

NGUYỄN CHÁNH TÚ

Khoa Toán, Đại Học Sư Phạm Huế

Giáo trình điện tử

LÍ THUYẾT MỞ RỘNG TRƯỜNG VÀ GALOIS



Huế 12-2006

ĐẶC TÍNH KỸ THUẬT

- Có thể tra cứu đến từng phần của giáo trình bằng cách click vào **Bookmarks** bên lề trái của Acrobat Reader.
- Có siêu liên kết tham khảo chéo và tham chiếu đến các tài liệu tham khảo (305).
- Có siêu liên kết để tra cứu các thuật ngữ hoặc nội dung cụ thể bằng Chỉ mục (307) ở cuối giáo trình.
- Có thể liên kết với trang web chỉ ra.
- Có siêu liên kết để tham khảo nhanh hướng dẫn giải của từng bài tập (250).
- Có thể đọc trên mạng, download hoặc nhanh chóng in thành giáo trình đọc.
- Có thể dùng để trình chiếu với chức năng **View | Full Screen**.

MỤC LỤC

LỜI NÓI ĐẦU	ix
HƯỚNG DẪN SỬ DỤNG	xiii
VÀI NÉT VỀ LỊCH SỬ	1
a) Lịch sử giải phương trình đa thức	1
b) Cuộc đời của Evariste Galois	10
Chương 0 KIẾN THỨC CHUẨN BỊ	21
0.1 Trường. Đặc số của trường.	22
0.2 Vành đa thức	25

0.3	Một số nhóm hữu hạn	30
0.4	Hàm Euler	37
	Bài tập	39
Chương 1	MỞ RỘNG TRƯỜNG	45
§ 1	Mở rộng trường. Bậc của mở rộng trường	45
1.1	Mở rộng trường	45
1.2	Bậc của mở rộng trường	48
	Bài tập	50
§ 2	Mở rộng đơn	53
2.1	Vành con và trường con sinh ra bởi một tập	53
2.2	Cấu trúc của mở rộng đơn	55
	Bài tập	61
§ 3	Mở rộng hữu hạn và mở rộng đại số	69
3.1	Tính chất của mở rộng hữu hạn và mở rộng đại số	69

3.2	Trường con các phần tử đại số. Trường đóng đại số. Bao đóng đại số.	71
	Bài tập	74
§ 4	Dựng hình bằng thước kẻ và compa	77
4.1	Ba bài toán dựng hình cổ điển	77
4.2	Điều kiện cần để đa giác đều p cạnh dựng được bằng thước kẻ và compa	81
	Bài tập	86
§ 5	Trường phân rã của một đa thức. Đa thức tách được	91
5.1	Trường phân rã của một đa thức	91
5.2	Đa thức tách được	98
	Bài tập	103
Chương 2 LÍ THUYẾT GALOIS		109
§ 6	Tự đẳng cấu và trường trung gian của mở rộng trường	109
6.1	Nhóm các tự đẳng cấu của mở rộng trường	110

6.2	Trường trung gian của mở rộng trường	114
	Bài tập	120
§ 7	Mở rộng tách được, chuẩn tắc và Galois	124
7.1	Mở rộng tách được và định lí phần tử nguyên thủy	124
7.2	Tiêu chuẩn của mở rộng Galois và chuẩn tắc	127
	Bài tập	133
§ 8	Định lí cơ bản của Lí thuyết Galois	137
	Bài tập	151
§ 9	Một số ứng dụng của Lí thuyết Galois	156
9.1	Trường hữu hạn	156
9.2	Trường và đa thức chia đường tròn	160
9.3	Đa giác đều dựng được bằng thước kẻ và compa	169
9.4	Định lí cơ bản của đại số	171
	Bài tập	173
§ 10	Nhóm Galois của đa thức	179
10.1	Biệt thức	179

10.2	Nhóm Galois của đa thức bậc 3	181
10.3	Đa thức bậc 4	184
10.4	Đa thức tổng quát	191
	Bài tập	197
§ 11	Tiêu chuẩn giải được bằng căn thức của đa thức	201
11.1	Mở rộng căn và tiêu chuẩn giải được	201
11.2	Tính không giải được của đa thức có bậc lớn hơn bốn	211
11.3	Nghiệm căn thức của các đa thức tổng quát có bậc không quá 4	213
	Bài tập	220
PHỤ LỤC		223
A	Nhóm giải được và nhóm đơn	223
B	Định lí Sylow và Định lí Cauchy	239
C	Bao đóng đại số của một trường	242
D	Sơ lược về Maple	245
HƯỚNG DẪN GIẢI BÀI TẬP		250

BẢNG KÍ HIỆU VÀ QUY ƯỚC	302
TÀI LIỆU THAM KHẢO	305
CHỈ MỤC	307

LỜI NÓI ĐẦU

Lí thuyết Galois là một trong những lí thuyết đẹp đẽ nhất của đại số, tập hợp nhiều kiến thức và phương pháp của các lĩnh vực toán học khác nhau, nhằm giải quyết các bài toán cổ điển và những vấn đề quan trọng khác của đại số hiện đại.

Một trong những ứng dụng chủ yếu của Lí thuyết Galois là giải quyết bài toán tìm nghiệm căn thức của phương trình đa thức, đặc biệt chỉ ra rằng phương trình bậc lớn hơn bốn không thể giải được bằng căn thức. Mặt khác, Lí thuyết Galois cho phép xác định đa giác đều n cạnh dựng được bằng thước kẻ và compa. Bên cạnh đó, chúng ta nhận được từ Lí thuyết Galois lời giải cho ba bài toán dựng hình cổ điển, đó là không thể (bằng thước kẻ và compa) chia ba một góc, gấp đôi hình lập phương hoặc cầu phương đường tròn.

Do tầm quan trọng của Lí thuyết Trường và Galois mà từ năm 1986, môn học này đã được Bộ Giáo dục và đào tạo đưa vào trong chương trình chính thức của khoa Toán các trường Đại học và Cao đẳng, đặc biệt là cho khoa Toán các Trường Sư phạm. Hơn thế, Lí thuyết Galois cũng được giảng dạy cho các lớp Cao Học, xem như kiến thức cơ bản để từ đó mở rộng cho những nghiên cứu lí thuyết và ứng dụng sâu sắc hơn.

Giáo trình này ra đời trên cơ sở bài giảng của tác giả cho sinh viên Khoa Toán, Trường Đại học sư phạm Huế suốt hơn 10 năm trực tiếp giảng dạy môn học này. Trong quá trình đó, bản thảo được chỉnh sửa và bổ sung sao cho vừa phù hợp với chương trình của Bộ Giáo dục và Đào tạo, vừa đáp ứng nhu cầu sử dụng các công cụ mới của đại số tính toán, vừa bổ sung những kiến thức liên quan khó có thể tìm đủ trong một vài quyển sách tham khảo. Vì thế, giáo trình ra đời, trước hết, nhằm đáp ứng nhu cầu sử dụng của sinh viên đại học, cao đẳng và học viên cao học ngành toán. Bên cạnh đó, giáo trình có thể là một tài liệu tham khảo bổ ích cho giáo viên phổ thông trung học và học sinh giỏi. Họ có thể tìm thấy trong giáo trình này cơ sở toán học chặt chẽ cho việc tìm nghiệm căn thức của phương trình đa thức, của các bài toán dựng hình bằng thước kẻ và compa, những kiến thức về lịch sử toán học liên quan. Ngoài ra, giáo trình sơ lược giới thiệu về Maple, một trong những hệ thống tính toán đại số mạnh mẽ và phổ biến nhất hiện nay. Thông qua những ví dụ minh họa, giáo trình chỉ ra khả năng tính toán mạnh mẽ của Maple cũng như việc hỗ trợ đắc lực của phần mềm này cho các giáo viên phổ thông, cho sinh viên và học sinh trong hoạt động giảng dạy, nghiên cứu và học tập toán.

Giáo trình được biên soạn trên nguyên tắc đảm bảo đầy đủ và chặt chẽ của kiến thức. Để làm việc với giáo trình này, độc giả chỉ cần một số kiến thức cơ sở của đại số tuyến tính, lôgic, đại số đại cương như đã học trong năm thứ nhất và thứ hai của Đại học hoặc Cao đẳng. Ngoài những kiến thức đó, những khái niệm mới được định nghĩa và những kết quả mới đều được chứng minh đầy đủ. Phần kiến thức bổ sung, nếu chưa được học trong những năm đầu tiên của chương trình Đại học, Cao đẳng, sẽ được giới thiệu chi tiết trong Phụ lục. Cuối mỗi tiết (§), giáo trình cung cấp một hệ thống phong phú các bài tập từ dễ đến khó, bắt đầu từ bài trắc nghiệm lí thuyết nhằm giúp độc giả nắm một cách chắc chắn những khái niệm và kết quả chủ yếu. Gần 150 bài tập trong giáo trình đều có phần hướng dẫn giải đầy đủ trong nỗ lực giúp độc giả có thể tự học. Qua thực tế giảng dạy, tác giả cho rằng việc dạy-học toán hiện nay nói chung, ở đại học nói riêng, người dạy và người học cần khai thác sự hỗ trợ hiệu quả của các phần mềm toán học. Có sự hỗ trợ này, việc dạy-học có những thay đổi tích cực và chất lượng giáo dục được cải thiện rõ rệt. Cùng với việc nắm vững kiến thức lí thuyết, có khả năng giải quyết các bài toán ứng dụng, người học cần biết sử dụng các phần mềm hỗ trợ cho các mục đích

tính toán cụ thể. Có nhiều tính toán rất khó và phức tạp trước đây nay trở nên vô cùng đơn giản với sự trợ giúp của các phần mềm toán học. Trên tinh thần đó, ở những vị trí thích hợp, tác giả bổ sung các lệnh và ví dụ minh họa cho việc sử dụng Maple.

Để hoàn thành giáo trình này, tác giả đã nhận được sự hỗ trợ của nhiều thế hệ sinh viên và học viên cao học trong việc phát hiện, sửa chữa sai sót trong giáo trình. Nhiều thầy cô, đồng nghiệp và bạn bè cũng đã đóng góp nhiều ý kiến quý báu trong quá trình biên soạn. Nhân dịp giáo trình này ra đời, tác giả, một lần nữa, gửi lời cảm ơn sâu sắc đến các thầy cô, đồng nghiệp, bạn bè và sinh viên về những giúp đỡ vô giá trên.

Mặc dù đã cố gắng, giáo trình này không thể tránh khỏi những thiếu sót. Tác giả vô cùng biết ơn nếu nhận được những ý kiến đóng góp, bình luận và những phát hiện lỗi trong giáo trình này của độc giả gần xa. Mọi ý kiến đóng góp, trao đổi xin gửi về địa chỉ : TS. Nguyễn Chánh Tú, Khoa Toán, Trường Đại học sư phạm Huế, 32 Lê Lợi, Thành phố Huế, email: nctu2000@yahoo.com.

Huế ngày 25 tháng 4 năm 2007.

HƯỚNG DẪN SỬ DỤNG

Lí thuyết Galois có nhiều cách tiếp cận khác nhau. Một cách tiếp cận có nhiều ưu điểm là trình bày Lí thuyết Galois trên cơ sở Lí thuyết mở rộng trường. Quan điểm đó của Bộ Giáo dục và đào tạo được chúng tôi thống nhất trong việc biên soạn giáo trình này. Giáo trình có 2 chương, ứng với Lí thuyết mở rộng trường và Lí thuyết Galois. Mỗi chương được chia ra thành các tiết (§) tương ứng với 4-5 giờ học tập trên lớp. Ngoài ra, giáo trình có bổ sung phần Kiến thức chuẩn bị (Chương 0), nhằm nhắc lại những kiến thức cũ chủ yếu có liên quan sau này. Giáo trình cố gắng trình bày theo thứ tự hợp lí nhất của việc giảng dạy-học tập môn học. Tuy nhiên tùy theo mục đích mà độc giả có thể sử dụng theo một thứ tự phù hợp khác. Sau khi đọc xong phần lí thuyết của tiết, độc giả cần tự mình giải quyết các bài tập cuối tiết và trả lời bài tập trắc nghiệm (có thể tham khảo phần hướng dẫn, nếu cần). Các bài tập được sắp xếp từ dễ đến khó ; những bài tập (*) đòi hỏi sự tư duy cao hơn. Như đã trình bày, nếu có điều kiện, độc giả nên khai thác sử dụng Maple thông qua các ví dụ và nội dung cụ thể trong giáo trình.

Từ (§ 8), giáo trình sử dụng thêm các kiến thức sâu sắc hơn của đại số đại cương.

Những kiến thức này được trình bày chi tiết trong Phụ lục.

Các định lí, mệnh đề, hệ quả, bổ đề được đánh số theo từng tiết, ví dụ “Mệnh đề 2.3” nằm trong § 2 và được trích dẫn là “Mệnh đề 2.3” hoặc gọn hơn là “2.3”. Các công thức hoặc phương trình được đánh số từ đầu đến cuối giáo trình về bên phải, ví dụ

$$D_f = -4p^3 - 27q^2 \quad (1)$$

được trích dẫn là “(1)”. Riêng phần Phụ lục, mọi định lí, mệnh đề,...được đánh số với một chữ cái đứng trước, ví dụ “Mệnh đề A.2.” được trích dẫn là “Mệnh đề A.2.” hay đơn giản là “A.2.”. Giáo trình có bảng các kí hiệu sử dụng trong giáo trình và phần **Chỉ Mục (307)** (Index) nhằm giúp độc giả dễ dàng tra cứu được nội dung khái niệm hoặc kiến thức cần thiết.

VÀI NÉT VỀ LỊCH SỬ ¹

A) LỊCH SỬ GIẢI PHƯƠNG TRÌNH ĐA THỨC

Ngày nay, người ta tin rằng, việc giải phương trình đa thức bậc hai đã được các nhà toán học cổ đại Babilon quan tâm cách đây gần 4000 năm. Những tấm đất sét có niên đại 1600 BC được tìm thấy của nền văn minh Babilon còn ghi lại việc tìm nghiệm của những phương trình bậc hai cụ thể. Tuy nhiên, những lời giải trên được mô tả bằng phương pháp hình học và do đó chỉ liên quan đến những phương trình bậc hai có hệ số lớn hơn 0.

Những phương pháp hình học để giải phương trình bậc hai tiếp tục được nhà toán học vĩ đại Hy Lạp Euclid (325 BC-265 BC) đề cập đến. Mãi đến thế kỉ thứ 7, nhà toán học Ấn Độ Brahmagupta (598-665), mới trình bày một cách giải phương trình bậc hai có sử dụng số âm và các kí hiệu, đánh dấu sự phát triển của đại số.

Việc xét một cách đầy đủ nghiệm của phương trình bậc hai bằng phương pháp đại số chỉ được thực hiện bởi các nhà toán học Arab, tiêu biểu là al-Khwarizmi

¹Thông tin trong phần này được tham khảo chủ yếu từ [5] và [7].

(780-880). Tuy nhiên, các nhà toán học Arab lại chưa biết đến số âm, do đó trong cuốn sách của mình có tên “*Hisabal-jabrw'al-muqaba*”, al-Khwarizmi đã phân thành 6 loại phương trình bậc hai, ứng với 6 chương trong cuốn sách và trình bày cách giải cho từng loại. Đây được xem là cuốn sách đầu tiên về đại số và từ “*Algebra*” (đại số) ra đời từ tên của cuốn sách này. Đến năm 1145, cuốn sách nổi tiếng của nhà toán học Tây Ban Nha, Abraham bar Hiyya Ha-Nasi (1070-1136) được xuất bản ở châu Âu có tên Latinh là “*Liber ambadorum*” cũng trình bày đầy đủ nghiệm của các phương trình bậc hai.

Trường phái toán học Italy khởi đầu khoảng năm 1500 với cuốn sách của Luca Pacioli (1445-1517) xuất bản năm 1494, được biết đến với tên viết tắt là “*Suma*”, trong đó lời giải của phương trình bậc hai được trình bày chi tiết bằng ngôn ngữ đại số hiện đại. Pacioli không đề cập đến việc giải phương trình đa thức bậc ba nhưng ông lại nhắc đến việc giải phương trình đa thức bậc bốn. Ông viết, theo ngôn ngữ của đại số ngày nay, “*phương trình bậc bốn $x^4 = a + bx^2$ giải được bằng phương pháp như đối với phương trình bậc hai, nhưng các phương trình $x^4 + ax^2 = b$ và $x^4 + a = bx^2$ thì không thể giải được*”.

