T.C.

HİTİT ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

ÖRGÜ GRUPLARI TEORİSİNDE KELİME PROBLEMİ

Yüksek Lisans Tezi

Emre AKAR

Çorum – 2023

ÖRGÜ GRUPLARI TEORİSİNDE KELİME PROBLEMİ

Emre AKAR

Lisansüstü Eğitim Enstitüsü

Matematik Anabilim Dalı

Yüksek Lisans Tezi

TEZ DANIŞMANI

Doç. Dr. Elif DALYAN

Çorum 2023

KABUL ONAY SAYFASI

Emre AKAR tarafından hazırlanan "Örgü Grupları Teorisinde Kelime Problemi" adlı tez çalışması 26/01/2023 tarihinde aşağıdaki jüri üyeleri tarafından oy birliği ile Hitit Üniversitesi Lisansüstü Eğitim Enstitüsü Matematik Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Doç. Dr. Elif DALYAN ……

Dr. Öğr. Üyesi Sabahattin ILBIRA ……

Dr. Öğr. Üyesi Hüseyin ALTUNDAĞ ……

Hitit Üniversitesi Lisansüstü Eğitim Enstitüsü Yönetim Kurulunun …/…/…… tarih ve …….. sayılı kararı ile ……'ın..... Anabilim Dalında Yüksek Lisans derecesi alması onanmıştır.

Prof. Dr. Muhammed Asıf YOLDAŞ

Lisansüstü Eğitim Enstitü Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını beyan ederim.

Emre AKAR

ÖRGÜ GRUPLARI TEORİSİNDE KELİME PROBLEMİ

Emre AKAR

ORCID: 0009-0005-6017-0153

HİTİT ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Yüksek Lisans Tezi

Mart 2023

ÖZET

Bu çalışmamızda geometrik örgü grupları incelendi. İlk olarak örgü teorisinde en çok bilinen problemlerden biri olan kelime problemi ele alınmıştır. Daha sonra bu soruna çözüm olarak Artin'in Örgü Tarama Algoritması tanıtılmış ve detaylı olarak anlatılmıştır.

Anahtar Kavramlar: Örgüler, Örgü teorisi, Kelime problemi

Bilim Kodu: 20405

WORD PROBLEM IN BRAID GROUP THEORY

Emre AKAR

ORCID: 0009-0005-6017-0153

HITIT UNIVERSITY

GRADUATE SCHOOL

Master of Science Thesis

MARCH 2023

ABSTRACT

In this thesis, geometric braid groups are studied. Firstly, the word problem, one of the most well-known problems in braid theory, is discussed. Then as a solution to this problem, Artin's Braid Combing Algorithm is introduced and described in detail.

Key Terms: Braids, Braid theory, Word problem.

Science Code: 20405

TEŞEKKÜR

Çalışmamda her zaman yanımda olan, bilgisini ve emeğini benden hiç esirgemeyen cesaretimin kırıldığı anlarda beni yüreklendiren kendisi tanımaktan çok mutlu olduğum, öğrencisi olmaktan her zaman gurur duyacağım, değerli danışmanım sn Doç. Dr. Elif DALYAN'a teşekkürlerimi sunarım. Her zaman yanımda olan beni hep destekleyen kıymetli eşim Kübra'ya sevgisiyle bana güç veren biricik kızım Yaren Sare'ye takıldığım her alanda beni destekleyen değerli dostum Oğuzhan ODABAŞ'a sonsuz teşekkür ederim.

Emre AKAR

İÇİNDEKİLER

Sayfa

ÖZET ..... **iv**

ABSTRACT ..... **v**

TEŞEKKÜR ..... **vi**

İÇİNDEKİLER ..... **viii**

ŞEKİLLER DİZİNİ ..... **ix**

SİMGELER VE KISALTMALAR ..... **xi**

GİRİŞ **1**

1. BÖLÜM

ÖRGÜ TEORİSİ

1.1. Geometrik Örgüler 3

1.2. Örgüler ve İzotopi 4

1.3. Kelime Problemi 10

1.3.1 Artin örgü tarama algoritması 12

SONUÇ **23**

KAYNAKLAR **24**

ŞEKİLLER DİZİNİ

Şekil **Sayfa**

Şekil 2.1. Geometrik Örgü....4

Şekil 2.2. İzotop Örgüler....4

Şekil 2.3. Örgü 5

Şekil 2.4. Bileşke işlemi....6

Şekil 2.5. β örgüsü ve tersi 6

Şekil 2.6. Örgü grubunda işlemler....7

Şekil 2.7. Pure (saf) örgü....7

Şekil 2.8. Örgü grubu değişmeli değildir....8

Şekil 2.9. Üreteçler....8

Şekil 2.10. Değişme ve örgü ilişkisi 9

Şekil 2.11. $\sigma_3\sigma_1{}^{-1}\sigma_2{}^{-1}\sigma_2{}^{-1}\sigma_1\sigma_3$ kelimesi 9

Şekil 2.12. β_1....11

Şekil 2.13. $\sigma_1^{-1}\sigma_3\sigma_2\sigma_3\sigma_1$....11

Şekil 2.14. $\sigma_1^{-1}\sigma_3\sigma_2\sigma_1\sigma_3$....11

Şekil 2.15. $\sigma_1^{-1}\sigma_3\sigma_2\sigma_1\sigma_2\ \sigma_2^{-1}\sigma_3$....11

Şekil 2.16. $\sigma_1^{-1}\sigma_3\sigma_1\sigma_2\sigma_1\ \sigma_2^{-1}\sigma_3$....12

Şekil 2.17. β saf örgüsü 13

Şekil 2.18. γ_1 örgüsü....13

Şekil 2.19. $\alpha_1$örgüsü....13

Şekil 2.20. β örgüsü....13

Şekil 2.21. $\gamma_2$örgüsü....14

Şekil 2.22. α_2 örgüsü....14

Şekil 2.23. Taranmış β örgüsü 14

Şekil 2.24. $\beta= \sigma_1^{-2}\ \sigma_2^2$....15

Şekil 2.25. $\beta= \sigma_1^{-2}\ \sigma_2^2 = (\ \sigma_1^{-2}\ \sigma_2^2\ \sigma_1^2)(\ \sigma_1^{-2})$ 15

Şekil 2.26. $\sigma_1^{-1}\,\sigma_1^{-1}\sigma_2\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\,\sigma_1^{-1}\,\sigma_2^{-1}$ 15

Şekil 2.27. $\sigma_1^{-1}\,\sigma_1^{-1}\sigma_2\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\,\sigma_1^{-1}\,\sigma_2^{-1}$ 15

Şekil 2.28. $\sigma_1^{-1}\,\sigma_1^{-1}\sigma_2\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\;\;\sigma_1^{-1}\sigma_1^{-1}\,\sigma_2^{-1}$ 16

Şekil 2.29. $\sigma_1^{-1}\,\sigma_1^{-1}\sigma_2\sigma_2\sigma_1\sigma_2\sigma_2\sigma_1\sigma_2\;\;\sigma_1^{-1}\sigma_1^{-1}\,\sigma_2^{-1}$ 16

Şekil 2.30. $\sigma_1^{-1}\,\sigma_1^{-1}\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\;\;\sigma_1^{-1}\sigma_1^{-1}\,\sigma_2^{-1}$ 16

Şekil 2.31. $\sigma_1^{-1}\,\sigma_1^{-1}\sigma_2\sigma_1\sigma_2\sigma_2\sigma_1\sigma_2\sigma_2\;\;\sigma_1^{-1}\sigma_1^{-1}\,\sigma_2^{-1}$ 16

Şekil 2.32. $\sigma_1^{-1}\,\sigma_1^{-1}\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_2\;\;\sigma_1^{-1}\sigma_1^{-1}\,\sigma_2^{-1}$ 17

Şekil 2.33. $\sigma_1^{-1}\,\sigma_1^{-1}\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1\sigma_2\sigma_2\;\;\sigma_1^{-1}\sigma_1^{-1}\,\sigma_2^{-1}$ 17

Şekil 2.34. a_i üreteci 18

Şekil 2.35. Beta örgüsü 19

Şekil 2.36. Kırmızı renkli şerit düzleştirilecek 19

Şekil 2.37. γ_1 19

Şekil 2.38. γ_1^{-1} 19

Şekil 2.39. $\alpha_1 = \beta\,\gamma_1^{-1}$ 20

Şekil 2.40. Kırmızı şerit düzleştirilecek 20

Şekil 2.41. γ_2 20

Şekil 2.42. $\alpha_2 = \gamma_1\,\gamma_2^{-1}$ 20

Şekil 2.43. $\alpha_3 = \gamma_2$ 21

Şekil 2.44. $\beta = \alpha_1\alpha_2\alpha_3$ 21

Şekil 2.45. β örgüsünün normal formu 22

Şekil 3.1. Çözüm için ihtiyaç duyulan zaman grafiği 23

SİMGELER

Simgeler

B_n	n şeritte örgü grubu
S_n	n şeritte saf örgü grubu
σ_i	i. Örgü grubu üreteci
σ_i^{-1}	i. Örgü grubu üretecinin tersi
$\mathcal{A}_k$	Son şeridi ortadan kaldırıldığında k-1 şeritteki birim örgüyü veren taranmış k- örgülerin kümesi
a_i	$\mathcal{A}_k$ grubunun i. üreteci

GİRİŞ

Örgülerin tarihçesi, yüzyıllar öncesine dayanır ve bilinen ilk evrensel kullanım alanları, süsleme ya da halatlara biçim verme gibi pratik çözümler bulma amacıyla yer bulmuştur. Günümüzde ise örgüler, 'Örgü Teorisi' adı altında soyut modellemeler aracılığıyla tanımlanmaktadır. Örgü teorisi, örgü kavramını ve matematiğin farklı alanlarından ortaya çıkan farklı genellemeleri çalışmaktadır. Örgüleri matematiksel olarak çalışmaya değer kılan şeylerden birisi, örgülerin bir grup yapısına sahip olmasıdır. Yani örgüler üzerinde tanımlı işlem birleşmelidir, her örgünün bir tersi vardır ve son olarak örgü grubunun birim örgü diye adlandırılan bir birim (etkisiz) elemanı vardır. Ancak bu işlemin iyi tanımlı olması için şerit sayısının sabit tutulması gerekir. Dolayısıyla 2 şeritte tanımlı örgüler bir gruptur, 3 şeritte tanımlı örgüler bir gruptur vs...

Örgü teorisi, matematiğin oldukça yeni bir alanıdır: Örgüler ilk olarak 1925 yılında Emil Artin tarafından tanımlanmış ve çalışılmıştır (Artin, 1925). Örgüler, her alanda karşımıza çıkabilecek objelerdir: Örgüler ve örgülerin bazı genellemeleri topoloji ve grup teori gibi alanlarda çalışılmaktadır.

