı 1'dir, yani neredeyse her zaman eğer derecesi $n \geq 5$ olan indirgenemez bir $f$ polinomu alsak $f$'nin köklerini ard arda kök alarak elde edemeyiz. Ama bu, bazen derecesi $n \geq 5$ olan böyle indirgenemez polinomlar bulabileceğimiz diye bi bulalım kökleri ard arda kök alarak elde edilebilsin, gerçeği ile çelişmez. Bunun için tabiki aradığımız polinomlar için yuka-

Yukarıdaki sonuca göre, $G \neq S_n$ olmalıdır. Mesela, (3)
bunun için bir önceki örneği düşünelim. $f = x^5 - 2 \in \mathbb{Q}[x]$.
Bu polinom için $|G| = |G(\mathbb{Q}(f)/\mathbb{Q})| = 20$ olduğunu
nu göstermiştik. Yani, açık bir şekilde $G \neq S_5$ 'dir.
Fakat burada $f$'nin kökleri $\sqrt[5]{2}$, $\zeta_5 \sqrt[5]{2}$, $\zeta_5^2 \sqrt[5]{2}$, $\zeta_5^3 \sqrt[5]{2}$, $\zeta_5^4 \sqrt[5]{2}$ açık bir şekilde ard arda kök alarak elde edilebilir. Bu örnekten şunu gördük:

- Öyle $f \in \mathbb{Q}[x]$ indirgenemez polinomlar vardır ki, $f$'nin derecesi $n \geq 5$ olan, $f$'nin kökleri ard arda kök alarak elde edilebilir.
- Van der Waerden'in teoremine göre herhangi bir indirgenemez polinom $f$ alırsak $\mathbb{Q}$ üzerinde derecesi $n \geq 5$ olan, $f$'nin köklerini ard arda kök alarak elde etme olasılığımız 1'dir. Yani $f = x^5 - 2 \in \mathbb{Q}[x]$ gibi durumlar azdır.

Şimdi $G$ grubunun yapısını inceleyelim. $\alpha = \sqrt[5]{2}$ olsun.

$$\sigma_\alpha : \begin{array}{l} \alpha \longmapsto \alpha \zeta_5 \\ \zeta_5 \longmapsto \zeta_5 \\ a \longmapsto a \quad (a \in \mathbb{Q}) \end{array} \qquad \sigma_{\zeta_5} : \begin{array}{l} \alpha \longmapsto \alpha \\ \zeta_5 \longmapsto \zeta_5^3 \\ a \longmapsto a \quad (a \in \mathbb{Q}) \end{array} \quad \text{olsun.}$$

Açık bir şekilde $\sigma_\alpha, \sigma_{\zeta_5} \in G$. $\sigma_\alpha$'nın mertebesinin 5 ve $\sigma_{\zeta_5}$'in mertebesinin 4 olduğunu görmek zor değildir.

$$\sigma_\alpha \circ \sigma_{\zeta_5} : \begin{array}{l} \alpha \longmapsto \alpha \zeta_5 \\ \zeta_5 \longmapsto \zeta_5^3 \end{array} \qquad \sigma_{\zeta_5} \circ \sigma_\alpha : \begin{array}{l} \alpha \longmapsto \alpha \zeta_5^3 \\ \zeta_5 \longmapsto \zeta_5^3 \end{array}$$

olduğundan ve $\sigma_\alpha \circ \sigma_{\zeta_5} \neq \sigma_{\zeta_5} \circ \sigma_\alpha$ olduğundan $G$ değişmeli bir grup değildir. Fakat $\sigma_{\zeta_5}^{-1} \circ \sigma_\alpha \circ \sigma_{\zeta_5} = \sigma_\alpha^2$ olduğundan, yani $\langle \sigma_\alpha \rangle$, $\langle \sigma_{\zeta_5} \rangle$'i normalize ettiğinden,

$$G = \langle \sigma_{\zeta_5} \rangle \ltimes \langle \sigma_\alpha \rangle \quad \text{olur.}$$