Người đầu tiên tìm được nghiệm của phương trình đa thức bậc ba là Scipione del Ferro (1465-1526), một giáo sư nổi tiếng của Đại học Bologna, Italy. Ferro tìm được nghiệm căn thức của phương trình $x^3 + mx = n$. Tất nhiên, nếu biết sử dụng khái niệm số âm của các nhà toán học Ấn Độ, thì công thức nghiệm đó là đủ để giải tất cả các dạng của phương trình bậc ba. Tuy nhiên, lúc bấy giờ, Ferro không biết điều đó. Ferro giải được phương trình bậc ba nêu trên vào năm 1515, nhưng giữ bí mật cho đến trước lúc qua đời năm 1526 mới tiết lộ cho một người học trò của mình là Antonio Fior. Fior là một người học toán bình thường và ngay lập tức làm rò rỉ lời giải của thầy mình ra ngoài. Tin đồn về lời giải của phương trình bậc ba lan rộng khắp Bologna và các vùng lân cận, kích thích nhà toán học nghiệp dư Niccolo Fontana(1499-1557) tìm ra lời giải của phương trình $x^3 + mx^2 = n$ không lâu sau đó. N. Fontana (được biết đến với tên Tartaglia) quyết định công bố thành công của mình. Một cuộc thách đố khoa học nổ ra giữa Tartaglia và Fior năm 1535. Luật của cuộc thi đơn giản là mỗi người sẽ đưa ra 30 phương trình bậc ba cho đối thủ, hẹn trong 50 ngày, ai giải được nhiều hơn thì thắng. Tất cả các phương trình mà Fior đưa ra cho Tartaglia đều có dạng $x^3 + mx = b$ và Fior tin



Hình 1: Chân dung Tartaglia

chắc là Tartaglia không thể giải được. Trước thời hạn cuối cùng 8 ngày, Tartaglia đã tìm được phương pháp tổng quát giải tất cả phương trình bậc ba. Trước công chúng, Tartaglia đưa ra lời giải của 30 bài toán trong vòng 2 giờ và được công nhận là người thắng cuộc. Tuy nhiên, ông không công bố lời giải chi tiết.

Chiến thắng của Tartaglia lan đến Milan, kích thích một nhà toán học nghiệp dư khác, bác sĩ Girolamo Cardano (1501-1576). Cardano lập tức mời Tartaglia

đến thăm Milan vào năm 1539 và tìm cách thuyết phục Tartaglia tiết lộ lời giải phương trình bậc ba cho mình. Tartaglia đồng ý với giao ước Cardano phải giữ bí mật về lời giải cho đến khi Tartaglia tự mình xuất bản công trình đó. Nhưng Cardano không giữ giao ước, lời giải của phương trình bậc ba và bậc bốn đã được xuất hiện chi tiết trong quyển sách “*Ars Magna*” nổi tiếng của Cardano, xuất bản năm 1545. Tartaglia vô cùng tức giận và trong một bài báo của mình xuất bản sau đó, Tartaglia khẳng định lại công lao của mình và lên án sự phản bội của Cardano.

Trong “*Ars Magna*”, cuốn sách tiếng Latinh đầu tiên trên thế giới về đại số, Cardano có đề cập đến công lao của Tartaglia chính là tác giả của công thức nghiệm của phương trình bậc ba, nhưng ông cũng giải thích thêm rằng việc chứng minh công thức cũng như trình bày lời giải chi tiết là của ông cùng các học trò của mình. Đặc biệt, cuốn sách của Cardano lần đầu tiên trình bày lời giải cho 20 loại phương trình đa thức bậc bốn. Các lời giải này đều có chung phương pháp là tìm nghiệm của một phương trình phụ bậc ba (ngày nay ta gọi là *giải thức bậc ba*), rồi sử dụng nó để giải phương trình bậc bốn đã cho. Tác giả của kết quả này là



Hình 2: Chân dung G. Cardano

Lodovico Ferari (1522-1565), một trong những học trò xuất sắc nhất của Cardano. Một lí do nữa để giải thích cho quyết định của Cardano là ông phát hiện ra rằng Ferro là người đã giải được các phương trình bậc ba trước đó 30 năm.

Sự ra đời của Ars Magna truyền cảm hứng cho nhiều nhà toán học trên thế giới tiếp tục nghiên cứu về phương trình đa thức như Bombelli (1526-1572, Italy), Viète (1540-1603, Pháp), Descartes (1596-1650, Pháp), Harriot (1560-1621, Anh),



Hình 3: Chân dung N. Abel

Tschirnhaus (1651-1708, Đức), Euler (1707-1783, Thụy Sĩ), Bezout (1730-1783, Pháp). Sau khi giải được phương trình đa thức bậc ba và bốn, vấn đề tìm nghiệm căn thức cho phương trình đa thức bậc năm được đặt ra một cách tự nhiên và thu hút sự quan tâm của nhiều nhà toán học trong một thời gian dài. Euler thất bại trong nỗ lực của mình nhưng đạt được một phương pháp mới giải phương trình bậc bốn. Lagrange (1736-1813), một nhà toán học Italy-Pháp, đã đạt được bước

tiến quan trọng trong việc nghiên cứu bản chất quá trình tìm nghiệm của phương trình bậc nhỏ hơn năm ; quá trình đó phụ thuộc vào việc xác định các hàm nghiệm mà chúng không đổi dưới tác động của các hoán vị đặc biệt trên tập nghiệm của đa thức ; ông cũng đã chỉ ra rằng quá trình đó không thể thực hiện được đối với đa thức bậc năm. Từ đó, giả thuyết về việc không thể giải được phương trình bậc năm bằng căn thức trở thành một thách thức cho các nhà toán học. Năm 1813, Ruffini (1765-1822, Italy) đã cố gắng đưa ra một chứng minh cho giả thuyết trên, rất tiếc chứng minh của ông còn nhiều điểm không chính xác. Vấn đề chỉ được giải quyết trọn vẹn bởi thần đồng toán học người Na Uy, Niels Henrik Abel (1802-1829) vào năm 1824. Abel chưa kịp giải quyết bài toán tổng quát hơn là “*khi nào một phương trình đa thức bậc n có thể giải được bằng căn thức*” thì ông qua đời lúc chưa tròn 27 tuổi. Công trình của Abel chỉ được công nhận và xuất bản sau đó, năm 1830.

Ba năm sau, một bi kịch tương tự cũng xảy ra với Evariste Galois (1811-1832), một thần đồng toán học khác. Sự ra đi đột ngột của ông đã không kịp cho thế giới toán học nhận ra một trong những lí thuyết đẹp đẽ nhất của đại số, mà từ đó dễ dàng có câu trả lời cho bài toán tổng quát trên. Phải đợi đến năm 1843, mười một



Hình 4: Chân dung Galois lúc 15 tuổi

năm sau ngày ông qua đời, những tuyên bố sau của nhà toán học Pháp Joseph Liouville (1809-1882) trong bức thư gửi cho Viện Hàn Lâm Khoa Học Pháp mới đánh dấu sự thừa nhận chính thức của cộng đồng toán học dành cho E. Galois. Liouville viết :

Hy vọng tôi sẽ mang đến cho Viện Hàn Lâm một sự quan tâm đặc biệt bằng việc công bố rằng tôi đã phát hiện được trong các công trình của Evariste

Galois lời giải hoàn hảo và sâu sắc cho bài toán nổi tiếng: khi nào thì phương trình đa thức giải được bằng căn thức.

Abel và Galois, hai số phận bất hạnh với nhiều điểm tương đồng kì lạ, xuất hiện và biến mất như hai vệt sao băng sáng chói trên bầu trời toán học. Sự tồn tại ngắn ngủi của họ đã để lại những di sản vĩ đại cho văn hóa nhân loại. Công trình của Abel và Galois khép lại một chương của lịch sử giải phương trình đa thức và mở ra nhiều chương mới của đại số hiện đại, khởi nguồn cho những lí thuyết đẹp đẽ cùng nhiều ứng dụng quan trọng khác.

B) CUỘC ĐỜI CỦA EVARISTE GALOIS

Evariste Galois sinh ngày 25 tháng 10 năm 1811 tại Bourg-la-Reine, một vùng ngoại ô củathủ đô Paris nước Pháp, trong một gia đình trí thức. Bố Galois là một người nổi tiếng, nhiều năm là thị trưởng của Bourg-la-Reine. Mẹ ông am hiểu nhiều lĩnh vực như triết học, ngôn ngữ, thần học. Galois được mẹ dạy tiếng Hy Lạp, Latinh, thần học cho đến năm 12 tuổi.

Tháng 10 năm 1823, Galois bắt đầu đến trường và vào học lớp 4, Trường Louis-

le-Grand. Tại đây, Galois sớm chứng kiến sự nổi dậy của học sinh hưởng ứng cuộc cách mạng chống lại vua Louis XVIII và sau đó là vua Charles X. Gần 40 học sinh của trường bị đuổi học trong năm học đầu tiên của Galois. Việc học của Galois trong năm học đầu tiên diễn ra thuận lợi. Galois đạt điểm số tốt và nhận được học bổng. Tuy nhiên, việc học trên lớp ngày càng trở nên kém hấp dẫn và Galois phải lưu ban vào năm 1826 do thiếu điểm môn tu từ học.

Năm 1827, Galois tham gia khóa học toán đầu tiên với giáo sư M. Vernier, và sớm say mê môn học này. Năm 1828, Galois thi vào trường École Polytechnique, trường đại học danh giá hàng đầu của Pháp nhưng không đỗ. Quay trở về Louis-le-Grand, anh tham gia khóa học toán với giáo sư Louis Richard (1795-1849) và bắt đầu nghiên cứu những đề tài riêng biệt của mình. Galois tìm đọc các giáo trình toán cao cấp như *Hình học của Legendre*, *lí thuyết Langrange*... Richard viết về Galois “*Sinh viên này chỉ quan tâm đến những lĩnh vực khó nhất của toán học*”. Sức hút của toán học làm anh chệnh mảng hơn với việc học trên lớp. Phiếu nhận xét về Galois những năm đó đều mô tả anh là một học sinh “*khác thường, lập dị, độc đáo và khép kín*”. Tháng 4 năm 1829, Galois có công trình toán đầu tiên



Hình 5: Chân dung Galois được anh trai vẽ lại năm 1848

xuất bản trên tạp chí *Annales de Mathématiques* về liên phân số. Cuối tháng 5 và đầu tháng 6, Galois gửi cho Viện hàn lâm khoa học Pháp các kết quả nghiên cứu về nghiệm của phương trình đại số. Cauchy (1789-1857) là người được phân công phản biện và ông đã bác bỏ các kết quả này.

Thảm kịch bắt đầu xảy ra với Galois khi cha anh tự tử từ một sự vụ cáo ác hiểm của vị thầy tế vùng Bourg-la-Reine. Cha của Galois là một chính khách theo phái

cộng hòa. Những xung đột chính trị phức tạp thời bấy giờ giữa phái cộng hòa và bảo hoàng đã lôi cuốn và góp phần đẩy đến những bi kịch liên tiếp cho Galois và gia đình anh. Cái chết của cha gây sốc mạnh mẽ và tác động lớn đến cuộc đời Galois sau này.

Chỉ vài tuần sau cái chết của cha, Galois phải trải qua lần thi thứ hai vào Trường École Polytechnique. Và Galois lại rớt ! Không nản chí, tháng 12 năm 1829, Galois thi và đỗ vào trường École Normal. Trong kì thi đó, vị giám khảo môn toán đã có nhận xét về Galois như sau :

Học sinh này nhiều khi diễn tả một cách rối rắm ý tưởng của mình nhưng là một học sinh thông minh và có khả năng đặc biệt trong nghiên cứu.

Còn những nhận xét của vị giám khảo môn văn học là :

Đây là học sinh duy nhất trả lời rất tồi câu hỏi của tôi và tỏ ra không biết gì cả. Trước đây, nhiều người nói với tôi rằng học sinh này có năng khiếu đặc biệt về toán học. Tôi thật sự ngạc nhiên về đánh giá đó vì sau kì thi này, tôi cho rằng anh ta không thông minh lắm.

Cuối năm 1829, Galois lại gửi một công trình khác về *lí thuyết phương trình* cho Cauchy. Một lần nữa Cauchy không thừa nhận kết quả của Galois. Tháng 2 năm 1830, Galois gửi công trình “Về điều kiện một phương trình giải được bằng căn thức” cho Viện hàn lâm khoa học Pháp để tham dự giải thưởng toán học của Viện. Thư kí Viện, giáo sư nổi tiếng J. Fourier (1768-1830), là người phản biện công trình của Galois. Nhưng Fourier qua đời đột ngột vào tháng 4 năm 1830. Và công trình của Galois không bao giờ được tìm thấy nữa. Khoảng thời gian này, Galois biết rằng một bài báo của nhà toán học quá cố Abel được xuất bản trên *Bulletin de Férussac* có một phần kết quả giống của mình. Sau khi tìm đọc các bài báo của Abel và Jacobi (1804-1851, Đức), Galois đã hoàn thành các nghiên cứu về các hàm *elliptic* và *tích phân abel*. Galois đã đăng 3 công trình trên *Bulletin de Férussac* trong tháng 4 năm 1830. Trong tháng 6, Galois biết tin giải thưởng toán học của Viện hàn lâm đã được trao đồng thời cho Abel và Jacobi.

Tháng 6 năm 1830, nước Pháp sục sôi với những xung đột giữa phe cộng hòa và bảo hoàng. Vua Charles X bị trục xuất khỏi Pháp, nhường ngai vàng cho vua Louis-Phillipe. Các cuộc biểu tình, bạo loạn, đàn áp tiếp tục xảy ra thường xuyên

trên các đường phố Paris. Hiệu trưởng trường École Normal, GS. M. Guigniault, nhốt học sinh trong trường để tránh không cho học sinh tham gia xuống đường. Trèo tường ra ngoài không thành, Galois viết một bài báo đăng trên *Gazette des Écoles* để phản đối việc khóa cửa nhốt học sinh trong trường của hiệu trưởng. Galois bị đuổi học và tham gia vào pháo binh, một binh chủng trong quân đội hoàng gia. Tuy nhiên, đến tháng 12 năm 1830, pháo binh bị giải tán bởi sắc lệnh của nhà vua do lo sợ binh chủng này là mối đe dọa cho ngai vàng.

Galois cố gắng quay trở lại làm toán. Anh mở một lớp học về đại số cao cấp thu hút khoảng 40 sinh viên. Nhưng sau buổi học đầu tiên, số sinh viên giảm một cách nhanh chóng và cuối cùng lớp học tan rã. Những công trình cuối cùng trong đời Galois là 2 bài báo nhỏ đăng trên *Annales de Gergonne* (tháng 12 năm 1830) và trên *Gazette des Écoles* (tháng 1 năm 1831).

Tháng 1 năm 1831, theo gợi ý của viện sĩ Viện hàn lâm khoa học Pháp Poisson (1781-1840), lần thứ ba, Galois gửi công trình nghiên cứu về phương trình của mình cho Viện hàn lâm.

Chính sự nước Pháp lại lôi cuốn Galois, người đang mang tâm trạng nặng nề

khi phải đối mặt với những bất hạnh dồn dập. Người thanh niên này liên tiếp rơi vào vòng xoáy của những ý nghĩ và hành động tiêu cực. Cuối năm 1830, mười chín sĩ quan pháo binh bị bắt về tội âm mưu lật đổ ngai vàng, nhưng được tha bổng sau đó. Ngày 9 tháng 5 năm 1831, những người cộng hòa tổ chức một bữa tiệc chào mừng sự kiện này và phô trương thanh thế. Phấn khích từ không khí của bữa tiệc, Galois đeo kính, tay cầm dao găm kêu gọi mọi người chống lại nhà vua. Sau bữa tiệc, Galois bị bắt giam ở nhà tù Sainte-Pélagie. Ra tòa, Galois được tha bổng vào ngày 15 tháng 6 năm 1831. Ngày 14 tháng 7, kỉ niệm sự kiện ngục Bastille, Galois lại xuất hiện ở hàng đầu trong cuộc biểu tình rầm rộ của những người cộng hòa, với trang phục pháo binh, tay cầm súng và kiếm. Galois lại bị tổng giam vào Sainte-Pélagie. Lần này Galois bị kết án 6 tháng tù giam. Trong tù, Galois nhận được tin về số phận hẩm hiu của công trình khoa học mà anh gửi lần thứ 3 cho Viện hàn lâm khoa học Pháp. Poisson nhận xét về công trình của Galois :

Chúng tôi đã cố gắng để hiểu chứng minh của Galois. Rất tiếc, lập luận của tác giả không rõ ràng và những kết quả đạt được chưa đủ để chúng tôi khẳng định được tính đúng đắn của công trình...Tôi cho rằng tác giả nên

biên soạn lại toàn bộ kết quả của mình trong một công trình thống nhất để có tính thuyết phục lớn hơn.

Tháng 3 năm 1832, dịch tả hoành hành ở Paris. Galois cùng các tù nhân được chuyển đến nhà an dưỡng Sieur Faultrier. Tại đây, một cơn gió mát tưởng chừng có thể làm dịu đi những đau buồn vô tận trong lòng người tù trẻ. Galois đem lòng yêu Stephanie-Felice du Motel, con gái của một nhà vật lí trong vùng. Bất hạnh thay, đây là một mối tình đơn phương và lại là khởi đầu cho bi kịch lớn nhất của Galois. Sau khi được tự do vào ngày 29 tháng 4 năm 1832, Galois tiếp tục theo đuổi cô gái nọ, nhưng cô luôn tìm cách từ chối tình cảm của anh.