Özellikle 1930'lardan bu yana, Alexander ve Markov tarafından örgüler ile düğümler arasında güçlü ilişkiler olduğu ortaya konulmuştur (Alexander, 1923). Bu güçlü bağ, 1980'lerde Jones'un örgü teorisi sayesinde düğümler için bir değişmez tanımlamasına da oldukça katkı sağlamıştır (Jones, 1985). Bunlara ek olarak, örgü teorisinin cebirsel geometri ve yansımalar tarafından üretilen sonlu gruplar teorisi gibi alanlarla da ilginç ilişkileri olduğu ortaya konulmuştur.

Bunlara ek olarak örgü teorisi kuantum fiziği alanında da sıklıkla kullanılır. Kuantum fiziği bağlamında örgü gruplarını ve ilgili topolojik kavramları içeren bir başka yoğun araştırma alanı, sözde anyonların teorisi ve bunların deneysel olarak uygulanmasıdır. Bunlar, hata düzeltmeli kuantum hesaplamanın temelini oluşturmaktadır ve bu nedenle bu çalışmalar şu anki kuantum bilgisinde temel öneme sahiptir.

Özellikle geçtiğimiz 25 yıl içerisinde; güvenliği örgü grubundaki kombinatoryal grup teoritik problemlerin çözümüne bağlı çok sayıda açık anahtar kriptosistemleri geliştirilmiştir. Kombinatoryal grup teorisi, kriptosistemlerin güvenliğinin dayanacağı çözülmesi zor problemler bulabilme açısından oldukça verimli bir alandır. Emil Artin tarafından tanımlanan örgü grubu ise birçok açıdan ilginç özelliklere sahiptir: Örgü grubunun hepsi birbirine denk olan farklı temsilleri vardır ve bu temsiller birbirinden çok farklı alanlarda kullanılmaktadır. Bunun dışında örgü grubu birçok problem içermektedir. Örneğin, kelime problemi (örgü grubunun herhangi iki elemanının birbirine eşit olup olmadığını belirleme problemi) veya dekompozisyon problemi (verilen kelimeyi daha basit faktörlerin çarpımı şeklinde yazma), konjuge problemi

(verilen iki elemanın birbirine konjuge olup olmadığını belirleme) gibi problemler halen açık problemlerdir. Konjuge problemini daha açık bir şekilde ifade etmek istersek, verilen herhangi iki x, y elemanı için, grubun $x = zyz^{-1}$ eşitliğini sağlayacak bir z elemanı olup olmadığını belirleme problemi olarak tanımlayabiliriz.

Biz bu tezde kelime problemi ve bunun çözümü olan algoritmayı çok güzel ve açıklayıcı videolarla desteklenmiş olan, (Dalvit,2011) kaynağından takip ederek anlatacağız.

Yakın zamanda güvenliği örgü grubuna ve örgü grubu ile ilgili problemlere dayalı olan iki önemli kriptosistem geliştirilmiştir. Bunlardan ilki Anshel ve Goldfield tarafından 1999'da (Anshel et al., 1999), ikincisi ise Ko ve Lee tarafından 2000 yılında geliştirilmiştir (Ko et al., 2000)(Birman et al., 1998). Geliştirilen bu kriptosistemlerin oldukça ses getirmesi, örgü grubu ve kriptografi ilişkisi hakkında geniş tartışmalara yol açmıştır.

1.BÖLÜM

ÖRGÜ TEORİSİ

1.1 Geometrik Örgüler

Geometrik örgünün tanımını vermeden önce, gözümüzde örgüleri nasıl canlandırabileceğimizi anlatmaya çalışalım. Uzayda birbirine paralel iki disk alalım. Daha sonra geometrik örgüyü, bir ucu verilen disklerden birinin üzerinde, diğer ucu da diğer diskin üzerinde sabit olan belirli sayıda tellerin oluşturduğu yapı olarak düşünebiliriz. Dolayısıyla bu tanımın sonucunda, verilen diskler arasında bu disklere paralel olan herhangi bir düzlem, her tel ile yalnızca bir kere kesilir. Geometrik örgülerin matematiksel tanımı ise aşağıdaki gibi verilir:

Tanım 1.1. Geometrik Örgü (Artin, 1950): Bir D diski ve bu diskin içinde n tane $p_1, p_2, \ldots, p_n$ noktaları verilsin. n tel (strand) üzerinde bir geometrik örgü, aşağıda verilen koşulları sağlayan bir $b_i: I \to I \times D$ fonksiyonlarının sıralı n'lisidir.

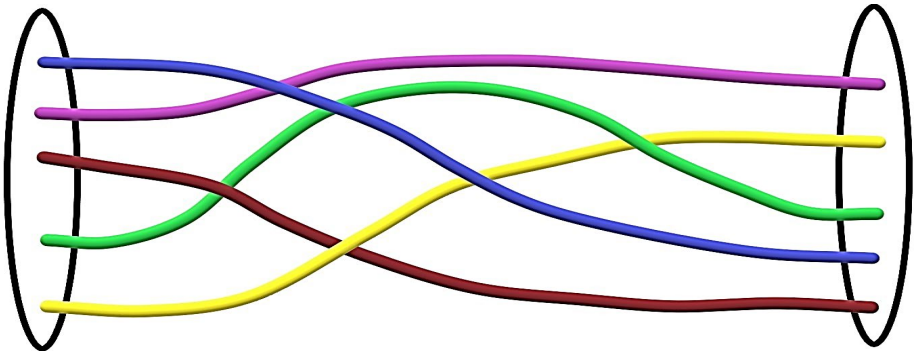
1. $\forall t \in I, b_i(t) \in \{t\} \times D$
2. $\forall i\ 1 \le i \le n, b_i(0) = (0, p_i)$
3. $b_i(1) = (1, p_{\pi(i)})$ koşulu sağlanacak şekilde bir $\pi \in S_n$ permütasyonu vardır.
4. $\forall t \in I, \forall i \neq j, b_i(t) \neq b_j(t)$

Bir önceki tanımda, geometrik örgü ile sadece $b_i\ 1 \le i \le n$ fonksiyonlarını değil, ayrıca görüntülerin oluşturduğu $(b_1(I), b_2(I), \ldots, b_n(I))$ sıralı n'liyi de belirtmiş oluyoruz.

Hem b_i hem de $b_i(I)$, örgünün i. ipliği olarak adlandırılır.

Ayrıca yukarıdaki tanımda belirtildiği gibi her örgü bir π permütasyonu belirtir. Diğer bir deyişle, her örgüye karşılık gelen bir permütasyon vardır.

Örneğin, şekil 2.1'de gösterilen örgüyü göz önüne alalım. Bu örgüye karşılık gelen permütasyon (14523) olur.

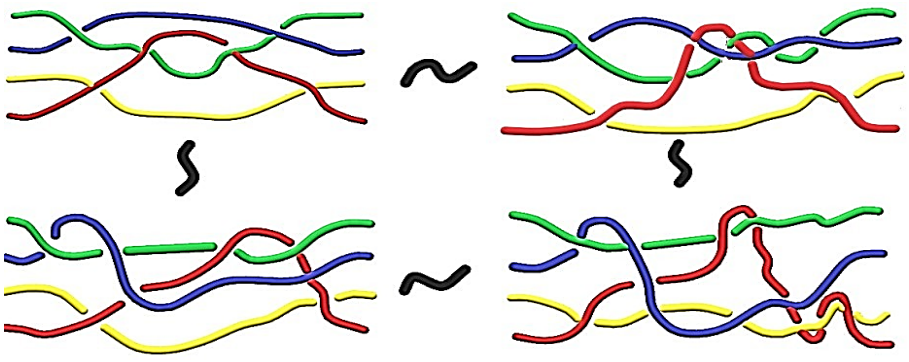


Şekil 2.1. Geometrik Örgü

1.2 Örgüler ve İzotopi

Eğer iki örgünün tellerinin (strand) bağlanma şekli aynı ise bu iki örgü eşdeğer kabul edilir. Diğer bir deyişle, verilen iki örgünün eşdeğer olup olmadığına bakarken, örgünün tellerini (strand) uzayda birer eğri olarak düşünürsek, bu eğrileri parametrize eden eşitlikler yerine (geometri), onların birbirine bağlanma şekilleri (topoloji) ile ilgileneceğiz. Sonrasında, eğer bir örgüden, tellerin (strand) uçlarını sabit tutarak ve telleri kesmeden (sürekli deformasyon) deforme ederek diğer bir örgüyü elde edebiliyorsak, bu iki örgüyü eşdeğer kabul edeceğiz.

Örneğin, şekil 2.2'de verilen 4 örgü birbirine eşdeğerdir.



Şekil 2.2. İzotop Örgüler

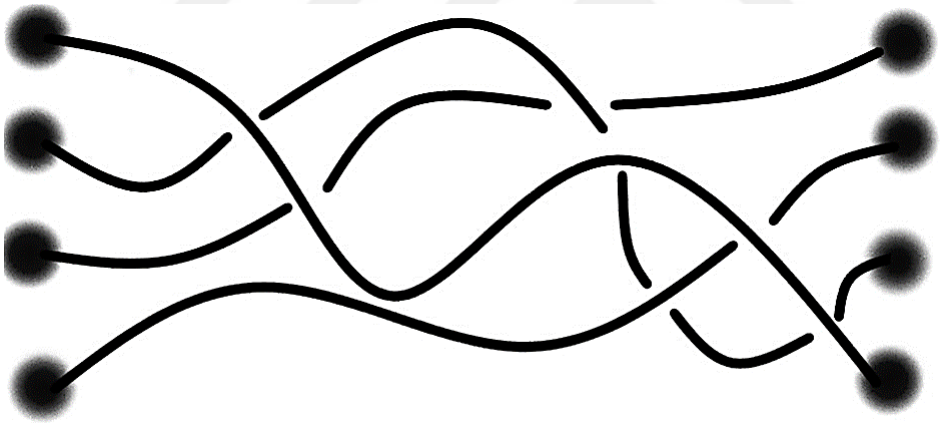
İzotopi kavramı ile ilgili daha matematiksel bir tanım vermek gerekirse, bu tanım verilebilir:

Tanım 1.2. Örgü İzotopisi: Herhangi iki β ve α n− örgüleri arasındaki izotopi, aşağıda verilen üç koşulu sağlayan $F_i : I\times I \to I\times D$ sürekli fonksiyonlarının sıralı n'lisi $(F_1, F_2, \ldots, F_n)$'dir.