Trong thời gian này, nghe theo lời khuyên của Poisson, Galois lặng lẽ khâu chuỗi lại những phát minh của mình bằng những trang viết vôi vàng (Hình 6).

Thế rồi, Galois bị lôi vào cuộc đấu súng định mệnh vào ngày 30 tháng 5 năm 1832 với Perscheux d'Herbinville. Nguyên nhân của cuộc đấu súng vẫn chưa thực sự rõ ràng nhưng chắc chắn là có liên quan trực tiếp đến Stephanie-Felice du Motel. Như tiên đoán được kết cục, đêm 29 tháng 5, Galois thức trọn để viết bức thư cuối cùng cho người bạn Auguste Chevalier, tóm tắt lại toàn bộ phát minh



Hình 6: Một trang bản thảo của Galois

của mình. Rất nhiều đoạn trong bức thư bị bôi xóa nhiều lần với chú thích “*tôi không có đủ thời gian*”. Sáng hôm sau, Galois bước chân đến đấu trường và kết cục tiên liệu đã xảy ra. Cuối ngày, một người nông dân trong vùng phát hiện Galois bị trọng thương nằm trên cánh đồng và đưa anh vào bệnh viện. Ngày 31 tháng 5 năm 1832, Galois trút hơi thở cuối cùng tại bệnh viện Cochin và được an táng tại

Montparnasse 2 ngày sau đó.

Anh của Galois và Chavalier gửi bức thư cùng toàn bộ những bản thảo dang dở của Galois cho Gauss (1777-1855, Đức) và Jacobi như di chúc của anh. Không hiểu vì lí do gì, không có một phản ứng hoặc ý kiến nào từ Gauss và Jacobi. May mắn là sau đó, công trình của Galois đến được tay Liouville. Mười một năm sau, Liouville đã viết thư thông báo cho Viện hàn lâm Pháp về sự đúng đắn và sâu sắc trong kết quả của Galois ; ông đã cho xuất bản những phát minh của Galois trên tạp chí *Revue Encyclopédia* của mình vào năm 1846.

Galois kết thúc bức thư định mệnh của mình bằng những dòng :

Xin gửi cho Gauss và Jacobi để họ đánh giá công khai, không phải về tính đúng đắn mà là tầm quan trọng của những định lí này. Tôi hi vọng hậu thế sẽ có người thấy được sự sâu sắc của chúng cũng như giải mã được tất cả những bí ẩn hiện thời.

Phát minh mà Galois đem lại cho khoa học để từ đó hậu thế đã, đang và sẽ tiếp tục “giải mã” là lí thuyết mang tên ông : **Lí thuyết Galois.**

Chương 0

KIẾN THỨC CHUẨN BỊ



Trong phần Kiến thức chuẩn bị, ta nhắc lại các kiến thức cơ bản nhất của đại số đại cương sẽ được sử dụng trong cuốn sách này. Chứng minh của các kết quả này dễ dàng tìm thấy trong các giáo trình đại số ở Cao đẳng và Đại học. Các kiến thức sâu sắc hơn về Lí thuyết nhóm cần thiết sẽ được trình bày chi tiết trong Phần Phụ lục. Đặc biệt, việc giải quyết các bài tập cuối tiết này tạo điều kiện cho độc giả nắm tốt hơn các tính chất và phương pháp cơ bản sử dụng trong Lí thuyết trường và vành đa thức.

0.1 TRƯỜNG. ĐẶC SỐ CỦA TRƯỜNG.

Định nghĩa. Trường là một vành giao hoán có đơn vị khác 0 và mọi phần tử khác 0 đều khả nghịch.

Nhận xét 0.1. Trường là một miền nguyên, đặc biệt trường không có ước của 0.

Ví dụ 1. \mathbb{Q} là trường các số hữu tỉ với các phép toán cộng và nhân thông thường. Tương tự, ta có trường \mathbb{R} các số thực và trường các số phức \mathbb{C} .

Ví dụ 2. Vành thương $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ là một trường khi và chỉ khi n nguyên tố. Trường \mathbb{Z}_p với p nguyên tố là trường hữu hạn có p phần tử.

Định nghĩa. Một đồng cấu trường là một đồng cấu vành biến đơn vị thành đơn vị. Tương tự như vành, ta có khái niệm đơn cấu, toàn cấu và đẳng cấu trường.

Cho F là một trường. Một đồng cấu (đẳng cấu) trường từ F vào F gọi là một tự đồng cấu (tự đẳng cấu) trường. Tập tất cả các tự đẳng cấu trường với phép toán tích các ánh xạ tạo thành một nhóm, ký hiệu $\text{Aut}(F)$.

Nhận xét 0.2. Mọi đồng cấu trường đều là đơn cấu.

Định nghĩa.

Một vành con A chứa phần tử 1 của trường F được gọi là *trường con* nếu A ổn định với phép lấy phần tử nghịch đảo.

Nhận xét 0.3.

- (i) Một trường con của F là một trường với các phép toán cảm sinh.
- (ii) Giao của một họ khác rỗng các trường con là một trường con.

Cho F là một trường. Xét ánh xạ

$$\begin{aligned}\varphi : \mathbb{Z} &\longrightarrow F \\ m &\longmapsto m 1_F.\end{aligned}$$

Dễ dàng chứng minh rằng φ là một đồng cấu vành. Xét $\text{Ker}(\varphi)$, ta có các trường hợp sau:

- $\text{Ker}(\varphi) \neq 0$. Do \mathbb{Z} là miền nguyên chính, ta có $\text{Ker}(\varphi) = (p)$ với $p > 0$ là số nguyên dương nhỏ nhất thỏa $p 1_F = 0$. Rõ ràng p là một số nguyên tố. Suy ra φ cảm sinh một đơn cấu từ \mathbb{Z}_p vào F , do đó F chứa một trường con đẳng cấu với \mathbb{Z}_p . Trường con này chứa trong tất cả các trường con của F . Số nguyên tố p được gọi là **đặc số** của trường F .

- $\text{Ker}(\varphi) = 0$, tức là 0 là số nguyên duy nhất để $m \cdot 1_F = 0$. Khi đó φ mở rộng duy nhất thành một đồng cấu trường từ \mathbb{Q} vào F định bởi $m/n \mapsto \varphi(m)\varphi(n)^{-1}$. Do đó F chứa một trường con đẳng cấu với \mathbb{Q} và trường con này chứa trong tất cả các trường con của F . Khi đó ta nói F là trường có đặc số 0 .

Định nghĩa.

Cho F là một trường. Giao của tất cả các trường con của F gọi là trường con nguyên tố của F .

Từ kết quả trên, ta có:

Mệnh đề 0.4. Một trường đặc số p có trường con nguyên tố đẳng cấu với \mathbb{Z}_p xác định bởi $\overline{m} \mapsto m \cdot 1_F$. Một trường đặc số 0 có trường con nguyên tố đẳng cấu với \mathbb{Q} xác định bởi $\frac{m}{n} \mapsto (m \cdot 1_F)(n \cdot 1_F)^{-1}$.

Nhận xét 0.5. Chú ý rằng chỉ có duy nhất một đồng cấu từ \mathbb{Q} hay \mathbb{Z}_p vào một trường cho trước F và đồng cấu đó xác định như trong mệnh đề trên. Thật vậy, giả sử F có đặc số 0 và $\phi : \mathbb{Q} \longrightarrow F$ là một đồng cấu trường. Khi đó $\forall m \in \mathbb{N}$,

$$\phi(m) = \phi(1 + \cdots + 1) = m\phi(1) = m \cdot 1_F.$$

Hơn nữa, $\phi(-m) = -\phi(m) = -(m1_F) = (-m)1_F$. Hay

$$\phi(m) = m1_F, \forall m \in \mathbb{Z}.$$

Do đó

$$\phi(m/n) = (m1_F)(n1_F)^{-1} \text{ với mọi } m/n \in \mathbb{Q}.$$

Tương tự với trường hợp F có đặc số p và $\phi : \mathbb{Z}_p \longrightarrow F$ là một đồng cấu, ta luôn có $\phi(\overline{m}) = m1_F$.

0.2 VÀNH ĐA THỨC

Cho A là một vành giao hoán có đơn vị $1 \neq 0$. Ký hiệu $A[x]$ là vành các đa thức biến x siêu việt có hệ tử trong A . Một đa thức

$$f = a_0 + a_1x + \cdots + a_nx^n \in A[x], a_n \neq 0$$

gọi là có bậc n , kí hiệu $\deg(f)$. Khi đó vành A chứa trong $A[x]$ như một vành con.

Mệnh đề 0.6 (Tính phổ dụng của vành đa thức). Cho vành đa thức $A[x]$ và R là một vành giao hoán và $\alpha \in R$. Khi đó mọi đồng cấu vành $\tau : A \longrightarrow R$ mở

rộng duy nhất thành đồng cấu vành φ từ $A[x]$ vào R thỏa

$$\varphi(x) = \alpha \text{ và } \varphi(a) = \tau(a), \forall a \in A.$$

Mệnh đề 0.7. *Cho $f, g \in A[x]$ và $g \neq 0$ có hệ tử dẫn đầu khả nghịch. Khi đó, tồn tại duy nhất $q, r \in D[x]$ sao cho $f = gq + r$ với $r = 0$ hay $\deg(r) < \deg(g)$. Đa thức q (tương ứng r) gọi là **thương** (tương ứng **du**) của phép chia (Euclide) f cho g .*

Vành đa thức trên trường đóng một vai trò đặc biệt quan trọng trong Lí thuyết mở rộng trường và Galois. Suốt trong cuốn sách này, ta kí hiệu F là một trường nếu không có giải thích khác.

Hệ quả 0.8. *Mọi ideal của $F[x]$ đều là ideal chính. Hơn thế ideal $(f) \subset F[x]$ là tối đại khi và chỉ khi f bất khả quy.*

Thuật toán Euclide cho phép ta tìm ước chung lớn nhất của 2 đa thức cho trước và hơn thế, cho phép ta tìm các đa thức s, t trong hệ quả sau:

Hệ quả 0.9. *Cho $f, g \in F[x]$. Kí hiệu $d = (f, g)$. Khi đó tồn tại các đa thức $s, t \in F[x]$ sao cho $sf + tg = d$.*

Với Maple, các thuật toán trên trong $\mathbb{Q}[x]$ được cho bởi các lệnh thể hiện trong ví dụ sau:

Sử dụng Maple 1. Để tính dư và thương của phép chia đa thức

$$f = x^5 + 2x^4 + x^3 + x - 1$$

cho $g = x^3 - x + 3$, ta có thể dùng lệnh `rem` hoặc `quo`:

```
> rem(x^5+2*x^4+x^3+x-1,x^3-x+3,x,'q');
```

$$-7 - 3x - x^2$$

```
> q;
```

$$x^2 + 2x + 2$$

Như thế khi chia f cho g ta được thương là $x^2 + 2x + 2$ và dư là $-7 - 3x - x^2$.

Để tính ước chung lớn nhất trong $\mathbb{Q}[x]$, ta dùng lệnh

```
> gcdex(x^5+2*x^4+x^3+x-1,x^3-x+3,x);
```

$$1$$

Lệnh trên cũng cho ta tính được đa thức s, t sao cho $sf + tg = d$ như ví dụ sau đây.

```
> gcdex(x^5+2*x^4+x^3+x-1, x^3-x+3, x, 's', 't');
```

1

```
> s, t;
```

$$-\frac{64}{511} + \frac{24}{511}x - \frac{1}{511}x^2, \frac{149}{511} + \frac{18}{511}x^2 + \frac{79}{511}x - \frac{22}{511}x^3 + \frac{1}{511}x^4$$

Tính toán trong vành $\mathbb{Z}_p[x]$, ta dùng lệnh Rem và Gcdex tương ứng.

Mệnh đề 0.10. Cho $f \in \mathbb{Z}[x]$ bất khả quy trên \mathbb{Z} . Khi đó f bất khả quy trên \mathbb{Q} .

Định nghĩa.

Cho D là một miền nguyên Gauss. Một đa thức thuộc vành $D[x]$ gọi là **chuẩn tắc** nếu hệ tử dẫn đầu của f bằng 1.

Mệnh đề 0.11. Cho $f \in \mathbb{Z}[x]$ là một đa thức chuẩn tắc. Nếu $g \in \mathbb{Q}[x]$ là một ước chuẩn tắc của f trong $\mathbb{Q}[x]$ thì $g \in \mathbb{Z}[x]$.

Chứng minh. Xem BT 0.14. □

Mệnh đề 0.12 (Tiêu chuẩn bất khả quy của Eisenstein).

Cho $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. Nếu tồn tại một số nguyên tố p sao cho: $p \nmid a_n$, $p \mid a_i, \forall i = 0, \dots, n-1$ và $p^2 \nmid a_0$ thì f bất khả quy trong $\mathbb{Q}[x]$.

Mệnh đề 0.13. Cho $f = a_0 + \cdots + a_n x^n \in \mathbb{Q}[x]$. Nếu phân tử $\frac{r}{s} \in \mathbb{Q}$, với $(r, s) = 1$, là nghiệm của f thì $r \mid a_0$ và $s \mid a_n$.

Sử dụng Maple 2. Maple có thể tìm dạng nhân tử hóa của một đa thức khác 0 bất kỳ trong $\mathbb{Q}[x]$ hay $\mathbb{Z}_p[x]$ bằng lệnh `factor` hay `Factor`.

> `factor(2*x^4+4*x^3+11*x^2+2*x+5);`

$$(2x^2 + 1)(x^2 + 2x + 5)$$

> `Factor(2*x^4+4*x^3+11*x^2+2*x+5) mod 13;`

$$2(x + 4)(x^2 + 7)(x + 11)$$

Xét vành thương \mathbb{Z}_m . Toàn cấu chính tắc $\mathbb{Z} \longrightarrow \mathbb{Z}_m$ mở rộng tầm thường thành toàn cấu vành $\mathbb{Z}[x] \longrightarrow \mathbb{Z}_m[x]$ biến $f = a_n x^n + \cdots + a_0$ thành $\bar{f} := \bar{a}_n x^n + \cdots + \bar{a}_0$.

Mệnh đề 0.14. Cho $f \in \mathbb{Z}[x]$. Nếu tồn tại một số nguyên tố p không chia hết hệ tử cao nhất của f và \bar{f} bất khả quy trong $\mathbb{Z}_p[x]$ thì f bất khả quy trong $\mathbb{Q}[x]$.

Chứng minh. Xem Bài tập 0.8. □

Chú ý rằng, mệnh đề trên chỉ cho một điều kiện đủ. Có những đa thức bất khả quy trong $\mathbb{Q}[x]$ nhưng ảnh của nó trong $\mathbb{Z}_p[x]$ là khả quy với mọi số nguyên tố p , xem Bài tập 0.6.

0.3 MỘT SỐ NHÓM HỮU HẠN

Cấp của một nhóm (nhân) hữu hạn G là số phần tử của nhóm, kí hiệu $(G : 1)$ hay $|G|$. Cấp của một phần tử $a \in G$ là cấp của nhóm con cyclic sinh ra bởi a . Ta giới thiệu một số nhóm hữu hạn quan trọng sẽ gặp trong nội dung của cuốn sách này.

a) Nhóm dihedral D_{2n}

Nhóm dihedral D_{2n} còn gọi là nhóm các phép đối xứng của đa giác đều n cạnh P_n , tức là nhóm các phép biến đổi đẳng cự của mặt phẳng biến P_n thành chính nó. Gọi σ là phép quay có tâm là tâm của P_n và góc quay là $2\pi/n$ (góc định hướng).

Rõ ràng σ có cấp n . Gọi τ là phép đối xứng trục với trục đối xứng đi qua một đỉnh chọn trước của P_n . Cấp của τ bằng 2. Khi đó

$$D_{2n} = \{\tau^i \sigma^j \mid i = 0, 1; j = 1, \dots, n\}$$

có cấp bằng $2n$.

Dễ dàng chỉ ra rằng

$$D_{2n} = \langle \sigma, \tau \mid \sigma^n = \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle.$$

b) Nhóm đối xứng S_n

Nhóm đối xứng S_n là nhóm các phép hoán vị n phần tử của tập $\Omega = \{1, \dots, n\}$, có cấp bằng $n!$. Mỗi phần tử của S_n gọi là một phép thế. Nhóm đối xứng S_n với $n \geq 3$ là một nhóm không giao hoán.

Một vòng xích $\sigma = (a_1 a_2 \dots a_m)$ gồm các số tự nhiên phân biệt của Ω biểu diễn một phép thế của S_n định bởi $\sigma(a_i) = a_{i+1}$ với $1 \leq i \leq m-1$, $\sigma(a_m) = a_1$ và giữ nguyên các phần tử còn lại của Ω .

Vòng xích σ gọi là có độ dài m nếu nó chứa m phần tử. Hai vòng xích gọi là độc lập nếu chúng không có phần tử chung. Tích của 2 vòng xích độc lập có tính giao

hoán. Có thể chứng minh dễ dàng kết quả sau.

Mệnh đề 0.15. Mọi phép thế đều có thể biểu diễn một cách duy nhất (sai khác thứ tự) dưới dạng tích của các vòng xích độc lập. Biểu diễn này được gọi là *biểu diễn vòng xích của phép thế*.

Ví dụ 3. Trong S_{12} , cho phép thế σ định bởi:

σ	1	2	3	4	5	6	7	8	9	10	11	12
	12	2	3	1	11	9	5	10	6	4	7	8

Ta có $\sigma = (1\ 12\ 8\ 10\ 4)(5\ 11\ 7)(6\ 9)$.

Khi được biểu diễn bằng tích của các vòng xích độc lập, nghịch đảo của phép thế được xác định một cách dễ dàng bằng cách viết đảo ngược các phần tử trong các vòng xích độc lập của nó. Ví dụ, với phép thế σ ở trên, ta có $\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(7\ 11\ 5)(6\ 9)$.

Ta cũng dễ dàng chứng minh được kết quả sau.

Mệnh đề 0.16. Cấp của phép thế σ bằng bội chung nhỏ nhất của độ dài của các vòng xích trong biểu diễn vòng xích của σ .

Chứng minh. Xem Bài tập 0.16. □

Một vòng xích có độ dài bằng 2 gọi là một **phép chuyển trí**. Mọi vòng xích đều được biểu diễn (không duy nhất) bằng tích của các phép chuyển trí, chẳng hạn :

$$\sigma = (a_1 a_2 \dots a_m) = (a_1 a_m) \cdots (a_1 a_3)(a_1 a_2). \quad (1)$$

Từ đó suy ra :

Mệnh đề 0.17. Mọi phép thế đều biểu diễn được dưới dạng tích của các phép chuyển trí.

Như thế tập hợp **T** tất cả các phép chuyển trí của S_n sinh ra S_n . Kết quả sau cũng được sử dụng sau này.

Mệnh đề 0.18. Nhóm đối xứng S_n được sinh bởi vòng xích $(1\ 2\ \dots\ n)$ và phép chuyển trí $(1\ 2)$.

Chứng minh. Cho $c = (1\ 2\ \dots\ n)$ và $t = (1\ 2)$. Gọi G là nhóm con sinh bởi t và c . Khi đó G chứa phần tử $c t c^{-1} = (2\ 3)$, nên chứa

$$c(2\ 3)c^{-1} = (3\ 4), \dots$$

và do đó chứa các phép chuyển trí dạng $(m \ m+1)$. Suy ra G chứa các phần tử

$$(1\ 2)(2\ 3)(1\ 2) = (1\ 3); \quad (1\ 3)(3\ 4)(1\ 3) = (1\ 4); \dots$$

như thế G chứa các phép chuyển trí dạng $(1\ m)$. Do đó G chứa các phần tử dạng $(1\ m)(1\ r)(1\ m) = (m\ r)$ với mọi $m, r \in \{1, \dots, n\}$. Tất cả các phép chuyển trí sinh ra S_n như đã thấy ở mệnh đề trên. Do đó $G = S_n$. \square

Ta nhắc lại khái niệm dấu của phép thế và giới thiệu nhóm thay phiên A_n .

Đặt

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Với $\sigma \in S_n$, tác động của σ trên Δ_n định bởi:

$$\sigma(\Delta_n) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Do σ là một song ánh, mỗi nhân tử $(x_i - x_j)$ của Δ_n xuất hiện đúng một lần với dấu $+$ hay $-$ trong $\sigma(\Delta_n)$. Như thế, ta có $\sigma(\Delta_n) = \pm \Delta_n$.

Đặt

$$\text{sign}(\sigma) = \frac{\sigma(\Delta_n)}{\Delta_n} \in \{\pm 1\}$$

gọi là **dấu** của phép thế σ .

Định nghĩa. Phép thế σ gọi là **phép thế chẵn** nếu $\text{sign}(\sigma) = 1$, là **phép thế lẻ** nếu $\text{sign}(\sigma) = -1$.

Mệnh đề 0.19. Ánh xạ $\text{sign} : S_n \longrightarrow \{\pm 1\}$ là một toàn cấu nhóm.

Chứng minh. Ta có

$$\begin{aligned} \text{sign}(\tau\sigma) &= \frac{\prod_{1 \leq i < j \leq n} (x_{\tau\sigma(i)} - x_{\tau\sigma(j)})}{\prod_{1 \leq i < j \leq n} (x_{\sigma(i)-\sigma(j)})} \frac{\prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})}{\prod_{1 \leq i < j \leq n} (x_i - x_j)} \\ &= \text{sign}(\tau) \text{sign}(\sigma). \end{aligned}$$

Dễ thấy rằng sign là một toàn ánh vì ảnh của phép chuyển trí $(1\ 2)$ bằng -1 . Như thế sign là một toàn cấu nhóm. \square

Hệ quả 0.20. Tập hợp tất cả các phép thế chẵn trong S_n là một nhóm con chuẩn tắc của S_n có chỉ số bằng 2, gọi là nhóm thay phiên (trên n phần tử), kí hiệu A_n .

Ví dụ 4. Ta tính dấu của phép chuyển trí tùy ý $(i j)$. Ta đã biết phép chuyển trí $(1 2)$ là một phép thế lẻ. Gọi $\tau = (1 i)(2 j)$ là phép thế hoán vị 1 cho i và 2 cho j . Khi đó ta có $(i j) = \tau(1 2)\tau$. Vì sign là đồng cấu nhóm, ta có

$$\text{sign}(i j) = (-1) \text{sign}(\tau)^2 = -1.$$

Vậy phép chuyển trí là phép thế lẻ.

Mệnh đề 0.21. Một vòng xích độ dài m là phép thế lẻ khi và chỉ khi m là số chẵn. Suy ra, một phép thế σ là lẻ khi và chỉ khi số các vòng xích độ dài chẵn trong biểu diễn vòng xích của σ là một số lẻ.

Chứng minh. Một vòng xích độ dài m có thể biểu diễn như tích của $m - 1$ phép chuyển trí (xem (1)). Do mỗi phép chuyển trí là lẻ, suy ra điều phải chứng minh. \square

c) Nhóm quaternion

Nhóm quaternion Q_8 là nhóm có 8 phần tử, xác định như sau. Cho

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\},$$

với phép nhân định bởi:

- $1a = a1 = a$ với mọi $a \in Q_8$;
- $(-1)(-1) = 1$; $(-1)a = a(-1) = -a$ với mọi $a \in Q_8$;
- $ii = jj = kk = -1$;
- $ij = k$; $ji = -k$;
- $jk = i$; $kj = -i$;
- $ki = j$; $ik = -j$.

Dễ dàng kiểm tra tất cả các tiên đề của nhóm đều thỏa mãn.

0.4 HÀM EULER

Ta nhắc lại khái niệm hàm Euler và một số tính chất quan trọng của nó. Phần chứng minh các tính chất này được thực hiện trong phần Bài tập.

Hàm Euler φ là một ánh xạ từ \mathbb{N}^* vào \mathbb{N}^* định bởi

Định nghĩa.

$$\varphi(n) = \#\{m \in \mathbb{N} \mid m \leq n, (m, n) = 1\}.$$

Nghĩa là $\varphi(n)$ là số các số tự nhiên không lớn hơn n và nguyên tố cùng nhau với n .

Một số tính chất của hàm Euler được phát biểu trong mệnh đề sau.

Mệnh đề 0.22. Kí hiệu φ là hàm Euler. Khi đó:

- (i) $\varphi(p) = p - 1$ với p là số nguyên tố ;
- (ii) $\varphi(p^m) = (p - 1)p^{m-1}$;
- (iii) $\varphi(ab) = \varphi(a)\varphi(b)$ với mọi $(a, b) = 1$;
- (iv) Nếu $a = p_1^{m_1} \cdots p_r^{m_r}$ thì

$$\varphi(a) = a \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) ;$$

- (v) $\sum_{d|n} \varphi(d) = n.$

Chứng minh. Xem Bài tập 0.17. □

Bài tập

👉 **0.1.** Chọn đúng (Đ), sai (S) cho các mệnh đề sau:

- a) Hai đa thức bất kỳ của $F[x]$ đều tồn tại ước chung lớn nhất.
- b) Tương ứng từ $F[x]$ vào \mathbb{Z} cho bởi $f \mapsto \deg(f)$ là một đồng cấu vành.
- c) Mọi trường đều đẳng cấu với trường các thương của nó.
- d) Vành \mathbb{Z}_n là một miền nguyên khi và chỉ khi nó là một trường.
- e) Mọi đa thức trên trường F đều có một nghiệm trong F .
- f) Mọi đa thức bất khả quy trên \mathbb{Q} đều bất khả quy trên \mathbb{Z} .
- g) Mọi đa thức bất khả quy trên \mathbb{Q} thì bất khả quy trên \mathbb{R} .
- h) Có vô hạn các đa thức bất khả quy bậc n trên \mathbb{Q} (trên \mathbb{R} , trên \mathbb{C}).
- i) Những đa thức nguyên tố cùng nhau thì có bậc khác nhau. (Xem HD 250)

👉 **0.2.** Cho F là trường có đặc số $p > 0$. Xét ánh xạ

$$\begin{aligned}\varphi : F &\longrightarrow F \\ a &\longmapsto a^p.\end{aligned}$$

gọi là **ánh xạ Frobenius**. Chứng minh rằng φ là một đồng cấu trường. Suy ra nếu F là trường hữu hạn thì φ là một tự đẳng cấu. (Xem HD 250)

👉 **0.3.** Cho D là miền nguyên và F_D là trường các thương của nó. Cho K là một trường và $\tau : D \longrightarrow K$ là một đơn cấu vành. Chứng minh rằng tồn tại duy nhất một đồng cấu trường $\varphi : F_D \longrightarrow K$ sao cho $\varphi(a) = \tau(a), \forall a \in D$. Suy ra tính duy nhất của trường các thương của D . (Xem HD 250)

👉 **0.4.** Xác định các tự đồng cấu của trường các số hữu tỷ. Tương tự, xác định các tự đồng cấu của \mathbb{Z}_p ; suy ra công thức Fermat $a^p \equiv a \pmod{p}$ với mọi $a \in \mathbb{Z}$. (Xem HD 251)

👉 **0.5.** Chứng minh rằng một trường F có đặc số 0 (tương ứng p nguyên tố) khi và chỉ khi tồn tại một đồng cấu (đơn cấu) trường từ \mathbb{Q} (tương ứng \mathbb{Z}_p) vào F . Hơn nữa, đồng cấu trường đó là duy nhất.

(Xem HD 252)

🍰 **0.6.** Cho $f = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$. Chứng minh rằng f bất khả quy trên \mathbb{Z} nhưng khả quy khi xét như một đa thức trong $\mathbb{Z}_p[x]$ với mọi p nguyên tố.

(Xem HD 252)

🍰 **0.7.** Chứng minh Hệ quả 0.8.

(Xem HD 252)

🍰 **0.8.** Chứng minh Mệnh đề 0.14.

(Xem HD 253)

🍰 **0.9.** Tìm $d = (f, g)$ với $f, g \in \mathbb{Z}_{11}[x]$ cho bởi $f = x^5 + 2x^4 + 3x^3 + 3x^2 - 5x + 2$, $g = 2x^3 + 7x^2 + 5x - 2$. Tìm $s, t \in \mathbb{Z}_{11}[x]$ sao cho $sf + tg = d$. Nên sử dụng Maple.

(Xem HD 253)

🍰 **0.10.** Chứng minh dạng tổng quát của MĐ. 0.10: cho D là miền nguyên Gauss và F_D là trường các thương của D . Nếu $f \in D[x]$ bất khả quy trên D thì bất khả quy trên F_D .

(Xem HD 253)

🍰 **0.11.** Xác định tính bất khả quy của các đa thức sau đây. Trong trường hợp khả quy, tìm dạng nhân tử hóa của đa thức trên trường chỉ ra.

a) $x^4 + 1$ trên \mathbb{Q} .

b) $x^4 + 1$ trên \mathbb{R} .

c) $x^7 + 11x^3 - 33x + 22$ trên \mathbb{Q} .

d) $x^4 + x^3 + x^2 + x + 1$ trên \mathbb{Q} .

e) $x^3 - 7x^2 + 3x + 3$ trên \mathbb{Q} .

f) $x^4 + 15x^3 + 7$ trên \mathbb{Q} .

g) $x^4 + 7$ trên \mathbb{Z}_{17} .

h) $x^3 - 5$ trên \mathbb{Z}_{11} . (Xem HD 253)

✎ **0.12.** Tìm nghiệm của các đa thức sau đây (trước tiên trong \mathbb{Q} sau đó trong \mathbb{R}, \mathbb{C}).

a) $x^3 + 1$.

b) $x^3 - 6x^2 + 11x - 6$.

c) $x^5 + x + 1$.

d) $x^2 + 1$.

e) $x^4 + x^3 + x^2 + x + 1$.

f) $x^4 - 6x^2 + 11$.

(Xem HD 254)

✎ **0.13.** Tìm tất cả các đa thức chuẩn tắc $x^2 + bx + c \in \mathbb{Z}_5[x]$. Đa thức nào bất khả quy? Trong mỗi trường hợp, tính $\Delta := b^2 - 4c$. Dự đoán và chứng minh tiêu chuẩn bất khả quy theo Δ . (Xem HD 254)

✎ **0.14.** Chứng minh Mệnh đề 0.11.

(Xem HD 254)

✎ **0.15.** Cho p là một số nguyên tố. Chứng minh rằng trong $\mathbb{Z}_p[x]$ có đúng $\frac{p^2 - p}{2}$ đa thức chuẩn tắc bất khả quy bậc 2. (Xem HD 255)

✎ **0.16.** Chứng minh Mệnh đề 0.16 bằng cách chứng minh các khẳng định sau.

- Nếu $\sigma = (a_1 a_2 \dots a_m)$ thì với mọi $i \in \{1, 2, \dots, m\}$, ta có $\sigma^i(a_k) = a_{k+i}$ với $k + i$ được lấy thẳng dư theo modulo m .
- Trong một nhóm nhân G , cho a, b là 2 phần tử giao hoán được, khi đó $(ab)^n = a^n b^n$ với mọi $n \in \mathbb{Z}$.

✎ **0.17.** Cho φ là hàm Euler. Chứng minh rằng

- nếu $q \mid n$ thì $\varphi(qn) = q\varphi(n)$;
- nếu $(p, n) = 1$ và p nguyên tố thì $\varphi(pn) = (p - 1)\varphi(n)$;
- suy ra nếu p nguyên tố và $(p, n) = 1$ thì

$$\varphi(p^m n) = (p - 1)p^{m-1}\varphi(n);$$

- suy ra $\varphi(ab) = \varphi(a)\varphi(b)$, $\forall (a, b) = 1$;

e) $\sum_{d|n} \varphi(d) = n.$

(Xem HD 255)

* **0.18.** Cho F là một trường. Chứng minh rằng mọi nhóm con hữu hạn của nhóm nhân $F^* = F - \{0\}$ là một nhóm cyclic. Suy ra nếu F là trường hữu hạn thì F^* là nhóm cyclic. (Xem HD 256)

* **0.19.** Xác định tập các tự đồng cấu của trường \mathbb{R} . (Xem HD 257)

Chương 1

MỞ RỘNG TRƯỜNG



§ 1 MỞ RỘNG TRƯỜNG. BẬC CỦA MỞ RỘNG TRƯỜNG

1.1 MỞ RỘNG TRƯỜNG

Định nghĩa.

Cho trường K và F là một trường con của K . Khi đó $F \subset K$ gọi là một mở rộng trường và K được gọi là một mở rộng (trường) của F . Một mở rộng trường $F \subset K$ còn được kí hiệu là $K : F$ hay K/F .

Nhận xét 1.1. (i) Mọi trường đều là mở rộng của trường con nguyên tố của nó.

(ii) Cho $K : F$ là một mở rộng trường. Khi đó trường con nguyên tố của chúng trùng nhau.

Ví dụ 5. $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{Q} \subset \mathbb{C}$, $\mathbb{R} \subset \mathbb{C}$ là các mở rộng trường.

Ví dụ 6. Cho F là một trường và $F(x)$ là trường các phân thức hữu tỷ biến x siêu việt trên F . Đồng nhất F với các phân thức hằng, ta có $F \subset F(x)$ là một mở rộng trường.

Định nghĩa.