1. $\forall t \in I, F_i(\{t\} \times I)_{i=1,2,\ldots,n}$ bir n−geometrik örgüdür.
2. $F_i(\{0\}\times I)_{i=1,2,\ldots,n} = \beta$
3. $F_i(\{1\}\times I)_{i=1,2,\ldots,n} = \alpha$

İzotop olma bağıntısı, bir denklik bağıntısıdır. Denklik sınıfları örgüler ya da n örgüler olarak adlandırılır.

Tanımdan da kolayca anlaşılacağı üzere, iki geometrik örgü arasındaki izotopi permütasyonu korur. Diğer bir deyişle, örgüye karşılık gelen permütasyon bir invaryanttır (değişmezdir). Örgüler arasındaki izotop olma bağıntısı bir denklik bağıntısıdır. Bu bağıntı altında denklik sınıfları örgüler ya da n− örgüler olarak adlandırılır. Örgüler ile çalışırken, daha kullanışlı olması bakımından şekil 2.3'teki figürde gösterilen ve örgü diyagramı adı verilen 2 boyutlu çizimler tercih edilir.



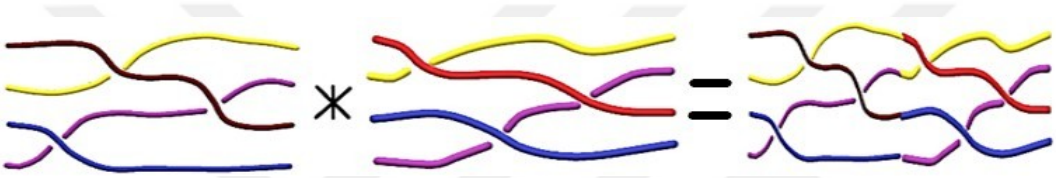
Şekil 2.3. Örgü

Herhangi iki örgü verildiğinde, bu örgülerin bileşkesinden bahsedebiliriz: Aşağıda şekil 2.4'te gösterildiği gibi, 1. örgünün bitim noktaları ile 2. örgünün başlangıç noktaları çakıştırıldığında, yeni bir örgü elde edilir. Elde edilen yeni örgüye bu iki örgünün bileşkesi adı verilir.

Tanım 1.3. $\beta = (b_1, b_2, ..., b_n)$ *ve* $\alpha = (c_1, c_2, ..., c_n)$ *örgüleri verilsin. Bu örgülere karşılık gelen permütasyonlara da sırasıyla* π *ve* σ *diyelim.* $\beta \star \alpha$ *ile gösterilen* β *ve* α *örgülerinin bileşkesi* $(d_1, d_2, ..., d_n)$ *olarak tanımlanır öyle ki:*

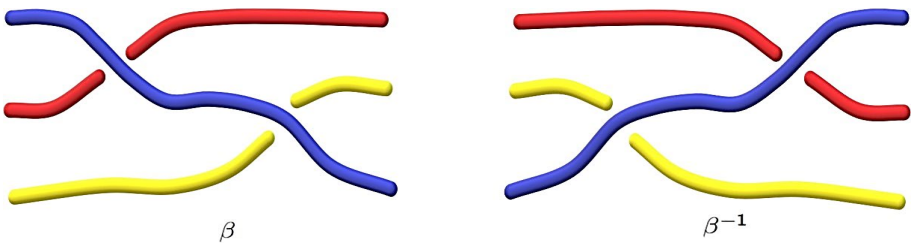
$$d_i(t) = \begin{cases} b_i(2t), & t \in \left[0, \frac{1}{2}\right] \\ c_{\pi(i)}(2t - 1), & t \in \left[\frac{1}{2}, 1\right] \end{cases}$$

Şekil 2.4' te görüldüğü gibi, böylece $\beta \star \alpha$ de bir n- örgüdür ve bu örgüye karşılık gelen permütasyon $\sigma\pi$ olur.



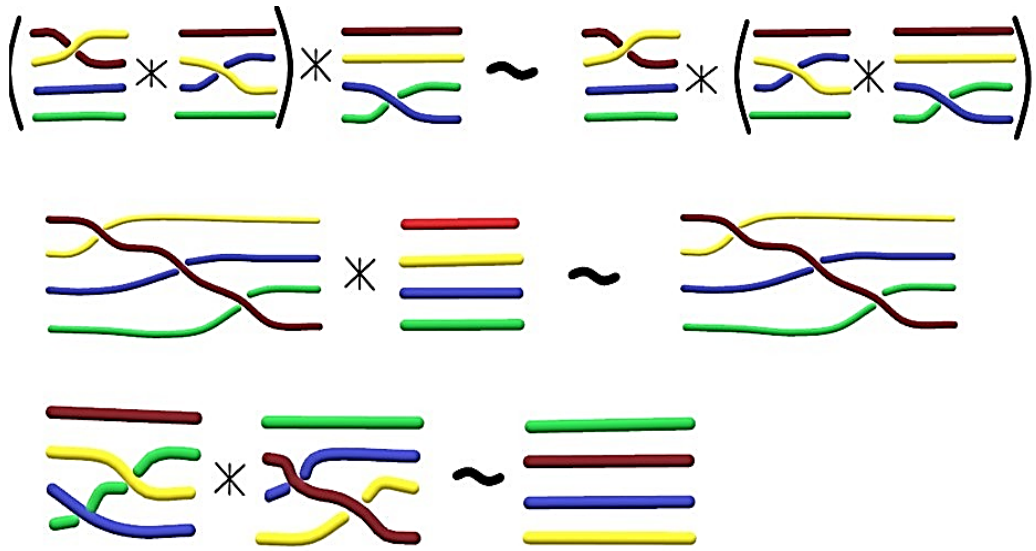
Şekil 2.4. Bileşke işlemi

Verilen herhangi bir $\beta = (b_1, b_2, ..., b_n)$ örgüsü için, bu örgünün yukarıda tanımlanan bileşke işlemine göre tersini belirleyebiliriz: Her $t \in I$ için $b_i^{-1}(t) = b_i(1 - t)$ olarak tanımlanırsa, $\beta^{-1} = (b_1^{-1}, b_2^{-1}, ..., b_n^{-1})$ istenen örgü olur. Diğer bir deyişle, örgüsünün $x = \frac{1}{2}$ doğrusuna göre simetriğini alarak β^{-1} örgüsünü elde edebiliriz.



Şekil 2.5 β örgüsü ve tersi

Her $n \geq 1$ için, n tel (strand) üzerinde örgülerin oluşturduğu küme, yukarıda tanımlanan bileşke işlemine göre bir gruptur. Grup özellikleri, şekil 2.6'da açıkça görüldüğü gibi sağlanır. Bu gruba Artin Örgü Grubu denir ve B_n ile gösterilir.

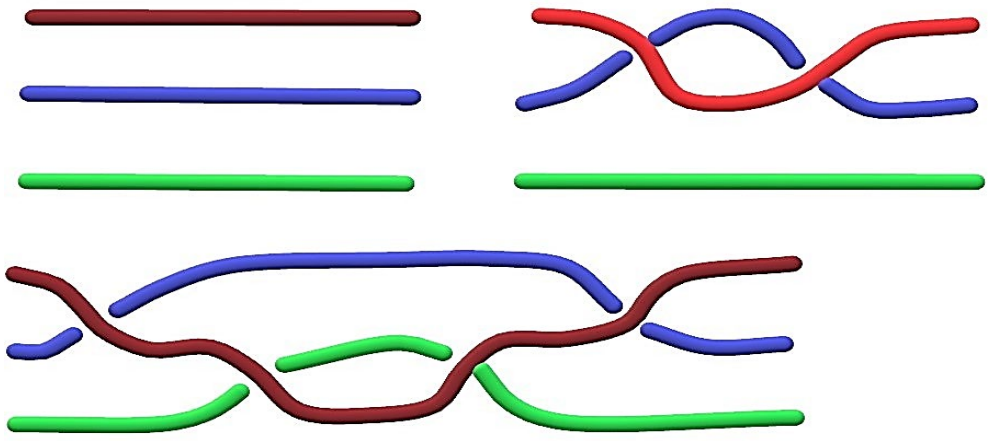


Şekil 2.6 Örgü grubunda işlemler

Herhangi bir $\beta \in B_n$ örgüsüne bir π permütasyonunun karşılık geldiğini biliyoruz. Özel olarak, bu örgülerden permütasyonu sadece birim permütasyon olanları düşünelim. Aşağıdaki tanımda görüldüğü gibi, B_n kümesinin bu alt kümesine özel bir ad verilmektedir.

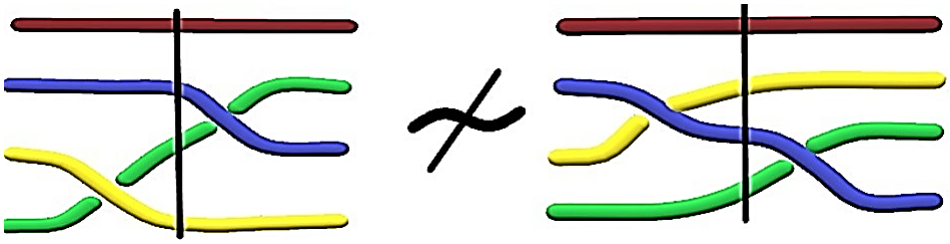
Tanım 1.4. Verilen herhangi bir örgüyü, o örgüye karşılık gelen permütasyona eşleyen $\phi : B_n \to S_n$ homomorfizmasının çekirdeği, B_n kümesinin bir alt grubudur ve bu kümeye Pure (saf) Örgüler kümesi adı verilir ve P_n ile gösterilir. (Bu tanımda S_n ile simetrik grup gösterilmektedir.)

Şekil 2.7'deki figürde çeşitli Pure (saf) örgü örnekleri görülmektedir:



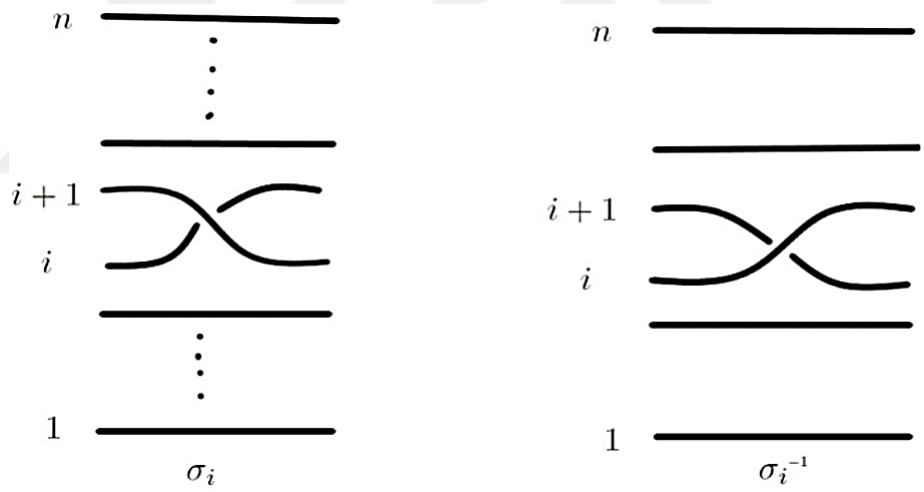
Şekil 2.7 Pure (saf) örgü

B_n kümesi, üzerinde tanımlanan bileşke işlemine göre değişmeli olmayan bir gruptur. Şekil 2.8'de bu durum açıkça görülmektedir:



Şekil 2.8 Örgü grubu değişmeli değildir.