Cho $K : F$ và $L : F$ là các mở rộng trường của F . Một đồng cấu (đẳng cấu) trường $\varphi : K \longrightarrow L$ thỏa $\varphi(a) = a, \forall a \in F$ gọi là F -đồng cấu (F -đẳng cấu). Mở rộng $K : F$ được gọi là F -đẳng cấu với mở rộng $L : F$ nếu tồn tại một F -đẳng cấu từ K vào L , kí hiệu $K \cong_F L$. Nếu $K = L$ thì các F -đồng cấu (F -đẳng cấu) gọi là F -tự đồng cấu (F -tự đẳng cấu).

Tổng quát hơn, ta có:

Định nghĩa.

Cho $F \subset K$ và $E \subset L$ là các mở rộng trường, cho $\tau : F \longrightarrow E$ là một đồng cấu (đẳng cấu) trường. Đồng cấu (đẳng cấu) $\varphi : K \longrightarrow L$ gọi là một **mở rộng** của τ nếu $\varphi(a) = \tau(a)$, $\forall a \in F$.

Định nghĩa.

Mở rộng $F \subset K$ gọi là **đẳng cấu** với mở rộng $E \subset L$ nếu tồn tại các đẳng cấu $i : F \longrightarrow E$ và một mở rộng của nó $j : K \longrightarrow L$, nghĩa là $j(a) = i(a)$, $\forall a \in F$.

Nhận xét 1.2. Quan hệ đẳng cấu của các mở rộng trường là một quan hệ tương đương. Đặc biệt, quan hệ “ \cong_F ” là một quan hệ tương đương.

Mệnh đề 1.3. Cho $K : F$ và $L : F$ là các mở rộng trường, cho $\varphi : K \longrightarrow L$ là một F -đồng cấu. Cho $\alpha \in K$ là một nghiệm của $f \in F[x]$. Khi đó $\varphi(\alpha) \in L$ là một nghiệm của f .

Chứng minh. Gọi $f = a_n x^n + \cdots + a_0$. Ta có

$$f(\alpha) = a_n \alpha^n + \cdots + a_0 = 0.$$

Suy ra

$$0 = \varphi(f(\alpha)) = a_n \varphi(\alpha)^n + \cdots + a_0 = f(\varphi(\alpha)).$$

Nghĩa là $\varphi(\alpha)$ là một nghiệm của f . □

Ta có dạng tổng quát của mệnh đề trên, xem Bài tập 1.8.

1.2 BẬC CỦA MỞ RỘNG TRƯỜNG

Cho $K : F$ là một mở rộng trường. Khi đó K có cấu trúc của một không gian véc tơ trên F với phép nhân vô hướng là phép nhân trên K . Một cơ sở của F —không gian véc tơ K cũng được gọi là cơ sở của mở rộng trường $K : F$.

Định nghĩa.

Bậc của mở rộng trường $K : F$ là chiều của F —không gian véc tơ K , kí hiệu $[K : F]$. Nếu $[K : F]$ hữu hạn thì ta gọi $K : F$ là một mở rộng hữu hạn. Nếu mở rộng $K : F$ không hữu hạn thì gọi là mở rộng vô hạn.

Ví dụ 7. Xét mở rộng trường $\mathbb{C} : \mathbb{R}$. Ta biết mọi phần tử của \mathbb{C} được viết một cách duy nhất dưới dạng $a + bi$ với $a, b \in \mathbb{R}$. Do đó $\{1, i\}$ là một cơ sở của $\mathbb{C} : \mathbb{R}$. Suy ra $[\mathbb{C} : \mathbb{R}] = 2$.

Ví dụ 8. Các mở rộng trường \mathbb{R}/\mathbb{Q} , \mathbb{C}/\mathbb{Q} , $K(x)/K$ là các mở rộng vô hạn.

Nhận xét 1.4. Bậc của mở rộng $F \subset K$ bằng 1 khi và chỉ khi $F = K$. Nói cách khác bậc của mở rộng trường bằng 1 khi và chỉ khi mở rộng là tầm thường. Thật vậy, nếu $K = F.\alpha$ thì $1 = a\alpha$, kéo theo $\alpha = a^{-1} \in F$. Do đó $F = K$.

Định lý 1.5. Cho $K : F$ và $L : K$ là các mở rộng trường. Khi đó $L : F$ là một mở rộng trường và

$$[L : F] = [L : K][K : F].$$

Hơn thế nếu $\{e_i\}_{i \in I}$ và $\{f_j\}_{j \in J}$ lần lượt là cơ sở của $K : F$ và $L : K$ thì $\{e_i f_j\}_{i \in I, j \in J}$ là một cơ sở của $L : F$.

Chứng minh.

Kí hiệu $E = \{e_i\}_{i \in I}$, $S = \{f_j\}_{j \in J}$ và $ES = \{e_i f_j\}_{i \in I, j \in J}$. Cho $u \in L$. Khi đó $u = \sum a_j f_j$ với $a_j \in K$. Do a_j biểu thị tuyến tính qua E nên thay a_j trong biểu diễn của u bởi các tổ hợp tuyến tính của S , ta có biểu diễn tuyến tính của u qua ES . Do đó ES là hệ sinh của không gian véc tơ L trên F .

Ta chứng minh rằng ES độc lập tuyến tính. Xét một tổ hợp tuyến tính trong L cho bởi $\sum_{i,j} a_{ij} e_i f_j = 0$ với $a_{ij} \in F$. Ta viết $\sum_j (\sum_i a_{ij} e_i) f_j = 0$ như một quan hệ

tuyến tính tầm thường của S . Do S độc lập tuyến tính, ta có $\sum_i a_{ij}e_i = 0$ với mọi j . Mặt khác, do E độc lập tuyến tính, ta có $a_{ij} = 0$ với mọi i, j . Vậy ES độc lập tuyến tính. \square

Nhận xét 1.6. Định lý trên cho thấy rằng $L : F$ là mở rộng hữu hạn khi và chỉ khi $L : K$ và $K : F$ là các mở rộng hữu hạn.

Bài tập

👉 **1.1.** Trong các trường hợp sau, đâu là mở rộng trường ?

a) $\mathbb{Q} \subset A := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} ;$

b) $\mathbb{Q} \subset B := \{a + b\sqrt{\alpha} \mid a, b \in \mathbb{Q}\}$ với $\alpha \in \mathbb{N} ;$

c) $\mathbb{Q} \subset C := \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\} ;$

d) $\mathbb{Q} \subset D := \{a + bi \mid a, b \in \mathbb{Q}\} ?$

(Xem HD 257)

👉 **1.2.** Xác định bậc của các mở rộng trường tìm được trong bài tập trên. (Xem HD 257)

👉 **1.3.** Chứng minh rằng $\mathbb{Q}[\sqrt{3}] := \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ và $\mathbb{Q}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ đều là các mở rộng trường bậc 2 của \mathbb{Q} nhưng không đẳng cấu với nhau. (Xem HD 257)

👉 **1.4.** Chứng minh rằng mở rộng $\mathbb{R} : \mathbb{Q}$ là vô hạn. (Xem HD 258)

👉 **1.5.** Chứng minh rằng mọi tự đồng cấu trường $\varphi : K \longrightarrow K$ đều là P -tự đồng cấu với P là trường con nguyên tố của K . (Xem HD 258)

👉 **1.6.** Chứng minh rằng quan hệ đẳng cấu của các mở rộng trường là một quan hệ tương đương.

👉 **1.7.** Cho $F \subset K$ là một mở rộng trường. Một trường E thỏa $F \subset E \subset K$ được gọi là *trường trung gian* của mở rộng $F \subset K$. Chứng minh rằng mọi mở rộng trường bậc nguyên tố không có trường trung gian nào khác F và K . (Xem HD 258)

👉 **1.8.** a) Cho $\tau : F \longrightarrow E$ là một đồng cấu trường. Khi đó τ mở rộng thành một đơn

cầu vánh $\tau_* : F[x] \longrightarrow E[x]$ định bởi:

$$\tau_*(a_0 + \cdots + a_n x^n) = \tau(a_0) + \cdots + \tau(a_n) x^n.$$

Đặc biệt, chỉ ra rằng nếu τ là đẳng cấu trường thì τ_* là đẳng cấu vánh và khi đó, nếu $f \in F[x]$ bất khả quy trên F thì $\tau_*(f)$ bất khả quy trên E . Để đơn giản, ta thường viết $\tau_* f$ thay cho $\tau_*(f)$.

b) Cho $F \subset K$ và $E \subset L$ là các mở rộng trường; cho $\tau : F \longrightarrow E$ là một đồng cấu trường và $\varphi : K \longrightarrow L$ là một mở rộng của τ . Chứng minh rằng nếu $\alpha \in K$ là nghiệm của $f \in F[x]$ thì $\varphi(\alpha) \in L$ là nghiệm của $\tau_* f$.

(Xem HD 258)

§ 2 MỞ RỘNG ĐƠN

2.1 VÀNH CON VÀ TRƯỜNG CON SINH RA BỞI MỘT TẬP

Định nghĩa.

Cho K là một trường và S là một tập con của K . Giao của tất cả các vành con (trường con) của K chứa S là một vành con (trường con) của K , gọi là **vành con (trường con) sinh ra bởi S** . Vành con (trường con) sinh ra bởi S là vành con (trường con) nhỏ nhất của K chứa S .

Định nghĩa.

Cho $F \subset K$ là một mở rộng trường, cho S là một tập con của K . Vành con (trường con) sinh ra bởi $F \cup S$ trong K được gọi là **vành con (trường con) sinh ra bởi S trên F** , kí hiệu $F[S]$ (tương ứng $F(S)$).

Nếu $S = \{s_1, \dots, s_n\}$ thì ta kí hiệu $F[s_1, \dots, s_n]$ cho $F[S]$. Tương tự kí hiệu $F(s_1, \dots, s_n)$ cho $F(S)$.

Nhận xét 2.1.

(i) Ta có $F(s_1, \dots, s_n) = F(s_1, \dots, s_{n-1})(s_n)$, $\forall n \geq 2$.

(ii) Nếu $S \subset F$, đặc biệt khi $S = \emptyset$ thì $F[S] = F(S) = F$. Trong trường hợp $S \neq \emptyset$ ta có kết quả sau:

Mệnh đề 2.2. Cho mở rộng trường $F \subset K$ và $\emptyset \neq S$ là một tập con của K . Khi đó

- (i) $F[S] = \left\{ \sum_{\text{hữu hạn}} a_{i_1 \dots i_n} s_1^{i_1} \cdots s_n^{i_n} \mid a_{i_1 \dots i_n} \in F, s_j \in S, n \in \mathbb{N} \right\}$ với quy ước $s^0 = 1, \forall s \in S$;
- (ii) $F(S) = \left\{ \frac{f}{g} := fg^{-1} \mid f, g \in F[S], g \neq 0 \right\}$. Nói cách khác, tập $F(S)$ là trường các thương của $F[S]$.

Chứng minh. (i) Đặt

$$E = \left\{ \sum_{\text{hữu hạn}} a_{i_1 \dots i_n} s_1^{i_1} \cdots s_n^{i_n} \mid a_{i_1 \dots i_n} \in F, s_j \in S, n \in \mathbb{N} \right\}.$$

Ta chứng minh rằng E là vành con nhỏ nhất chứa $F \cup S$. Rõ ràng $F \subset E$ do quy ước trên. Tập E là một vành con vì nó là một nhóm con và đóng kín với phép nhân. Cuối cùng mọi vành con của K chứa $F \cup S$ đều chứa các phần tử của E .

(ii) Hiển nhiên do tính nhỏ nhất của trường các thương.



Ví dụ 9. $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}(i)$. Tương tự, ta có $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$.

2.2 CẤU TRÚC CỦA MỞ RỘNG ĐƠN

Định nghĩa.

Mở rộng trường $F \subset K$ gọi là mở rộng đơn nếu tồn tại $\alpha \in K$ sao cho $K = F(\alpha)$. Phần tử α gọi là phần tử nguyên thủy của mở rộng đơn. Chú ý rằng một mở rộng đơn có thể có nhiều phần tử nguyên thủy khác nhau.

Ví dụ 10. Các mở rộng $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}(\pi)$, $\mathbb{Q} \subset \mathbb{Q}(i)$, $F \subset F(x)$ là các mở rộng đơn.

Định nghĩa.

Cho $K : F$ là mở rộng trường. Phần tử $u \in K$ được gọi là đại số trên F nếu nó là nghiệm của một đa thức f khác 0 trong $F[x]$. Một phần tử $u \in K$ không đại số trên F được gọi là siêu việt trên F .

Định nghĩa.

Mở rộng $K : F$ được gọi là **mở rộng đại số** nếu mọi phần tử của K đều đại số trên F .

Ví dụ 11. Các phần tử $i, \sqrt{2}, \sqrt{2} + \sqrt[3]{5}$ đều đại số trên \mathbb{Q} .

Nhận xét 2.3. Năm 1844, Liouville (1809-1882, Pháp) chứng minh sự tồn tại của số siêu việt (trên \mathbb{Q}). Năm 1873, Hermite (1822-1901, Pháp) chứng minh số e siêu việt. Sau đó, số π siêu việt được Lindemann (1852-1939, Đức) chứng minh năm 1882. Năm 1874, Cantor (1845-1918, Pháp) chứng minh rằng tập các số đại số trên \mathbb{Q} là đếm được và tập các số thực \mathbb{R} là không đếm được. Như thế, số các số thực siêu việt là “nhiều hơn” số các số thực đại số. Tuy nhiên, nói chung, rất khó để chứng minh một số thực cụ thể là siêu việt.

Năm 1934, Gel'fond (1906-1968, Nga) và Schneider độc lập chứng minh bài toán thứ 7 nổi tiếng của Hilbert (1862-1943), rằng các số α^β là siêu việt, trong đó α, β đại số trên \mathbb{Q} , $\alpha \neq 0, 1$ và $\beta \notin \mathbb{Q}$.

Bây giờ, chúng ta sẽ phân tích sâu hơn về cấu trúc của các mở rộng đơn $F(u)$ ứng với các trường hợp u đại số hoặc siêu việt trên F .

Cho $K : F$ là một mở rộng trường và $u \in K$. Xét đồng cấu vành :

$$\begin{aligned}\varphi : F[x] &\longrightarrow F[u] \\ f &\longmapsto f(u).\end{aligned}$$

Rõ ràng φ là một toàn cấu. Xét $\text{Ker}(\varphi)$, có 2 trường hợp như sau :

- $\text{Ker}(\varphi) = 0$. Nghĩa là u siêu việt trên F . Khi đó φ là một đẳng cấu, do đó $F(x) \cong F(u)$.
- $\text{Ker}(\varphi) \neq 0$. Nghĩa là u đại số trên F . Do $F[x]$ là miền nguyên chính nên $\text{Ker}(\varphi) = (f)$, với $0 \neq f \in F[x]$. Khi đó f chính là đa thức có bậc nhỏ nhất nhận u làm nghiệm. Suy ra f bất khả quy và do đó $\text{Ker}(\varphi)$ là iđêan tối đại (xem 0.8). Theo định lý đồng cấu vành, ta có $F[x]/\text{Ker}(\varphi) \cong F[u]$. Do $F[x]/\text{Ker}(\varphi)$ là một trường nên $F[u] = F(u)$.

Như thế, ta đã chứng minh kết quả sau đây :

Mệnh đề 2.4. Cho $K : F$ là một mở rộng trường và $u \in K$.

(i) Nếu u siêu việt trên F thì $F(u) \cong_F F(x)$, trường các phân thức hữu tỷ trên F .

(ii) Nếu u đại số trên F thì

$$F(u) = F[u] \cong_F F[x]/(f)$$

với $f \neq 0$ là một đa thức có bậc nhỏ nhất nhận u làm nghiệm.

Nhận xét 2.5. Cho $K : F$ là mở rộng trường và $u \in K$ đại số trên F . Khi đó :

- (i) Đa thức $0 \neq f \in F[x]$ có bậc nhỏ nhất nhận u làm nghiệm khi và chỉ khi f bất khả quy nhận u làm nghiệm. Điều đó tương đương với $f(u) = 0$ và f chia hết mọi đa thức nhận u làm nghiệm.
- (ii) Nếu f và g là 2 đa thức của $F[x]$ có bậc nhỏ nhất nhận u làm nghiệm thì $\deg(f) = \deg(g)$ và hơn thế $f \sim g$. Trong các đa thức có bậc nhỏ nhất nhận u làm nghiệm, tồn tại duy nhất một đa thức có hệ tử dẫn đầu bằng 1, đa thức đó được gọi là *đa thức tối tiểu của u* . Bậc của f được gọi là *bậc của u* (trên F).

Hệ quả 2.6. Cho $K : F$ là một mở rộng trường và $u \in K$ đại số trên F có bậc n . Khi đó mọi phần tử của $F(u)$ được viết duy nhất dưới dạng

$$a_0 + a_1u + \cdots + a_{n-1}u^{n-1}, \quad a_i \in F$$

với mọi $i = 0, \dots, n-1$. Nói cách khác tập $\{1, u, \dots, u^{n-1}\}$ là một cơ sở của $F(u) : F$. Suy ra mở rộng đơn $F(u) : F$ là một mở rộng hữu hạn.

Chứng minh. Gọi f là đa thức tối tiểu của u . Cho $\alpha \in F(u)$. Gọi $\alpha = b_0 + b_1u + \dots + b_mu^m$. Xét $g = b_0 + b_1x + \dots + b_mx^m$. Tồn tại $q, r \in F[x]$ sao cho $g = fq + r$ với $r = a_0 + a_1x + \dots + a_tx^t$, với $t < n$. Rõ ràng

$$\alpha = g(u) = r(u) = a_0 + a_1u + \dots + a_tu^t.$$

Hơn nữa, nếu có 2 biểu diễn

$$\alpha = a_0 + a_1u + \dots + a_{n-1}u^{n-1} = c_0 + c_1u + \dots + c_{n-1}u^{n-1},$$

thì chúng trùng nhau, nghĩa là $a_i = c_i, \forall i = 0, \dots, n-1$. Thật vậy, nếu không thì $0 = (a_0 - c_0) + \dots + (a_{n-1} - c_{n-1})u^{n-1}$ trái với giả thiết u có bậc n . \square

Mọi mở rộng đơn đại số đều là mở rộng hữu hạn. Điều ngược lại nói chung không đúng. Sau này, ta sẽ xác định điều kiện để một mở rộng hữu hạn là mở rộng đơn đại số.

Hệ quả 2.7. Cho $K : F$ là một mở rộng trường và $u, v \in K$ đại số trên F . Nếu u và v có cùng một đa thức tối thiểu thì tồn tại duy nhất một F -đẳng cấu trường $\varphi : F(u) \longrightarrow F(v)$ sao cho $\varphi(u) = v$.

Chứng minh. Thật vậy các mở rộng đơn $F(u)$ và $F(v)$ đều đẳng cấu với $F[x]/(f)$ với f là đa thức tối thiểu của u và v . □

Ta thấy rằng, ứng với một mở rộng đơn đại số trên F có một lớp các đa thức bất khả quy liên kết với nhau trên F nhận u làm nghiệm. Ngược lại, ta chứng minh rằng :

Mệnh đề 2.8. Cho F là một trường và $f \in F[x]$ là một đa thức bất khả quy. Khi đó tồn tại một mở rộng đơn đại số $F(\alpha) : F$ sao cho α là một nghiệm của f .


Chứng minh. Đặt $K := F[x]/(f)$. Theo (0.8), nhất $a \in F$ với $\bar{a} \in K$, ta có $K : F$ là một mở rộng trường. Đặt $\alpha = \bar{x}$. Rõ ràng $f(\alpha) = \bar{f} = 0$ và $K = F(\alpha)$. □


Bài tập

✎ 2.1. Xác định tính đúng, sai cho các mệnh đề sau :

- a) Mọi trường đều có một mở rộng không tầm thường.
- b) Mọi trường đều có một mở rộng đại số không tầm thường.
- c) Mọi mở rộng đơn đều là mở rộng đại số.
- d) Mọi mở rộng trường đều là mở rộng đơn.
- e) Mọi mở rộng đơn đại số đều đẳng cấu.
- f) Mọi mở rộng đơn siêu việt của một trường cho trước đều đẳng cấu.
- g) Mọi đa thức tối tiểu đều bất khả quy.
- h) Mọi đa thức bất khả quy thuộc $F[x]$ nhận $u \in K \supset F$ làm nghiệm đều có cùng bậc.
- i) Mọi đa thức bất khả quy thuộc $F[x]$ nhận $u \in K \supset F$ làm nghiệm đều là đa thức tối tiểu của u .

j) Bậc của đa thức bất khả quy thuộc $F[x]$ nhận $u \in K \supset F$ làm nghiệm gọi là bậc của u . (Xem HD 258)

 **2.2.** Cho $K = \mathbb{Q}[\alpha]$ với $\alpha \in \mathbb{C}$ là nghiệm của đa thức $x^3 - x^2 + x + 2$. Biểu diễn các phần tử $(\alpha^2 + \alpha + 1)(\alpha^2 - \alpha)$ và $(\alpha - 1)^{-1}$ của K như các đa thức theo α có bậc không quá 2. (Xem HD 258)

 **2.3.** Mô tả các mở rộng đơn $F(\alpha)$ với α là một nghiệm của các đa thức sau trên trường chỉ ra :


a) $x^2 - 5 \in \mathbb{Q}[x]$;

b) $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$;

c) $x^2 + x + 1 \in \mathbb{Z}_2[x]$;

d) $x^3 + 2 \in \mathbb{Q}[x]$.

(Xem HD 259)

 **2.4.** Cho $K : F$ là một mở rộng hữu hạn và $f \in F[x]$ là một đa thức bất khả quy có $\deg(f) > 1$. Chứng minh rằng nếu $[K : F]$ và $\deg(f)$ nguyên tố cùng nhau thì f không có nghiệm trong K . (Xem HD 259)

👉 **2.5.** Cho $K : F$ là một mở rộng trường và $[K : F] = n$. Cho $f \in F[x]$ là đa thức bất khả quy bậc m thỏa $(m, n) = 1$. Chứng minh rằng f bất khả quy trên K .
(Xem HD 259)

👉 **2.6.** Xác định bậc và chỉ ra một cơ sở của các mở rộng trường :

- a) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, i)$; b) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{5}, \sqrt{-2})$;
 c) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{18}, \sqrt[3]{2})$; d) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{27}, 3 + \sqrt{12})$;
 e) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{18}, \sqrt[4]{2})$; f) $\mathbb{Q} \subset \mathbb{Q}(u, \sqrt[3]{2})$ với u là nghiệm của $x^4 + 6x^2 + 3$.

(Xem HD 260)

👉 **2.7.** Xác định tất cả tự đồng cấu của các trường $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt[3]{2})$. (Xem HD 260)

👉 **2.8.** Chứng minh rằng $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$, $\forall a, b \in \mathbb{N}$. (Xem HD 260)

👉 **2.9.** Biểu diễn các trường con sau của $\mathbb{Z}_2(x)$:

a) $\mathbb{Z}_2(x^2)$;

b) $\mathbb{Z}_2(x + 1)$.

(Xem HD 260)

✎ **2.10.** Tìm đa thức tối tiểu của các phần tử sau đây trên trường chỉ ra :

a) $\frac{\sqrt{5} + 1}{2}$ trên \mathbb{Q} ;

b) $\frac{i\sqrt{3} - 1}{2}$ trên \mathbb{Q} ;

c) $\alpha \in \mathbb{Z}_3(t)(\alpha)$ với α thỏa $\alpha^2 = t + 1$ trên $\mathbb{Z}_3(t)$;

d) $\sqrt[4]{5} + \sqrt{5}$ trên \mathbb{Q} ;

e) $\sqrt[3]{2} + \sqrt[3]{4}$ trên \mathbb{Q} ;

f) $u^2 + u$ với u là nghiệm của $x^3 + 3x^2 - 3$;

g) $\xi + \xi^6$ với $\xi = e^{2\pi i/7}$ trên \mathbb{Q} ;

h) $\xi + \xi^2 + \xi^4$ với $\xi = e^{2\pi i/7}$ trên \mathbb{Q} ;

i) $\xi^2 + \xi^5$ với $\xi = e^{2\pi i/7}$ trên \mathbb{Q} .

(Xem HD 260)

✎ **2.11.** Cho α và β lần lượt là nghiệm của $x^2 - 2$ và $x^2 - 4x + 2$ thuộc $\mathbb{Q}[x]$. Chứng minh rằng $\mathbb{Q}(\alpha) \cong_{\mathbb{Q}} \mathbb{Q}(\beta)$.

(Xem HD 261)

✎ **2.12.** Cho F là trường có đặc số khác 2 và f là một đa thức bậc 2 có hệ tử trong

F . Chứng minh rằng cả 2 nghiệm của f đều thuộc một mở rộng đơn $F(u)$ với $u^2 \in F$. Suy ra tính chất “mọi đa thức bậc 2 đều giải được trên mở rộng trường của F nhận được bằng cách ghép vào các căn bậc 2 của các phân tử của F ”. Chứng tỏ rằng tính chất đó không đúng với trường có đặc số 2. (Xem HD 261)

✎ 2.13. a) Chứng minh rằng mọi mở rộng bậc 2 trên \mathbb{Q} đều đẳng cấu với $\mathbb{Q}(\sqrt{d})$ với $d \in \mathbb{Z}$ là một số không chính phương.

b) Chứng minh rằng mọi mở rộng bậc 2 trên \mathbb{R} đều đẳng cấu với \mathbb{C} .

(Xem HD 262)

✎ 2.14. Cho $K : F$ là một mở rộng trường và $[K : F] = n$. Chứng minh rằng bậc của phần tử $u \in K$ là một ước của n . Suy ra nếu n nguyên tố thì $K = F(u)$ với mọi $u \in K \setminus F$. (Xem HD 262)

✎ 2.15. Tìm tất cả các đa thức bất khả quy bậc 2 trên \mathbb{Z}_3 . Mô tả các mở rộng đơn bậc 2 trên \mathbb{Z}_3 . Chứng minh tất cả các mở rộng đơn đó là đẳng cấu với nhau.

(Xem HD 262)

✎ **2.16.** Cho $E = F(\alpha)$ là một mở rộng thực sự của F với α là nghiệm chung của $x^3 - 1$ và $x^4 + x^2 + 1$. Xác định đa thức tối thiểu của α . (Xem HD 262)

✎ **2.17.** Cho $i : F \longrightarrow E$ là một đẳng cấu trường. Gọi α là nghiệm của một đa thức $f = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ bất khả quy. Gọi β là một nghiệm của đa thức

$$i_*f := i(a_0) + i(a_1)x + \cdots + i(a_n)x^n \in E[x].$$

Chứng minh tồn tại một mở rộng $j : F(\alpha) \longrightarrow E(\beta)$ của i sao cho $j(\alpha) = \beta$.
Kết quả trên mở rộng cho Hệ quả 2.7. (Xem HD 262)

✎ **2.18.** Cho mở rộng đơn đại số $F(\alpha)$ với $f \in F[x]$ là đa thức tối thiểu của α . Cho $K : F$ là một mở rộng trường. Chứng minh rằng

a) Nếu $\varphi : F(\alpha) \longrightarrow K$ là một F -đồng cấu thì $\varphi(\alpha)$ là một nghiệm của f .

b) Ánh xạ $\varphi \mapsto \varphi(\alpha)$ xác định một song ánh giữa tập các F -đồng cấu từ $F(\alpha)$ vào K và tập các nghiệm của f trong K . Suy ra số các F -đồng cấu bằng số nghiệm phân biệt của f trong K . (Xem HD 262)

✎ **2.19.** Cho mở rộng đơn đại số $F(\alpha)$ với $f \in F[x]$ là đa thức tối thiểu của α . Cho

$\tau : F \longrightarrow K$ là một đồng cấu trường. Chứng minh:

- a) Nếu $\varphi : F(\alpha) \longrightarrow K$ là một mở rộng của τ thì $\varphi(\alpha)$ là một nghiệm của $\tau_* f$ trong K . Xem Bài tập 1.8 về định nghĩa của $\tau_* f$.
- b) Ánh xạ $\varphi \mapsto \varphi(\alpha)$ là một song ánh giữa tập các mở rộng của τ với tập các nghiệm phân biệt của $\tau_* f$ trong K .

Bài tập này là dạng tổng quát của bài tập trên.

(Xem HD 263)

* **2.20.** Chứng minh các mở rộng $\mathbb{Q} \subset \mathbb{R}$ và $\mathbb{Q} \subset \mathbb{C}$ đều không phải là các mở rộng đơn.

(Xem HD 263)

* **2.21.** Cho F là trường có đặc số khác 2 và cho $E : F$ là một mở rộng trường có bậc bằng 2. Đặt

$$S(E) = \{a \in F^* \mid a = b^2, \text{ với } b \in E\}.$$

Chứng minh rằng:

- a) $S(E)$ là một nhóm con của F^* chứa $(F^*)^2$;

- b) Hai mở rộng bậc hai E, E' của F là F -đẳng cấu khi và chỉ khi $S(E) = S(E')$;
- c) Tồn tại vô hạn các mở rộng bậc hai E_1, E_2, \dots của \mathbb{Q} sao cho $E_i \not\cong E_j, \forall i \neq j$.
- d) Tồn tại duy nhất (sai khác đẳng cấu) một trường có đúng p^2 phần tử.
(Xem HD 264)

§ 3 MỞ RỘNG HỮU HẠN VÀ MỞ RỘNG ĐẠI SỐ

3.1 TÍNH CHẤT CỦA MỞ RỘNG HỮU HẠN VÀ MỞ RỘNG ĐẠI SỐ

Ta biết rằng một mở rộng đơn đại số là mở rộng hữu hạn. Ta có kết quả tổng quát hơn sau đây :

Mệnh đề 3.1. Cho $K : F$ là một mở rộng trường và $u_1, \dots, u_n \in K$ sao cho u_1 đại số trên F và u_j đại số trên $F(u_1, \dots, u_{j-1})$, $\forall j = 2, \dots, n$. Khi đó $F(u_1, \dots, u_n)$ là mở rộng hữu hạn trên F .

Chứng minh. Ta chứng minh bằng quy nạp trên n . Với $n = 1$ ta có mở rộng đơn đại số nên là mở rộng hữu hạn. Giả thiết kết quả đúng cho k . Đặt $E = F(u_1, \dots, u_k)$. Ta có

$$[F(u_1, \dots, u_{k+1}) : F] = [F(u_1, \dots, u_{k+1}) : E][E : F].$$

Theo giả thiết quy nạp, ta có $[E : F]$ hữu hạn. Mặt khác, ta có mở rộng $F(u_1, \dots, u_{k+1}) : E = E(u_{k+1}) : E$ có u_{k+1} đại số trên E nên là mở rộng hữu hạn. Suy ra $F(u_1, \dots, u_{k+1}) : F$ là mở rộng hữu hạn. \square

Mệnh đề 3.2. Mọi phần tử của một mở rộng hữu hạn bậc n đều đại số và có bậc là một ước của n .

Chứng minh. Cho $K : F$ là mở rộng hữu hạn và đặt $n = [K : F]$. Xét $u \in K$. Tập hợp $\{1, u, \dots, u^n\}$ là một tập gồm $n+1$ phần tử trong K nên phụ thuộc tuyến tính. Do đó tồn tại quan hệ tuyến tính không tầm thường $a_0 + a_1u + \dots + a_nu^n = 0$. Nói cách khác u là nghiệm của đa thức $f = a_0 + a_1x + \dots + a_nx^n \in F[x]$ khác 0. Do đó u đại số trên F . Mặt khác, ta có

$$[K : F] = [K : F(u)][F(u) : F] = n.$$

Do đó $[F(u) : F] \mid n$. Vậy bậc của u là ước của n . □

Sau này (xem 3.6) ta sẽ chỉ ra rằng tồn tại các mở rộng đại số không hữu hạn.

Hệ quả 3.3. Một mở rộng $K : F$ là mở rộng hữu hạn khi và chỉ khi tồn tại $u_1, \dots, u_n \in K$ đại số trên F sao cho $K = F(u_1, \dots, u_n)$.

Chứng minh. Giả sử $[K : F] = n$. Gọi $\{u_1, \dots, u_n\}$ là một cơ sở của mở rộng $K : F$. Theo mệnh đề trên u_1, \dots, u_n đại số trên F . Rõ ràng $K = F(u_1, \dots, u_n)$. Điều kiện đủ có được do Mệnh đề 3.1. □

Mệnh đề 3.4. Cho $F \subset K \subset L$ là các mở rộng trường. Khi đó $L : F$ là mở rộng đại số khi và chỉ khi $L : K$ và $K : F$ là các mở rộng đại số.

Chứng minh. Nếu $L : F$ đại số thì rõ ràng các mở rộng $L : K$ và $K : F$ đại số. Ngược lại, giả sử $L : K$ và $K : F$ đại số. Xét $u \in L$. Do u đại số trên K nên ta có $b_0 + b_1 u + \cdots + b_n u^n = 0$ với $b_i \in K$ không đồng thời bằng 0. Xét mở rộng $F(b_0, \dots, b_n, u) : F$, theo Mệnh đề 3.1, đó là một mở rộng hữu hạn. Do đó u đại số trên F . \square

3.2 TRƯỜNG CON CÁC PHẦN TỬ ĐẠI SỐ. TRƯỜNG ĐÓNG ĐẠI SỐ. BAO ĐÓNG ĐẠI SỐ.

Mệnh đề 3.5. Cho $K : F$ là một mở rộng trường. Tập hợp

$$E = \{u \in K \mid u \text{ đại số trên } F\}$$

là một trường con của K chứa F , gọi là trường con các phần tử đại số của K trên F . Suy ra $E : F$ là một mở rộng đại số.