Her n ≥ 1 için B_n kümesi üzerinde bir grup yapısı olduğunu biliyoruz. Herhangi bir örgü diyagramına bakıldığında, diyagramın çaprazlamalardan oluştuğunu görüyoruz. Herhangi 1 ≤ i ≤ n için i. tel ile i + 1. tel arasında açıkça sadece iki tür çaprazlama gerçekleşebilir: Bu çaprazlamaya i. telin i+ 1. telin üzerinden geçmesiyle ya da tam tersi durumun gerçekleşmesi ile oluşur. Bu çaprazlamalara temel örgü adı verilmektedir. Açıkça görüleceği gibi her örgü, temel örgülerin birleşiminden oluşur. Diğer bir deyişle, elementer örgüler B_n grubu için üreteç görevi görmektedir. Şekil 2.9'da görüldüğü gibi bu iki çaprazlama sonucunda oluşan temel örgüler, σ_i ve σ_i^{-1} ile gösterilmektedir.



Şekil 2.9 Üreteçler

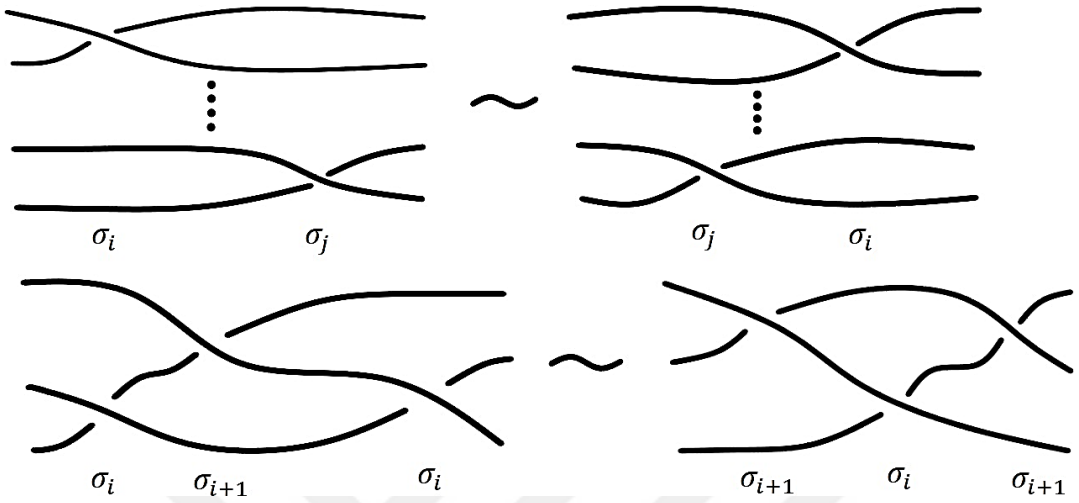
Yukarıdaki paragraftan hareketle, şu teorem verilebilir:

Teorem 1.1. *(Artin, 1925)* n ≥ 1 *olsun. Temel örgüler* $\sigma_1, \sigma_2, \ldots, \sigma_n$, B_n *grubunun üreteçleridirler. Grup bağıntıları aşağıda verilmiştir.*

$$|i - j| > 1 \Rightarrow \sigma_i\sigma_j = \sigma_j\sigma_i \quad \textit{olur.}$$

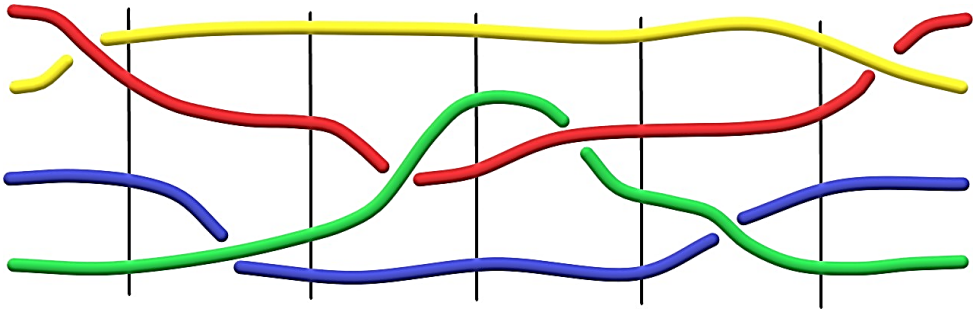
$$1 \le i \le n-2 \Rightarrow \sigma_i\sigma_{i+1}\sigma i = \sigma_{i+1}\sigma_i\sigma_{i+1} \quad \textit{sağlanır.}$$

Yukarıdaki teoremde verilen grup bağıntıları, yani $|\mathbf{i}-\mathbf{j}|>1$ ise değişme özelliği ve $1 \leq \mathbf{i} \leq \mathbf{n}-2$ ise örgü bağıntısı şekil 2.10'da görüldüğü gibi sağlanmaktadır.



Şekil 2.10 Değişme ve örgü ilişkisi

Yukarıdaki tanım ve teoremin sonucunda, her $n \geq 1$ için n tel (strand) üzerinde örgü grubu B_n, sonlu sayıda eleman tarafından üretilen (sonlu üretilen) ancak sonsuz elemanlı bir gruptur. Artin üreteçlerinin tanımı ve yine yukarıdaki teoremin sonucunda, her $\beta \in B_n$ örgüsü, Artin üreteçlerinden oluşan bir kelime (word) belirtir. Örnek vermek gerekirse, şekil 2.11'deki figürde verilen örgüye karşılık gelen kelime $\sigma_3\sigma_1^{-1}\sigma_2^{-1}\sigma_2^{-1}\sigma_1\sigma_3$ dir.



Şekil 2.11. $\sigma_3\sigma_1^{-1}\sigma_2^{-1}\sigma_2^{-1}\sigma_1\sigma_3$ kelimesi

1.3 Kelime Problemi

Kelime problemi en genel haliyle, verilen iki matematiksel ifadenin birbirine denk olup olmadığını belirleme problemidir. Bu problemin en tipik örnekleriyle grup teorisinde karşılaşırlar. Giriş kısmında bahsedilen üç problem (kelime problemi, konjuge problemi, izomorfizma problemi), kombinatoryal grup teorisi adlı alanda çalışılmaktadır ve hepsi olmasa da, bazı grup temsilleri için bu problemler çözülmüştür.

Diğer bir deyişle, etkili ve verimli algoritmalar bulunmuştur. Bunlara karşın, yukarıdaki üç problemden görece en kolay olanının, yani kelime probleminin bile çözülemediği gruplar vardır.

Bazı durumlarda ise problem çözülüyor olsa bile, yani elimizde bir algoritma olsa bile bu algoritma pek verimli olmayabilir. Algoritmanın verimli olmaması, karmaşıklığının çok fazla olmasından dolayı pratikte işlem yapmanın çok zor hatta bazı durumlarda imkansız olması demektir. Bir algoritmanın karmaşıklığı, problemi çözmek için ne kadar işlem yapmanın gerektiğini belirleyen bir ölçüttür.

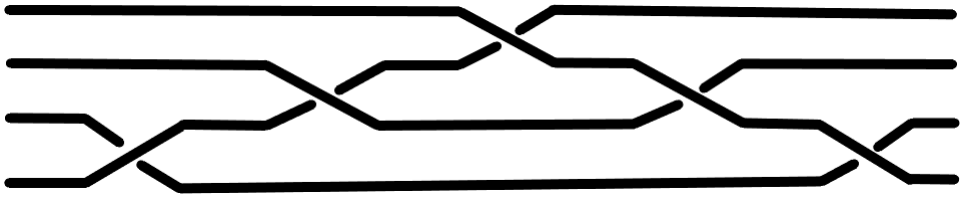
Kombinatoryal grup teorisinde araştırılan bir başka problem ise genelleştirilmiş kelime problemidir. Problemin tanımı şu şekildedir: Kabul edelim ki, B_n ve H B_n in alt grubu verilsin. Eğer w ϵ B_n ise w ϵ H olur mu? (H={1} olduğunda bu bize kelime problemini verir). Dolayısıyla yukarıda bahsedilen kelime problemi, az önce bahsedilen genelleştirilmiş kelime probleminin özel bir halidir.

Örgü gruplarında ise, kelime ve konjuge problemleri çözülmüştür. Diğer bir deyişle, çözüm için çeşitli algoritmalar mevcuttur. Üstelik, bu algoritmalardan bazıları oldukça etkili ve verimlidir.

Örgü Grubunda Kelime Problemi**:** Herhangi iki β_1 ve β_2 örgüleri verilsin. Bu iki örgü birbirine izotop mudur değil midir?

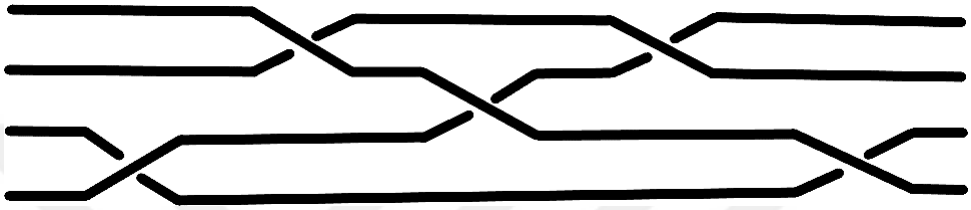
Dikkat edilirse yukarıdaki problemi çözmenin, verilen herhangi bir örgünün birim örgüye denk olup olmadığını belirlemekle eşdeğer olduğu kolayca görülür. Bunun sebebi, eğer $\beta_1 = \beta_2$ ise $\beta_1\beta_2^{-1} = 1$ dir.