Chứng minh. Vì mọi phần tử thuộc F đều đại số trên F nên $F \subset E$. Cho

$u, v \in E$. Xét mở rộng $F(u, v) : F$. Theo (3.1) và (3.2), ta có $F(u, v)$ là đại số trên F . Suy ra $F(u, v) \subset E$. Suy ra $u - v, uv \in F(u, v) \subset E$ và nếu $u \neq 0$ ta có $u^{-1} \in F(u, v) \subset E$. Vậy E là trường. \square

Nhận xét 3.6. Trường con E các phần tử đại số của \mathbb{R} trên \mathbb{Q} là một mở rộng vô hạn trên \mathbb{Q} . Thật vậy, nếu $[E : \mathbb{Q}] = n$ thì dễ dàng chỉ ra một phần tử đại số thuộc \mathbb{R} có bậc lớn hơn n . Điều này mâu thuẫn với Mệnh đề 3.2.

Định nghĩa. Một trường K được gọi là **đóng đại số** nếu mọi đa thức bậc lớn hơn 0 đều có ít nhất một nghiệm trong K .

Ví dụ 12. Trường các số phức \mathbb{C} là một trường đóng đại số. Đây là một kết quả cổ điển thường được gọi là Định lý cơ bản của đại số. Ta sẽ đưa ra một chứng minh của định lý này trong § 9.

Nhận xét 3.7. Cho K là một trường. Các mệnh đề sau là tương đương :

- (i) K đóng đại số ;
- (ii) mọi đa thức thuộc $K[x]$ có bậc lớn hơn không đều phân tích thành tích các nhân tử bậc nhất ;

(iii) mọi đa thức bất khả quy trong $K[x]$ đều là đa thức bậc nhất ;

(iv) mọi mở rộng đại số của K đều trùng với K .

Định nghĩa.

Cho mở rộng trường $K : F$. Trường K được gọi là **bao đóng đại số** của F nếu K đóng đại số và $K : F$ là mở rộng đại số.

Ví dụ 13. Trường \mathbb{C} là bao đóng đại số của \mathbb{R} nhưng không phải là bao đóng đại số của \mathbb{Q} .

Mệnh đề 3.8. Cho $K : F$ là mở rộng trường, trong đó K đóng đại số. Kí hiệu E là trường con các phần tử đại số của $K : F$. Khi đó E là một bao đóng đại số của F .

Chứng minh. Ta đã biết $F \subset E$ là mở rộng đại số. Cho

$$f = a_0 + a_1x + \cdots + a_nx^n \in E[x]$$

là một đa thức bậc lớn hơn 0. Do K đóng đại số, đa thức f có nghiệm $u \in K$. Rõ ràng $F(a_0, \dots, a_n, u) : F$ là một mở rộng đại số (Mệnh đề 3.1) nên u đại số trên F . Suy ra $u \in E$. Vậy E đóng đại số. \square

Nhận xét 3.9. Mọi trường con của \mathbb{C} đều tồn tại một bao đóng đại số. Sau này ta sẽ chỉ ra rằng mọi trường đều tồn tại một bao đóng đại số, xem (C.1) trong Phụ lục.

Bài tập

✎ **3.1.** Chọn đúng, sai cho các mệnh đề sau :

- a) Mọi mở rộng hữu hạn cùng bậc đều đẳng cấu.
- b) Các mở rộng trên cùng một trường F và F -đẳng cấu với nhau thì có cùng bậc.
- c) Mọi mở rộng đại số đều là mở rộng hữu hạn.
- d) Mọi mở rộng siêu việt đều là mở rộng vô hạn.
- e) Mọi phần tử của \mathbb{C} đều đại số trên \mathbb{R} .
- f) Mọi mở rộng của \mathbb{R} đều là mở rộng hữu hạn.
- g) Mọi mở rộng đại số của \mathbb{Q} đều là mở rộng hữu hạn.
- h) Trường con \mathbb{A} các phần tử đại số của \mathbb{C} trên \mathbb{Q} là trường con lớn nhất của \mathbb{C} sao cho nó là mở rộng đại số của \mathbb{Q} . (Xem HD 264)

✎ **3.2.** Chứng minh rằng mọi mở rộng đại số của \mathbb{R} đều đẳng cấu với \mathbb{R} hoặc với \mathbb{C} .

(Xem HD 265)

👉 **3.3.** Xét mở rộng trường $F \subset F(x)$ với biến x siêu việt trên F . Cho mở rộng $M \subset F(x)$ với M chứa F như một trường con thực sự. Chứng minh rằng $M \subset F(x)$ là một mở rộng đại số. (Xem HD 265)

👉 **3.4.** Xét tính bất khả quy các đa thức sau trên trường được chỉ ra :

a) $x^3 + 4$ trên $\mathbb{Q}(\sqrt{11})$;

b) $x^2 + 1$ trên $\mathbb{Q}(\sqrt{-2})$;

c) $x^5 + 5x^2 - 25x - 5$ trên $\mathbb{Q}(\sqrt{2}, \sqrt{3}, 1 - i)$. (Xem HD 265)

👉 **3.5.** Trong mỗi trường hợp sau, xét xem u có sinh ra mở rộng được chỉ ra của trường \mathbb{Q} hay không ?

a) $u = \sqrt{2} + \sqrt{5}$ trong $\mathbb{Q}(\sqrt{2}, \sqrt{5})$;

b) $u = \frac{2}{3} + \sqrt[3]{3}$ trong $\mathbb{Q}(\sqrt[3]{3})$;

c) $u = \frac{\sqrt{2} - 1}{1 + \sqrt{2}}$ trong $\mathbb{Q}(\sqrt{2})$;

d) $u = v^2 + v + 1$ trong $\mathbb{Q}(v)$, với v là nghiệm của $f = x^3 + 5x - 5$.

(Xem HD 265)

✎ **3.6.** Cho $F \subset K$ là mở rộng đại số và $f \in K[x]$ là một đa thức khác 0. Chứng minh rằng tồn tại $g \in F[x]$ khác 0 sao cho f là ước của g .

(Xem HD 265)

✎ **3.7.** Cho $E : F$ là một mở rộng đại số. Chứng minh rằng E là bao đóng đại số của F nếu mọi đa thức $f \in F[x]$ có bậc lớn hơn 0 đều phân rã trong E .

(Xem HD 266)

* **3.8.** Cho $K : F$ là một mở rộng hữu hạn với F là trường vô hạn. Chứng minh rằng $K : F$ là mở rộng đơn khi và chỉ khi K chỉ có hữu hạn các trường con chứa F .

(Xem HD 266)

§ 4 DỰNG HÌNH BẰNG THƯỚC KẼ VÀ COMPA

Ta sẽ ứng dụng lí thuyết về mở rộng trường để tìm câu trả lời cho 3 bài toán dựng hình xuất hiện thời Hy Lạp cổ đại và xét bài toán dựng đa giác đều n -cạnh bằng thước kẻ và compa.

4.1 BA BÀI TOÁN DỰNG HÌNH CỔ ĐIỂN

Ba bài toán dựng hình cổ điển là: dùng thước kẻ và compa để

- “chia 3 một góc” cho trước ;
- “gấp đôi một hình lập phương”, tức là dựng một hình lập phương có thể tích gấp đôi thể tích một hình lập phương cho trước ;
- “cầu phương đường tròn”, tức là dựng một hình vuông có diện tích bằng diện tích của một hình tròn cho trước.

Ta xây dựng các khái niệm cơ bản về điểm và số dựng được.

Trong mặt phẳng \mathbb{R}^2 , cho 2 điểm $P_0 = (0, 0)$, $P_1 = (1, 0)$. Một điểm $P \in \mathbb{R}^2$ được gọi là dựng được (bằng thước kẻ và compa) nếu tồn tại dãy hữu hạn P_0, P_1, \dots, P_n sao cho $P = P_n$ và với mọi $j \geq 2$, điểm P_j xác định từ $S_{j-1} := \{P_0, P_1, \dots, P_{j-1}\}$ bởi một trong 3 “phép dựng” sau :

Định nghĩa.

- giao của 2 đường thẳng phân biệt, trong đó mỗi đường thẳng đi qua 2 điểm bất kỳ của S_{j-1} ;
- giao của một đường thẳng qua 2 điểm của S_{j-1} và một đường tròn có tâm tại một điểm của S_{j-1} và có bán kính bằng khoảng cách giữa 2 điểm trong S_{j-1} ;
- giao của 2 đường tròn phân biệt, trong đó mỗi đường tròn có tâm tại một điểm của S_{j-1} và có bán kính bằng khoảng cách giữa 2 điểm trong S_{j-1} .

Định nghĩa.

Một đường thẳng gọi là dựng được nếu nó đi qua 2 điểm dựng được. Một đoạn thẳng gọi là dựng được nếu 2 điểm mút dựng được. Một đường tròn gọi là dựng được nếu có tâm là một điểm dựng được và có bán kính bằng khoảng cách giữa 2 điểm dựng được.

Định nghĩa.

Một số thực x được gọi là dựng được (bằng thước kẻ và compa) nếu điểm $(x, 0) \in \mathbb{R}^2$ dựng được. Rõ ràng, độ dài của một đoạn thẳng dựng được là một số thực dựng được.

Định nghĩa.

Một góc β gọi là dựng được nếu $\cos \beta$ (tương đương $\sin \beta$) là số thực dựng được.

Định lí 4.1. Cho $P = (\alpha, \beta) \in \mathbb{R}^2$ là một điểm dựng được. Khi đó $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^r$ với $r \in \mathbb{N}$.

Chứng minh. Cho $P_0, P_1, \dots, P_n = P$ là một dãy hữu hạn như trong định nghĩa của điểm dựng được. Đặt $K_0 = K_1 = \mathbb{Q}$ và $K_j = K_{j-1}(\alpha_j, \beta_j)$ với $2 \leq j \leq n$ và $P_j = (\alpha_j, \beta_j)$. Dễ dàng thấy rằng các số thực α_j, β_j là nghiệm của một đa thức

bậc 1 hoặc bậc 2 có hệ tử trong K_{j-1} . Do đó $[K_j : K_{j-1}] = 2^t$ với $t \in \mathbb{N}$. Suy ra

$$[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(\alpha, \beta)][\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^m$$

với $m \in \mathbb{N}$. Do đó $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^r$ với $r \in \mathbb{N}$. □

Hệ quả 4.2. *Không thể chia ba góc $\pi/3$ bằng thước kẻ và compa.*

Chứng minh. Điểm $(-1/2, \sqrt{3}/2) = (\cos(\pi/3), \sin(\pi/3))$ là dựng được. Đặt $u = \cos(\pi/9), v = \sin(\pi/9)$. Chia ba góc $\pi/3$ tương đương với việc điểm (u, v) dựng được. Ta có

$$\cos(\pi/3) = \cos(3\pi/9) = 4\cos^3(\pi/9) - 3\cos(\pi/9).$$

Hay $1/2 = 4u^3 - 3u$. Suy ra $8u^3 - 6u - 1 = 0$. Đa thức $8x^3 - 6x - 1$ bất khả quy trên \mathbb{Q} nên $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. Từ Định lý 4.1, suy ra (u, v) không dựng được. Nói cách khác không thể chia ba góc $\pi/3$ bằng thước kẻ và compa. □

Dùng phương pháp tương tự, ta có các kết quả sau đây :

Hệ quả 4.3. *Không thể dựng được điểm $(\sqrt[3]{2}, 0)$. Nói cách khác không thể gấp đôi hình lập phương có cạnh bằng 1.*

Chứng minh. Xem Bài tập 4.4. □

Hệ quả 4.4. Không thể dựng được điểm $(\sqrt{\pi}, 0)$. Nói cách khác không thể dựng được hình vuông có diện tích bằng diện tích hình tròn bán kính 1.

Chứng minh. Xem Bài tập 4.5. □

4.2 ĐIỀU KIỆN CẦN ĐỂ ĐA GIÁC ĐỀU P CẠNH DỰNG ĐƯỢC BẰNG THƯỚC KẼ VÀ COMPA

Ta nhắc lại các kết quả sơ cấp quen thuộc trong dựng hình.

Bổ đề 4.5.

- (i) Trung điểm của đoạn thẳng dựng được là dựng được.
- (ii) Nếu 3 đỉnh của một hình bình hành dựng được thì đỉnh còn lại dựng được (tương đương với phép dựng đường thẳng song song với một đường thẳng cho trước qua một điểm cho trước).

Chứng minh. Xem Bài tập 4.6 □

Bổ đề 4.6. Nếu $(a, 0)$ là điểm dựng được thì $(0, a)$ và $(-a, 0)$ là điểm dựng được.

Chứng minh. Trước tiên ta dựng trục tung. Điểm $(-1, 0)$ dựng được vì nó là giao của trục hoành với đường tròn tâm $(0, 0)$ và đi qua $(1, 0)$. Trục tung là đường thẳng đi qua giao điểm của 2 đường tròn lần lượt có tâm $(1, 0)$ và $(-1, 0)$ bán kính bằng 2.

Điểm $(0, a)$ dựng được vì nó là một trong 2 giao điểm của trục tung với đường tròn tâm $(0, 0)$ đi qua $(a, 0)$. Ngoài ra đường tròn này cắt trục hoành tại điểm $(-a, 0)$ nên điểm $(-a, 0)$ dựng được. \square

Mệnh đề 4.7. Điểm (a, b) dựng được khi và chỉ khi a và b dựng được.

Chứng minh. Nếu a và b dựng được, tức là các điểm $(a, 0)$ và $(0, b)$ dựng được. Suy ra điểm $(0, b)$ dựng được. Điểm (a, b) dựng được vì nó là điểm thứ tư của hình bình hành có 3 điểm $(0, 0)$, $(a, 0)$ và $(0, b)$ dựng được.

Ngược lại, nếu (a, b) là điểm dựng được. Xét 2 đường tròn tâm $(0, 0)$ và $(1, 0)$ đi qua (a, b) . Giao điểm của chúng là (a, b) và $(a, -b)$. Đường thẳng đi qua 2 điểm này cắt trục hoành tại $(a, 0)$ nên $(a, 0)$ dựng được. Điểm $(0, b)$ dựng được vì nó

là điểm thứ tư của hình bình hành có 3 điểm $(0, 0)$, $(a, 0)$ và (a, b) dựng được. Đến lượt điểm $(b, 0)$ dựng được vì nó là một trong các giao điểm của trục hoành và đường tròn tâm $(0, 0)$ đi qua $(b, 0)$. \square

Định lí 4.8. *Tập tất cả các số dựng được là một trường con của \mathbb{R} . Hơn nữa, nếu c dựng được và $c > 0$ thì \sqrt{c} dựng được.*

Chứng minh. Gọi E là tập tất cả các số dựng được. Cho $a, b \in E$. Ta đã chứng minh $-a \in E$. Do $(a, 0)$ và $(b, 0)$ dựng được, điểm giữa $Q = (\frac{a+b}{2}, 0)$ dựng được. Giao điểm của trục hoành và đường tròn tâm Q qua $(0, 0)$ là $(a + b, 0)$. Do đó $a + b$ dựng được.

Để chứng minh $ab \in E$, ta chỉ cần xét trường hợp $ab \neq 0$ và $b \neq 1$. Do $(b - 1)$ dựng được nên điểm $(0, b - 1)$ dựng được. Theo Bổ đề 4.5, điểm $(a, b - 1)$ dựng được. Giao điểm của đường thẳng qua $(0, b)$ và $(a, b - 1)$ với trục hoành là điểm $(ab, 0)$. Vậy ab dựng được.

Ta chứng minh rằng $a^{-1} \in E$ nếu $a \neq 0$. Do $a \in E$, ta có $1 - a \in E$, hay điểm $(0, 1 - a)$ dựng được. Theo Bổ đề 4.5, điểm $(1, 1 - a)$ dựng được. Đường thẳng qua $(0, 1)$ và $(1, 1 - a)$ cắt trục hoành tại $(a^{-1}, 0)$. Vậy $a^{-1} \in E$.

Cho $c \in E$ và $c > 0$. Do $\frac{1}{2}(1 - c)$ dựng được, điểm $Q = (0, \frac{1-c}{2})$ dựng được. Đường tròn tâm Q qua điểm $(0, 1)$ cắt trục hoành tại 2 điểm có tọa độ $(u, 0)$ và $(-u, 0)$ với $u > 0$. Theo Định lí Pythagore, ta có $u^2 + \frac{1}{4}(1 - c)^2 = \frac{1}{4}(1 + c)^2$. Suy ra $u^2 = c$, do đó $u = \sqrt{c}$. Vậy \sqrt{c} dựng được. \square

Ta xét bài toán dựng đa giác đều n cạnh. Rõ ràng đa giác đều n cạnh dựng được nghĩa là điểm $(\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n}))$ dựng được. Điều đó tương đương với $\cos(\frac{2\pi}{n})$ là một số dựng được. Trong phần này ta chỉ đưa ra điều kiện cần của bài toán cho trường hợp $n = p$ nguyên tố. Kết quả đầy đủ sẽ được xét trong phần sau (xem § 9).