Örnek: $\beta_1 = \sigma_1^{-1}\sigma_2\sigma_3\sigma_2\sigma_1$ ile $\beta_2 = \sigma_1^{-1}\sigma_3\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_3$ örgüleri verilsin. Bu iki örgünün birbirine izotop olup olmadığını belirlemeye çalışalım. Öncelikle şekil 2.12'de verilen β_1 örgüsünü dikkate alalım:



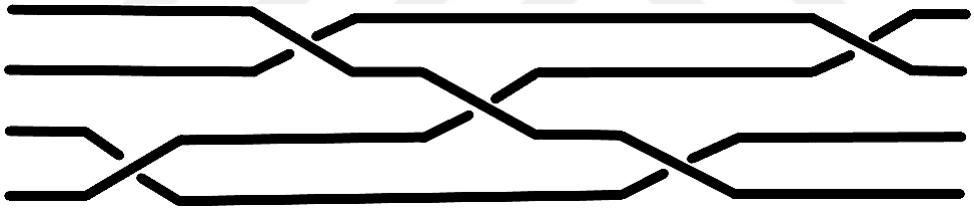
Şekil 2.12. β_1

$\sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3$ eşitliğini kullanarak, β_1 örgüsünün şekil 2.13'te verilen $\sigma_1{}^{-1}\sigma_3\sigma_2\sigma_3\sigma_1$ örgüsüne izotop olduğu görülür.



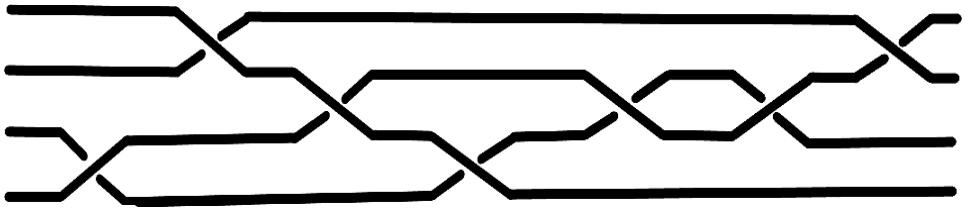
Şekil 2.13. $\sigma_1{}^{-1}\sigma_3\sigma_2\sigma_3\sigma_1$

Daha sonra $\sigma_1\sigma_3 = \sigma_3\sigma_1$ eşitliğini kullanırsak, $\sigma_1{}^{-1}\sigma_3\sigma_2\sigma_3\sigma_1$ örgüsünün şekil 2.14'te verilen $\sigma_1{}^{-1}\sigma_3\sigma_2\sigma_1\sigma_3$ örgüsüne izotop olduğunu görürüz.



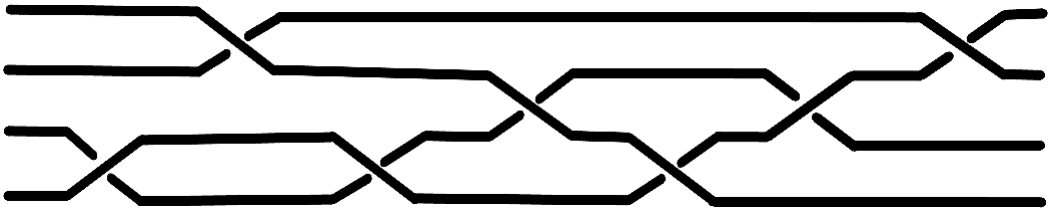
Şekil 2.14. $\sigma_1{}^{-1}\sigma_3\sigma_2\sigma_1\sigma_3$

$\sigma_2\sigma_2{}^{-1}$ örgüsü birim örgüye izotop olduğundan, $\sigma_1{}^{-1}\sigma_3\sigma_2\sigma_1\sigma_3$ örgüsü, şekil 2.15'te gösterilen $\sigma_1{}^{-1}\sigma_3\sigma_2\sigma_1\sigma_2\sigma_2{}^{-1}\sigma_3$ örgüsüne izotoptur.



Şekil 2.15. $\sigma_1{}^{-1}\sigma_3\sigma_2\sigma_1\sigma_2\sigma_2{}^{-1}\sigma_3$

Elde ettiğimiz örgüde $\sigma_2\sigma_1\sigma_2 = \sigma_1\sigma_2\sigma_1$ eşitliğini kullanırsak, bu örgünün şekil 2.16'da verilen $\beta_2 = \sigma_1{}^{-1}\sigma_3\sigma_1\sigma_2\sigma_1\sigma_2{}^{-1}\sigma_3$ örgüsüne izotop olduğu görülür.



Şekil 2.16. $\beta_2 = \sigma_1{}^{-1}\sigma_3\sigma_1\sigma_2\sigma_1\sigma_2{}^{-1}\sigma_3$

Dolayısıyla β_1 ve β_2 örgüleri izotoptur.

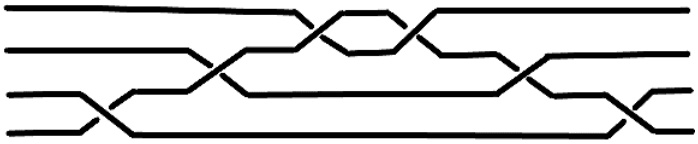
Yukarıdaki örnekte de görüleceği gibi, örgü grubu bağıntılarını kullanarak iki örgünün birbirine izotop olduğunu gösterebiliriz. Diğer bir deyişle verilen herhangi iki örgüden bir tanesine sonlu tane örgü grubu bağıntısı kullanarak diğerini elde edebiliyorsak, bu iki örgü birbirine izotoptur deriz. Ancak tahmin edileceği gibi, bu her zaman mümkün değildir. Bunun birinci sebebi, verilen örgüler çok karmaşık olabilir. Örneğin 50 şeritte verilen iki örgünün birbirine izotop olduğunu örgü grubu bağıntılarını kullanarak göstermek çok kolay bir işlem olmayacaktır. İkinci sebep ise, verilen örgüler izotop olmayabilir. Bundan dolayı, kelime probleminin çözümü için verimli bir algoritmaya ihtiyaç vardır. Daha açık ifade etmek gerekirse, herhangi iki örgüyü girdi olarak kabul eden ve çıktı olarak evet ya da hayır (İzotoptur ya da izotop değildir) cevabını veren bir algoritmaya ihtiyaç vardır.

1.3.1. Artin tarama algoritması

Artin örgü tarama algoritması kelime problemini çözmek için tasarlanmıştır. Bu algoritma Artin (Artin, 1925) tarafından keşfedilmiştir. β ile B_n örgü grubunun rastgele bir elemanını göstersin. Kelime problemi, β örgüsünün birim örgüye izotopik olup olmadığını belirleme problemidir. Şimdi Artin Tarama Algoritmasının ne olduğunu adım adım açıklayalım.

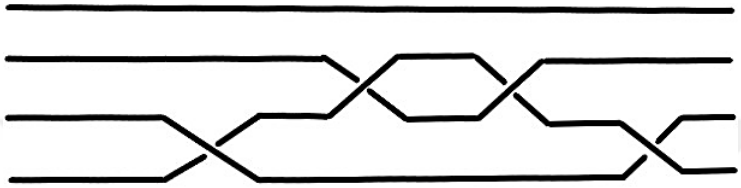
Tanım 1.5. Herhangi $\beta \in B_n$ örgüsü için, eğer karşılık gelen permütasyon σ_β birim permütasyona eşit ise, bu örgüye **saf örgü** denir.

1.Adım: Herhangi bir $\beta \in B_n$ örgüsü verilsin. Öncelikle bu örgünün bir saf örgü olup olmadığı belirlenmelidir. Çünkü birim örgü bir saf örgüdür. Dolayısıyla β örgüsü eğer saf örgü değilse birim örgüye denk olamaz. Örgünün saf olup olmadığını belirleme işlemi ise oldukça kolaydır. Yapılması gereken tek şey örgüye karşılık gelen permütasyonu bulup, bu permütasyonun birim permütasyon olup olmadığına bakılmasıdır. Eğer permütasyon birim permütasyon değil ise, örgü saf örgü değildir. Tersine, eğer permütasyon birim permütasyon ise verilen örgü bir saf örgüdür. O halde β örgüsünün saf bir örgü olduğunu kabul edelim. Eğer örgü bir saf örgü ise ikinci adıma geçilir.



Şekil 2.17. β saf örgüsü

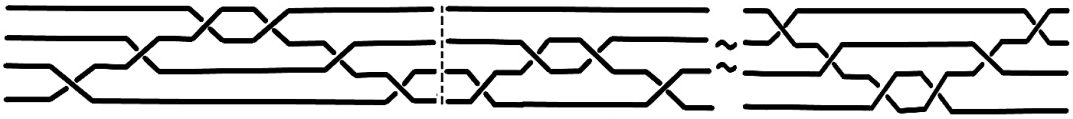
2.Adım: İlk olarak, β örgüsünün son şeridi silinir ve yerine diğer örgülerle çaprazlama içerisinde olmayan düz bir şerit yerleştirilir. Bu işlem sonucunda elde edilen yeni örgüye γ_1 adını verelim. Şekil 2.17'deki β- örgüsüne bu işlemi yaptığımızda şekil 2. 18'deki γ_1 örgüsünü elde ederiz.



γ_1

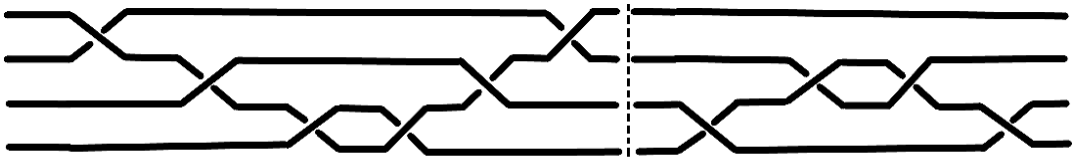
Şekil 2.18. γ_1 örgüsü

Şimdi de $\alpha_1 = \beta\gamma_1{}^{-1}$ örgüsünü dikkate alalım. Eğer bu örgünün son şeridi ortadan kaldırırsak, yukarıdaki şekilden de açıkça görüleceği üzere n – 1 şeritteki birim örgüyü elde ederiz. Dolayısıyla, α_1 örgüsünü ilk n−1 şeridi düz, sonuncu şeridi ise onun altındaki şeritlerle bağlanabilecek formda olan bir örgü olarak düşünebiliriz. Bu formdaki örgüye taranmış örgü denir. Aşağıda verilen şekil 2.19 ve şekil 2.20 bu prosedürü anlatmaktadır.



$\alpha_1 = \beta\gamma_1^{-1}$

Şekil 2.19. α_1 örgüsü

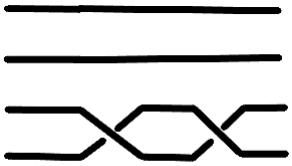


$\beta = \alpha_1\gamma_1$ Sol taraftaki örgü taranmış örgüdür.

Şekil 2.20. β örgüsü

α_1 örgüsünün tanımını tekrar yazarsak, $\beta = \alpha_1\gamma_1$ eşitliğini elde ederiz.

Öncelikle γ_1 örgüsünü dikkate alalım. Bu örgünün ilk n − 1 şeridinde çaprazlamalar olup, son şeridi düz bir şerittir. Bu örgünün sondan ikinci şeridini (n-2.) kaldırıp yerine diğer örgülerle çarprazlama yapmayan düz bir şerit koyalım ve bu işlem sonucunda elde ettiğimiz örgüyü γ_2 ile gösterelim. Şekil 2.21 γ_2 figürünü göstermektedir.



γ_2

Şekil 2.21. γ_2 örgüsü

$\alpha_2 = \gamma_1\gamma_2^{-1}$

Şekil 2.22. α_2 örgüsü

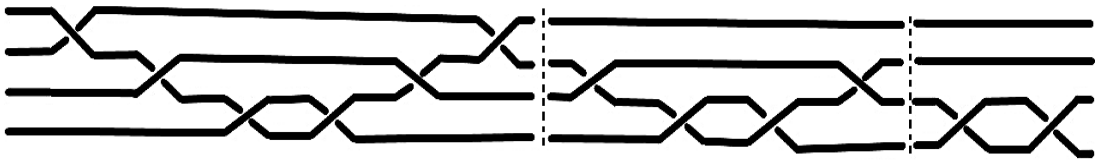
$\alpha_2 = \gamma_1\gamma_2^{-1}$ örgüsü şu forma sokulabilir: n − 2 şerit düz, n − 1. şerit kendisinden önce gelen şeritlerle çaprazlama yapabilir, n. yani son şerit ise düz. O halde, α_2 örgüsü taranmış, bir örgüdür ve aşağıdaki eşitlik sağlanır:

$$\beta = \alpha_1\alpha_2\gamma_2$$

Yukarıda uygulanan prosedürü n − 1 kere uygulayarak,

$$\beta = \alpha_1\alpha_2 \ldots \alpha_{n-1}$$

dekompozisyonunu elde ederiz. Daha önce belirtildiği gibi, bu dekompozisyonda α_i her $i \in \{1, 2, ..., n-1\}$ için taranmış, bir örgüdür. Daha açık olmak gerekirse; α_i örgüsünde (n+1−i). şerit haricindeki bütün şeritler düz, yani hiçbir çarprazlama yapmaz, (n +1 − i). şerit ise 1, 2, …n − i. Şeritlerle çarpazlama yapabilir. Şekil 2.23'de verilen figür $\beta = \alpha_1\alpha_2 \ldots \alpha_{n-1}$ dekompozisyonunu göstermektedir.

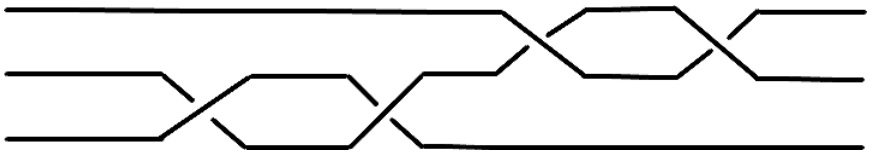


Beta taranmış örgüsü; $\beta = \alpha_1\alpha_2\alpha_3$

Şekil 2.23. Taranmış β örgüsü

Şimdi $\beta = \sigma_1^{-2}\sigma_2^{2}$ kelimesinin bu forma nasıl dönüştürdüğümüzü gösteren bir örnek verelim.

Örnek: $\beta = \sigma_1^{-2}\sigma_2^2$ Örgüsünü dikkate alalım.



Şekil 2.24. $\beta = \sigma_1^{-2}\sigma_2^2$

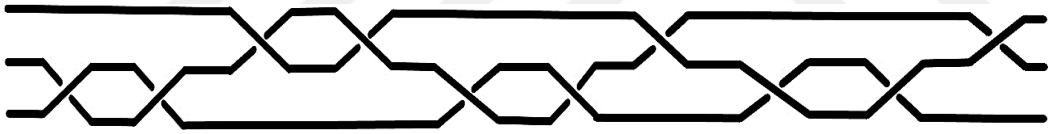
Artin Örgü Tarama Algoritmasındaki adımları uygulayarak bu örgüyü taranmış örgüler cinsinden yazmak istersek $\alpha_1 = \sigma_1^{-2}\sigma_2^2\,\sigma_1^2$ ve $\alpha_2 = \sigma_1^{-2}$ taranmış örgülerini elde ederiz. Şekil 2.25'da verilen şekil, bu işlemi göstermektedir.

Şekil 2.25. $\beta = \sigma_1^{-2}\sigma_2^2 = (\sigma_1^{-2}\sigma_2^2\sigma_1^2)(\sigma_1^{-2})$

Daha açık olmak gerekirse, şu eşitliği elde ederiz:

$$\beta = \sigma_1^{-2}\sigma_2^2 = (\sigma_1^{-2}\sigma_2^2\sigma_1^2)(\sigma_1^{-2})$$

Şimdi $\alpha_1 = \sigma_1^{-2}\sigma_2^2\sigma_1^2$ örgüsünü dikkate alalım. Bu örgünün sağına $\sigma_2\sigma_1\sigma_1^{-1}\sigma_2^{-1}$ birim örgüsünü ekleyerek, aşağıdaki α_1 örgüsüne izotop olan ve şekil 2.26'de verilen

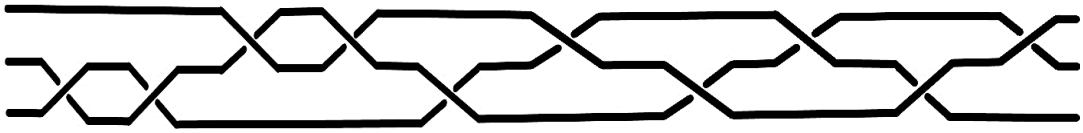


Şekil 2.26. $\sigma_1^{-1}\sigma_1^{-1}\sigma_2\sigma_2\sigma_1\sigma_1\,\sigma_2\sigma_1\sigma_1^{-1}\sigma_2^{-1}$

$$\sigma_1^{-1}\sigma_1^{-1}\sigma_2\sigma_2\sigma_1\sigma_1\,\sigma_2\sigma_1\sigma_1^{-1}\,\sigma_2^{-1}$$

örgüsü elde edilir.

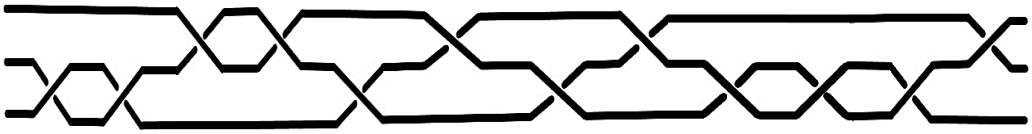
Elde edilen son örgüde, $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ dönüşümü yaparak, aşağıda şekil 2.27'de verilen



Şekil 2.27. $\sigma_1^{-1}\sigma_1^{-1}\sigma_2\sigma_2\,\sigma_1\sigma_2\sigma_1\,\sigma_2\sigma_1^{-1}\sigma_2^{-1}$

$$\sigma_1^{-1}\sigma_1^{-1}\sigma_2\sigma_2\,\sigma_1\sigma_2\sigma_1\;\sigma_2\sigma_1^{-1}\sigma_2^{-1}$$

Daha sonra bu örgüde, σ_2 ile σ_1^{-1} üreteçleri arasına $\sigma_1\sigma_1^{-1}$ birim örgüsü eklenerek, buörgüye izotop olan ve şekil 2.28'da verilen

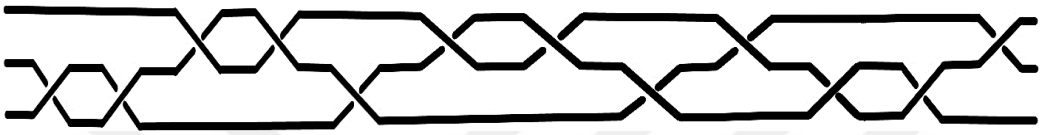


Şekil 2.28. $\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\ \sigma_1\sigma_1{}^{-1}\ \sigma_1{}^{-1}\sigma_2{}^{-1}$

$$\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\ \sigma_1\sigma_1{}^{-1}\ \sigma_1{}^{-1}\sigma_2{}^{-1}$$

örgüsü elde edilir.

Elde edilen son örgüde, $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ dönüşümü yaparak, şekil 2.29'da verilen

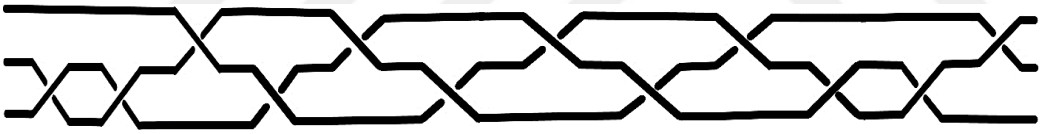


Şekil 2.29. $\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2\ \sigma_1\sigma_2\sigma_1\ \sigma_2\sigma_1\sigma_2\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2{}^{-1}$

$$\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2\ \sigma_1\sigma_2\sigma_1\ \sigma_2\sigma_1\sigma_2\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2{}^{-1}$$

örgüsü elde edilir.

Benzer şekilde $\sigma_2\sigma_1\sigma_2 = \sigma_1\sigma_2\sigma_1$ dönüşümü yaparak, şekil 2.30'de verilen

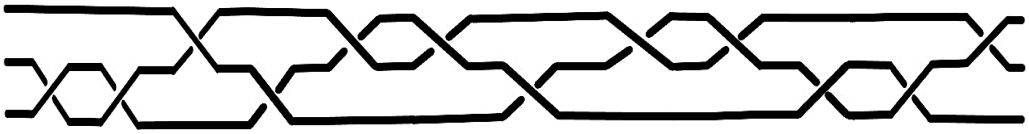


Şekil 2.30. $\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2\ \sigma_2\sigma_1\sigma_2\ \sigma_2\sigma_1\sigma_2\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2{}^{-1}$

$$\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2\ \sigma_2\sigma_1\sigma_2\ \sigma_2\sigma_1\sigma_2\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2{}^{-1}$$

örgüsü elde edilir.

Yine bu örgüde $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ dönüşümü yapılırsa, şekil 2.31'de gösterilen

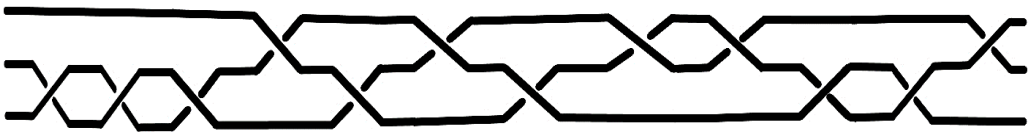


Şekil 2.31. $\sigma_1{}^{-1}\sigma_1{}^{-1}\ \sigma_2\sigma_1\sigma_2\ \sigma_2\sigma_1\sigma_2\sigma_2\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2{}^{-1}$

$$\sigma_1{}^{-1}\sigma_1{}^{-1}\ \sigma_2\sigma_1\sigma_2\ \sigma_2\sigma_1\sigma_2\sigma_2\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2{}^{-1}$$

örgüsü elde edilir.

Elde edilen son örgüde $\sigma_2\sigma_1\sigma_2 = \sigma_1\sigma_2\sigma_1$ dönüşümü yaparak, şekil 2.32'de verilen

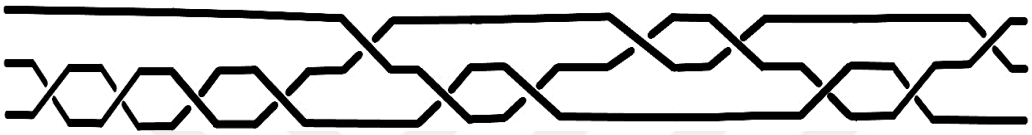


Şekil 2.32. $\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_1\sigma_2\ \sigma_1\sigma_2\sigma_1\ \sigma_2\sigma_2\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2{}^{-1}$

$\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_1\sigma_2\ \sigma_1\sigma_2\sigma_1\sigma_2\sigma_2\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2{}^{-1}$

örgüsü elde edilir.

Son olarak bu örgüde $\sigma_2\sigma_1\sigma_2 = \sigma_1\sigma_2\sigma_1$ dönüşümü yaparak, şekil 2.33'de gösterilen



Şekil 2.33. $\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_1\ \sigma_1\sigma_2\sigma_1\ \sigma_1\sigma_2\sigma_2\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2{}^{-1}$

$\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_1\ \sigma_1\sigma_2\sigma_1\ \sigma_1\sigma_2\sigma_2\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2{}^{-1}$

örgüsünü elde ederiz.

Yukarıda son adımda elde edilen örgüyü $(\sigma_2\sigma_1{}^2\sigma_2)(\sigma_2\sigma_1{}^{-1}\sigma_1{}^{-1}\sigma_2{}^{-1})$ formunda yazarsak,

$$\beta = (\sigma_2\sigma_1{}^2\sigma_2)(\sigma_2\sigma_1{}^{-2}\sigma_2{}^{-1})(\sigma_1{}^{-2})$$

olduğu görülür.

Her bir k pozitif tamsayısı için, A_k son şeridi ortadan kaldırıldığında k − 1 şeritteki birim örgüyü veren taranmış, k− örgülerin kümesini göstersin. O halde, $\beta = \alpha_1\alpha_2...\alpha_{n-1}$ dekompozisyonundaki her bir α_i örgüsü, herhangi bir $k \leq n$ için A_k' da bir örgü olarak düşünülebilir: $\alpha_1 \in A_n$ ve $\alpha_i \in A_{n+1-i}$. A_k grubunu B_n örgü grubunun bir alt grubu olarak düşünebiliriz. Aşağıda verilen teorem grubunun bir serbest grup olduğunu ve bu grubun üreteçlerinin B_n örgü grubunun üreteçleri cinsinden nasıl ifade edilebileceğini göstermektedir.

G bir grup olsun. Her $a \in G$ için, grubun elemanları arasında $aa^{-1} = a^{-1}a = 1$ dışında başka bir bağıntı yoksa, G grubuna **serbest grup** denir.

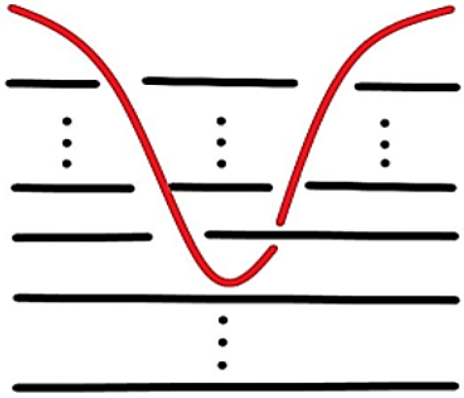
Örnek: Serbest grubun en basit örneği olarak, aşikar grup (tek elemanlı grup) verilebilir. Aşikar grup, boş bir küme tarafından rahatça üretilir.

Örnek: Sonsuz elemanlı devirli grup tam sayılar (Z, +) bir serbest abel gruptur. Bu grup, üreteçleri olan 1 ve −1 tarafından serbestçe üretilir.

Örnek: $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ ve $\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ matrisleri tarafından üretilen grup: 2x2 , tamsayı girişli ve det = 1 olan matrislerin bir alt grubu ve aslında bir serbest gruptur.

Teorem 1.2. *Her* $k > 0$ *tamsayısı için,* A_k *bir serbest gruptur ve her* $1 \leq i \leq k-1$ *tamsayısı için, bu grubun* $k-1$ *tane üreteci şu şekilde ifade edilebilir:*

$$a_i = (\sigma_{k-1}\sigma_{k-2}\ldots\sigma_{i+1})\sigma_i^{\,2}(\sigma_{i+1}^{\,-1}\sigma_{i+2}^{\,-1}\ldots\sigma_{k-1}^{\,-1})$$



$a_i \in A_k$

Şekil 2.34. a_i üreteci

Kelime problemi, serbest gruplar için çözülebilirdir. Serbest grubun elemanı olan herhangi bir kelimenin, grubun aşikar elemanı olup olmadığını belirlemek için, serbest sadeleştirmeleri yapmak yeterli olacaktır. Daha açık olmak gerekirse verilen bir kelimenin aşikar olup olmadığını belirlerken, ww^{-1} şeklindeki serbest sadeleştirmeleri yapıp, elde edilen kelimenin aşikar olup olmadığına bakılmalıdır. Az önce verilen teorem ile aşağıda verilen teoremi birleştirirsek, kelime probleminin örgü grupları için çözülebilir olduğunu görüyoruz.

Teorem 1.3. β *örgüsünün 2. adımın sonunda elde edilen dekompozisyonunun (ayrışımı)*

$$\beta = \alpha_1\alpha_2\ldots\alpha_{n-1}$$

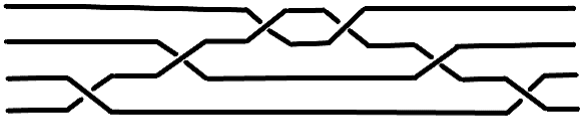
şeklinde olduğunu varsayalım. Bu durumda, β *örgüsü birim örgüye eşdeğerdir ancak ve ancak yukarıdaki dekompozisyondaki her bir* α_i *örgüsü birim örgüye eşdeğerdir.*

3.Adım: Bu adımda β örgüsünün 2. adımda elde edilen ayrışımındaki her bir α_i örgüsünün birim örgüye denk olup olmadığı belirlenir. Kelime probleminin serbest gruplar için çözülebilir olduğu bilinen bir gerçektir. Dolayısıyla, her bir α_i örgüsünün

serbest grubun elemanı olup olmadığını belirlenebilirse, kelime problemi örgü grupları için çözülmüş olur.

Öncelikle verilen bir örgüyü, taranmış örgüler cinsinden yazma işlemini anlatan, yukarıda adımları açıklamalı olarak verilen Artin Örgü Tarama Algoritmasının nasıl çalıştığını anlamak için, bütün adımların tek tek anlatıldığı tam bir örnek yapalım.

Örnek: Şekil 2.35'te gösterilen $\beta = \sigma_1\sigma_2{}^{-1}\sigma_3{}^{-1}\sigma_3{}^{-1}\sigma_2{}^{-1}\sigma_1$ örgüsünü ele alalım.

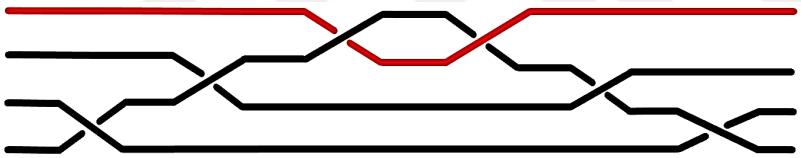


β

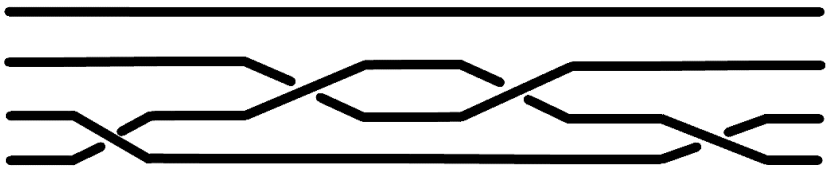
Şekil 2.35. Beta örgüsü

Artin Örgü Tarama Algoritmasının ilk adımında belirtildiği gibi, yukarıdaki şekilde kırmızı ile işaretli şeridi düzleştirerek, şekil 2.37'de verilen γ_1 örgüsünü elde ederiz.

γ_1 örgüsünün tersi ise aşağıdaki gibidir:

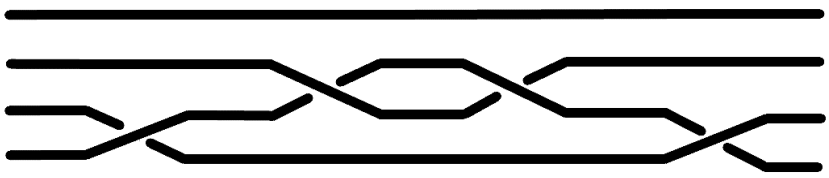


Şekil 2.36. Kırmızı renkli şerit düzleştirilecek



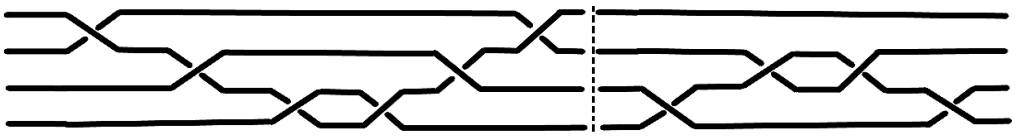
γ_1

Şekil 2.37. γ_1



Şekil 2.38. $\gamma_1{}^{-1}$

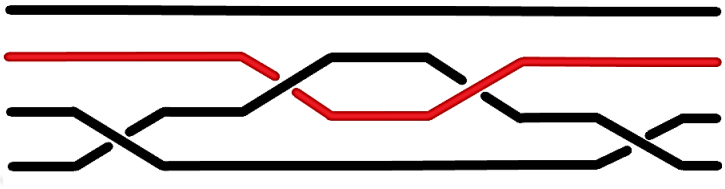
O halde, $\alpha_1 = \beta\gamma_1{}^{-1}$ örgüsü aşağıdaki gibidir:



$\beta = \alpha_1\gamma_1$ Sol taraftaki örgü taranmış örgüdür.

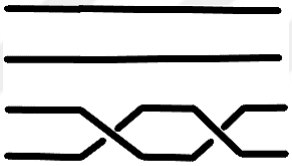
Şekil 2.39. $\alpha_1 = \beta\gamma_1{}^{-1}$

γ_1 örgüsünü tekrar ele alalım:



Şekil 2.40. Kırmızı şerit düzleştirilecek

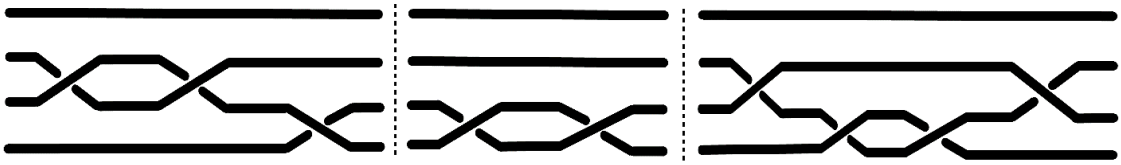
Yukarıda verilen figürde, kırmızı ile gösterilen şeridi düzleştirerek, şekil 2.41'de verilen γ_2 örgüsünü elde ederiz.



γ_2

Şekil 2.41. γ_2

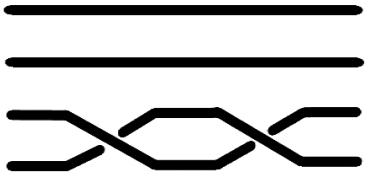
Daha sonra, aşağıda şekil 2.42'de verilen $\alpha_2 = \gamma_1\gamma_2{}^{-1}$ örgüsünü elde ederiz:



$\alpha_2 = \gamma_1\gamma_2{}^{-1}$

Şekil 2.42. $\alpha_2 = \gamma_1\gamma_2{}^{-1}$

γ_2 örgüsünün 2. şeridini çaprazlama içermeyen düz bir şerit ile değiştirirsek, birim örgüyü elde ederiz. Dolayısıyla α_3 örgüsü γ_2 örgüsünün kendisi olmalıdır:



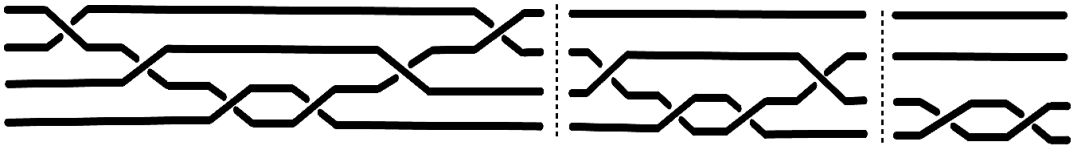
γ_2

Şekil 2.43. $\alpha_3 = \gamma_2$

Sonuç olarak, β örgüsünün taranmış, formu

$$\beta = (\sigma_3 \sigma_2^{-1}\sigma_1^{-1}\sigma_3^{-1}\sigma_2 \sigma_3^{-1})(\sigma_2^{-1}\sigma_1^{-1}\sigma_1^{-1}\sigma_2)(\sigma_1^{-1}\sigma_1^{-1})$$

şeklindedir:



Beta taranmış örgüsü ; $\beta = \alpha_1\alpha_2\alpha_3$

Şekil 2.44. $\beta = \alpha_1\alpha_2\alpha_3$

$\beta = (\sigma_3\sigma_2^{-1}\sigma_1^{-1}\sigma_3^{-1}\sigma_2\sigma_3^{-1})(\sigma_2^{-1}\sigma_1^{-1}\sigma_1^{-1}\sigma_2)(\sigma_1^{-1}\sigma_1^{-1})$ örgüsünü dikkate alalım.

A_4 serbest grup ve a_1, a_2, a_3 bu grubun üreteçleri olsun. Yukarıdaki β örgüsünün dekompozisyonunda, $\alpha_1 \in A_4$, $\alpha_2 \in A_3$ ve $\alpha_3 \in A_2$'dır. A_4 grubunun üreteçleri aşağıdaki gibidir:

$$a_1 = \sigma_3 \sigma_2 \sigma_1^2 \sigma_2^{-1} \sigma_3^{-1}$$

$$a_2 = \sigma_3 \sigma_2^2 \sigma_3^{-1}$$

$$a_3 = \sigma_3^2$$

α_1 örgüsünü bu üreteçler cinsinden yazmak istersek:

$$\alpha_1 = a_2^{-1} a_1^{-1} a_2$$

olduğu kolayca görülür.

Benzer şekilde , A_3 serbest grubunun üreteçleri a_1 ve a_2 olmak üzere, bu üreteçler aşağıdaki gibidir:

$$a_1 = \sigma_2 \sigma_1^2 \sigma_2^{-1}$$

$$a_2 = \sigma_2^2$$

Eğer α_2 örgüsünü bu üreteçler cinsinden yazmak istersek, şu eşitliği elde ederiz:

$$\alpha_2 = a_2^{-1}a_1^{-1}a_2$$

Son olarak A_2 serbest grubunun üreteçleri a_1 olmak üzere, $a_1 = \sigma_1^2$'dir. α_3 örgüsünü buüreteç cinsinden yazmak istersek:

$$\alpha_3 = a_1^{-1}$$

eşitliğini elde ederiz.

β *örgüsünün normal formu* $\beta = \alpha1\alpha2\alpha3$

$$\alpha_1 = a_2^{-1}a_1^{-1}a_2$$

$$\alpha_2 = a_2^{-1}a_1^{-1}a_2$$

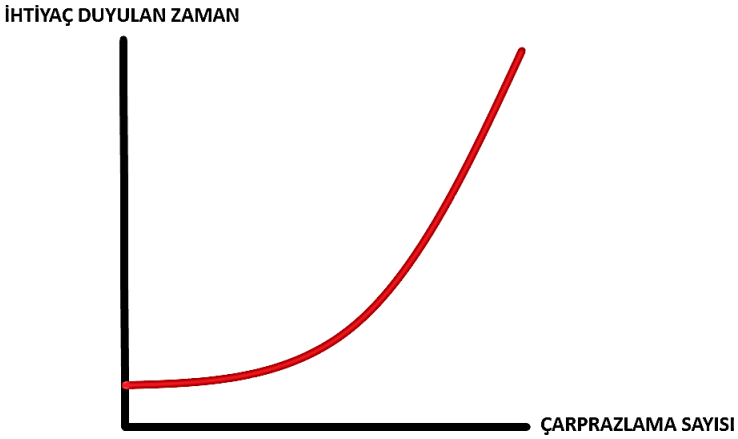
$$\alpha_3 = a_1^{-1}$$

Şekil 2.45. β örgüsünün normal formu

Teorem 2.2 ve Teorem 2.3'den β örgüsü birim örgüye izotop olmadığı sonucunu çıkartırız.

SONUÇ

Bir önceki bölümde Emil Artin tarafından tanımlanan tarama algoritmasından bahsetmiştik. Bu tarama algoritması sayesinde; verilen her örgü için yukarıda anlatılan ayrışım (dekompozisyon, normal form) mevcuttur. Artin'in Örgü Tarama Algoritması sayesinde, verilen herhangi bir örgünün birim örgüye izotop olup olmadığı belirlenebilir. Diğer bir deyişle örgü grubunda kelime problemi, Artin'in bu algoritması sayesinde çözüme kavuşmuştur. Şerit sayısı algoritmanın karmaşıklığı logaritmik bir şekilde artmakta olup, algoritmanın verimi oldukça düşmektedir. Daha açık olmak gerekirse, Artin'in Örgü Tarama Algoritması sayesinde teorik olarak verilen her örgünün normal formunun olduğu bilinsede, pratikte istenen normal formu bulmak şerit sayısı arttıkça oldukça karmaşık bir işlem haline gelmektedir. Diğer bir deyişle, Artin'in Örgü Tarama Algoritması oldukça yavaş, bir algoritmadır. Verilen bir örgüde çaprazlama sayısı arttıkça, bu örgünün normal formunu bulmak için gereken zaman oldukça artmaktadır. Üstelik böyle bir işlem bilgisayara yaptırmak istenilse bile, yine oldukça fazla zamana ihtiyaç duyulacaktır. Aşağıda verilen grafik, verilen bir örgüdeki çaprazlama sayısı arttıkça örgünün normal formunu bulmak için ihtiyaç duyulan zamanın ne kadar arttığını göstermektedir. Bu sebeple şu andaki güncel çalışmalar, daha hızlı ve verimli bir algoritma bulma üzerinedir. Örgü grubunda kelime problemine Emil Artin'in dışında, bundan yaklaşık 26 yıl kadar önce Fransız Matematikçi Dehornoy tarafından da bir çözüm getirilmiştir (Dehornoy, 1997).



Şekil 3.1. Çözüm için ihtiyaç duyulan zaman grafiği

KAYNAKÇA

Alexander, J. W. (1923). A lemma on systems of knotted curves. *Proceedings of the NationalAcademy of Sciences*, 9(3):93–95.

Anshel, I., Anshel, M., and Goldfeld, D. (1999). An algebraic method for public-key cryptog-raphy. *Mathematical Research Letters*, 6:287–291.

Artin, E. (1925). Theorie der zopfe. *Hamburg Abh*, 4:47–72.

ARTIN, E. (1950). The theory of braids. *American Scientist*, 38(1):112–119.

Birman, J., Ko, K. H., and Lee, S. J. (1998). A new approach to the word and conjugacy

problems in the braid groups. *Advances in Mathematics*, 139(2):322–353.

Dehornoy, P. (1997). A fast method for comparing braids. *Advances in Mathematics*, 125(2):200–235.

Jones, V. F. R. (1985). A polynomial invariant for knots via von Neumann algebras. *Bulletin (New Series) of the American Mathematical Society*, 12(1):103 – 111.

Ko, K. H., Lee, S., Cheon, J. H., Han, J. W., Kang, J.-S., and Park, C. (2000). New public-key cryptosystem using braid groups. In *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, volume 1880 of *Lecture Notes in Computer Science*, pages 166–183. Springe