Ta biết rằng với p nguyên tố, đa thức $x^{p-1} + \dots + x + 1$ bất khả quy trên \mathbb{Q} . Do đó nó là đa thức tối tiểu của $e^{2\pi i/p} = \cos(\frac{2\pi}{p}) + i \sin(\frac{2\pi}{p})$. Xét các mở rộng trường $\mathbb{Q} \subset \mathbb{Q}(\cos(\frac{2\pi}{p})) \subset \mathbb{Q}(e^{2\pi i/p})$. Ta có

$$[\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}(\cos(2\pi/p))].[\mathbb{Q}(\cos(2\pi/p)) : \mathbb{Q}] = [\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}] = p - 1.$$

Do $\cos(\frac{2\pi}{p}) = \frac{1}{2}(e^{2\pi i/p} + e^{-2\pi i/p})$, ta có

$$2 \cos(2\pi/p) e^{2\pi i/p} = (e^{2\pi i/p})^2 + 1.$$

Nghĩa là bậc của $e^{2\pi i/p}$ trên $\mathbb{Q}(\cos(\frac{2\pi}{p}))$ bằng 2. Do đó

$$[\mathbb{Q}(e^{\frac{2\pi i}{p}}) : \mathbb{Q}(\cos(2\pi/p))] = 2.$$

Suy ra $[\mathbb{Q}(\cos(\frac{2\pi}{p})) : \mathbb{Q}] = \frac{p-1}{2}$. Do $\cos(\frac{2\pi}{p})$ dựng được, ta có $p = 2^t + 1$. Hơn thế, nếu t có một ước lẻ $r > 1$ thì

$$p = 2^t + 1 = 2^{rt_1} + 1 = (2^{t_1} + 1)(2^{t_1(r-1)} - 2^{t_1(r-2)} + \dots + 1).$$

Do đó t có dạng 2^m . Vậy $p = 2^{2^m} + 1$ với $m \in \mathbb{N}$. Số nguyên tố có dạng này gọi là số nguyên tố Fermat¹.

Như thế ta đã chứng minh kết quả sau:

Mệnh đề 4.9. Nếu đa giác đều p cạnh (p nguyên tố) dựng được thì p là số nguyên tố Fermat.

Nhận xét 4.10. Năm 19 tuổi, Gauss (1777-1855) chứng minh rằng đa giác đều 17

¹Năm 1640, Fermat (1601-1665) cho rằng tất cả những số có dạng $F_m := 2^{2^m} + 1$ với $m \in \mathbb{N}$ đều nguyên tố. Tuy nhiên hơn 100 năm sau, Euler (1707-1783) chỉ ra rằng $F_5 = 2^{32} + 1 = 641.6700417$. Có thể dễ dàng kiểm tra kết quả đó với Maple. Thực ra tất cả những số F_m với $5 \leq m \leq 16$ đều là hợp số. Các số F_{20}, F_{22}, F_{24} cũng là các hợp số (F_{24} là hợp số được chứng minh bởi Crandall năm 1999). Cho đến nay, chúng ta vẫn chưa biết những số nguyên tố Fermat nào ứng với $m > 4$.

chính dựng được bằng cách chỉ ra công thức:

$$\cos\left(\frac{2\pi}{17}\right) = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

Bài tập

👉 4.1. Chọn đúng, sai cho các mệnh đề sau :

- Số π không thể dựng được bằng thước kẻ và compa;
- Góc π không thể chia 3 bằng thước kẻ và compa;
- Không thể gấp 3 một hình lập phương bằng thước kẻ và compa.
- Nếu điểm $(0, \alpha) \in \mathbb{R}^2$ không thể dựng được bằng thước kẻ và compa thì α siêu việt trên \mathbb{Q} .
- Tọa độ của một điểm dựng được nằm trong trường con của \mathbb{R} và có bậc trên \mathbb{Q} là một lũy thừa của 2.

- f) Một đoạn thẳng độ dài π không thể dựng được bằng thước kẻ và compa.
- g) Nếu đa giác đều n cạnh dựng được bằng thước kẻ và compa thì n là số nguyên tố.
- h) Nếu đa giác đều p (nguyên tố) cạnh dựng được bằng thước kẻ và compa thì p là số nguyên tố Fermat.
- i) Đa giác đều 65537 cạnh dựng được bằng thước kẻ và compa.
(Xem HD 267)

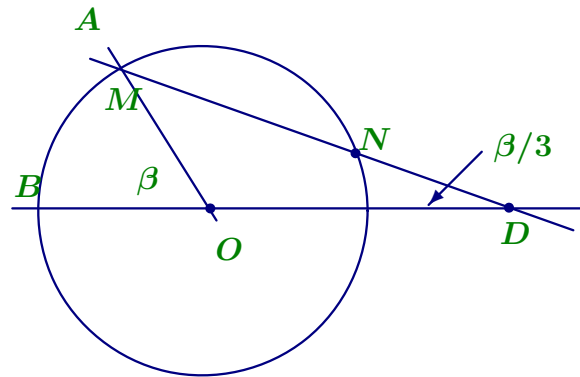
👉 4.2. Chứng tỏ rằng trong chứng minh Định lý 4.1, ta có $[K_j : K_{j-1}] \leq 2$. Suy ra nếu (α, β) là điểm dựng được thì $\alpha, \beta \in \mathbb{Q}(\sqrt{\gamma_1}, \dots, \sqrt{\gamma_{n-1}})$ với $\gamma_j \in \mathbb{Q}(\sqrt{\gamma_1}, \dots, \sqrt{\gamma_{j-1}}), \forall j = 1, \dots, n-1$.
(Xem HD 267)

👉 4.3. Dùng Định lý 4.8 để chứng minh chiều ngược lại của phát biểu trên: nếu $\alpha, \beta \in \mathbb{Q}(\sqrt{\gamma_1}, \dots, \sqrt{\gamma_{n-1}})$ trong đó $\gamma_j \in \mathbb{Q}(\sqrt{\gamma_1}, \dots, \sqrt{\gamma_{j-1}})$, với mọi $1 \leq j \leq n-1$ thì (α, β) là điểm dựng được.
(Xem HD 269)

👉 4.4. Chứng minh Bổ đề 4.3.
(Xem HD 269)

- ✎ 4.5. Chứng minh Bổ đề 4.4. (Xem HD 269)
- ✎ 4.6. Chứng minh Bổ đề 4.5. (Xem HD 269)
- ✎ 4.7. Chứng minh rằng trường các số dựng được là một mở rộng đại số trên \mathbb{Q} nhưng không phải là mở rộng hữu hạn. (Xem HD 269)
- ✎ 4.8. Chứng minh rằng đa giác đều năm cạnh dựng được bằng thước kẻ và compa. (Xem HD 270)
- ✎ 4.9. Chứng minh rằng có thể chia 3 góc $\frac{2\pi}{5}$ bằng thước kẻ và compa. (Xem HD 270)
- ✎ 4.10. Chứng minh rằng không thể dựng đa giác đều 18 cạnh bằng thước kẻ và compa.
- ✎ 4.11. Chứng minh rằng không thể dựng đa giác đều 9 cạnh bằng thước kẻ và compa.
- ✎ 4.12. Cho β là một góc dựng được. Chứng minh rằng góc β có thể chia 3 bằng thước kẻ và compa khi và chỉ khi đa thức $4x^3 - 3x - \cos \beta$ khả quy trên trường $\mathbb{Q}(\cos \beta)$. (Xem HD 270)

✎ **4.13.** Chứng minh rằng ta có thể chia 3 một góc cho trước bằng compa và một thước đánh dấu như sau (xem Hình 1).



Hình 1: Chia 3 một góc bằng compa và thước đánh dấu

Giả sử trên thước, ta đánh dấu 2 điểm N, D có độ dài bằng r .

- Dựng góc \widehat{AOB} bằng β .
- Dựng đường tròn tâm O bán kính bằng r , cắt OA tại M .

- Đặt thước kẻ đi qua M , sao cho 1 điểm đánh dấu D nằm trên BO , điểm đánh dấu còn lại N nằm trên đường tròn. Góc \widehat{ODN} chính là góc cần dựng.
(Xem HD 271)

§ 5 TRƯỜNG PHÂN RÃ CỦA MỘT ĐA THỨC. ĐA THỨC TÁCH ĐƯỢC

5.1 TRƯỜNG PHÂN RÃ CỦA MỘT ĐA THỨC

Định nghĩa.

Cho $f \in F[x]$ và K là một mở rộng trường của F . Ta nói f phân rã trong K hay K phân rã f nếu f có thể viết được dưới dạng $f = a(x - u_1) \cdots (x - u_n)$ với $a, u_i \in K$, $\forall i = 1, \dots, n$.

Ví dụ 14. Nếu K là một bao đóng đại số của F thì K phân rã mọi đa thức của $F[x]$.

Ví dụ 15. Cho $f = x^3 - 2 \in \mathbb{Q}[x]$. Ba nghiệm của f trong \mathbb{C} là $\sqrt[3]{2}, \xi \sqrt[3]{2}$ và $\xi^2 \sqrt[3]{2}$ với $\xi = e^{\frac{2\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ (chú ý rằng $\xi^3 = 1$). Rõ ràng tất cả các trường con của \mathbb{C} chứa 3 nghiệm của f đều phân rã f . Đặc biệt $\mathbb{Q}(\sqrt[3]{2}, \xi \sqrt[3]{2}, \xi^2 \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \xi)$ là trường nhỏ nhất phân rã f . Ta có định nghĩa :

Định nghĩa.

Cho $0 \neq f \in F[x]$. Một mở rộng trường K của F được gọi là trường phân rã (hay trường nghiệm) của f trên F nếu K phân rã f và f không phân rã trong bất kỳ trường con thực sự nào của K .

Nhận xét 5.1.

- (i) Cho $f = a(x - u_1) \cdots (x - u_n)$ với $a, u_i \in K$. Khi đó K là trường phân rã của f nếu $K = F(u_1, \dots, u_n)$.
- (ii) Trường phân rã E_f của đa thức f trên F là một mở rộng hữu hạn của F . Nói riêng, mọi phần tử của E_f đều đại số trên F .

Ví dụ 16. Ta xây dựng trường phân rã của $f = x^2 + x + 1$ trên \mathbb{Z}_2 . Trong trường hợp này ta không thể dùng nghiệm trong \mathbb{C} như trong Ví dụ 15. Rõ ràng f bất khả quy trên \mathbb{Z}_2 . Gọi $\mathbb{Z}_2(\alpha)$ là mở rộng đơn sao cho α là một nghiệm của f . Khi đó $\mathbb{Z}_2(\alpha)$ có 4 phần tử $0, 1, \alpha$ và $1 + \alpha$. Ta có $\alpha^2 + \alpha + 1 = 0$. Rõ ràng $(1 + \alpha)^2 + (1 + \alpha) + 1 = 0$, nên f có 2 nghiệm trong $\mathbb{Z}_2(\alpha)$, do đó f phân rã trong $\mathbb{Z}_2(\alpha)$. Suy ra $\mathbb{Z}_2(\alpha)$ là trường phân rã của f trên \mathbb{Z}_2 .

Ví dụ 17. Nhiều đa thức khác nhau có thể có cùng một trường phân rã. Cho $f = (x^2 - 3)(x^3 + 1) \in \mathbb{Q}[x]$. Tập nghiệm của f trong \mathbb{C} là $\{-1, \pm\sqrt{3}, \xi, \xi^2\}$, với $\xi = (1 + \sqrt{3}i)/2$. Do đó một trường phân rã của f trên \mathbb{Q} là $\mathbb{Q}(\sqrt{3}, i)$. Dễ dàng thấy rằng $\mathbb{Q}(\sqrt{3}, i)$ cũng là trường phân rã của $g = (x^2 - 2x - 2)(x^2 + 1)$ trên \mathbb{Q} .

Mệnh đề 5.2. Cho đa thức $f \in F[x]$ bậc n . Tồn tại một trường phân rã E_f của f trên F sao cho $[E_f : F]$ là ước của $n!$.

Chứng minh. Ta chứng minh bằng quy nạp theo n . Với $n = 1$, kết quả là hiển nhiên. Giả sử kết quả đúng với mọi đa thức có bậc nhỏ hơn n .

Nếu f không bất khả quy, ta viết $f = gh$ với $\deg(g) = m < n$ và $\deg(h) = n - m$. Theo giả thiết quy nạp, ta có $[E_g : F] | m!$, với E_g là trường phân rã của g trên F . Gọi E_h là trường phân rã của h trên E_g và có $[E_h : E_g] | (n - m)!$. Khi đó E_h cũng là trường phân rã của $f = gh$ trên F . Hơn thế $[E_h : F] = [E_g : F][E_h : E_g]$ là ước của $m!(n - m)!$, do đó $[E_h : F]$ là ước của $n!$.

Xét trường hợp f bất khả quy. Gọi α là một nghiệm của f . Đặt $F_1 = F(\alpha)$. Ta viết $f = (x - \alpha)f_1$ với $f_1 \in F_1[x]$. Do $\deg(f_1) = n - 1$ nên theo giả thiết quy nạp, tồn tại trường phân rã E_{f_1} của f_1 trên F_1 và $[E_{f_1} : F_1] | (n - 1)!$. Rõ ràng E_{f_1}

là trường phân rã của f trên F . Hơn nữa,

$$[E_{f_1} : F] = [E_{f_1} : F_1][F_1 : F](n-1)!n = n!.$$

□

Sử dụng Maple 3. Maple cho phép phân tích một đa thức trên một mở rộng hữu hạn của \mathbb{Q} hay \mathbb{Z}_p . Do đó, có thể tìm được trường phân rã của một đa thức trên \mathbb{Q} hay \mathbb{Z}_p .

Ví dụ 18. Cho đa thức $f = x^3 + 3x^2 + 3x + 4 \in \mathbb{Q}[x]$.

```
> f:=x^3+3*x^2+3*x+4;
```

$$f := x^3 + 3x^2 + 3x + 4$$

Ta xác định dạng nhân tử hóa của f trên \mathbb{Q} .

```
> factor(f);
```

$$x^3 + 3x^2 + 3x + 4$$

Như thế f bất khả quy. Gọi α là một nghiệm của f . Phân tích f trong vành $\mathbb{Q}(\alpha)[x]$ như trong chứng minh của mệnh đề trên.

```
> alias(alpha=RootOf(f,x)):
```

> factor(f,alpha);

$$(x - \alpha)(x^2 + 3x + x\alpha + 3 + 3\alpha + \alpha^2)$$

Đó là dạng nhân tử hóa của f trong $\mathbb{Q}(\alpha)[x]$, tiếp tục gọi β là một nghiệm của nhân tử thứ hai trong biểu diễn trên. Sau đó phân tích f trong $\mathbb{Q}(\alpha, \beta)[x]$.

> g:=factor(f/(x-alpha));

$$g := x^2 + 3x + x\alpha + 3 + 3\alpha + \alpha^2$$

> alias(beta=RootOf(g,x));

> factor(f,{alpha,beta});

$$(x - \beta)(x + 3 + \alpha + \beta)(x - \alpha)$$

Ví dụ 19. Xét đa thức $h = x^4 + x^2 + 2 \in \mathbb{Z}_3[x]$.

> h:=x^4+x^2+2;

$$h := x^4 + x^2 + 2$$

Ta xác định dạng nhân tử hóa của h trong $\mathbb{Z}_3[x]$.

> Factor(h) mod 3;

$$x^4 + x^2 + 2$$

Như thế h bất khả quy trên \mathbb{Z}_3 . Gọi γ là một nghiệm của h và tìm dạng nhân tử hóa của h trong $\mathbb{Z}_3(\gamma)[x]$

> `alias(gamma=RootOf(h,x) mod 3):`

> `Factor(h,gamma) mod 3;`

$$(x + 2\gamma)(x + \gamma)(x + \gamma^3)(x + 2\gamma^3)$$

Vậy h phân rã trong $\mathbb{Z}_3(\gamma)$, nên trường phân rã của h trên \mathbb{Z}_3 là $\mathbb{Z}_3(\gamma)$.

Trường phân rã của một đa thức trên một trường là duy nhất, sai khác đẳng cấu, như được thể hiện sau đây.

Mệnh đề 5.3. Cho $\tau : F_1 \longrightarrow F_2$ là một đẳng cấu trường và $f \in F_1[x]$. Gọi K_1 và K_2 tương ứng là trường phân rã của f trên F_1 và của $\tau_*f = \tau(a_n)x^n + \cdots + \tau(a_0) \in F_2[x]$ trên F_2 . Khi đó τ mở rộng thành một đẳng cấu $\varphi : K_1 \longrightarrow K_2$, nghĩa là $\varphi(a) = \tau(a)$, $\forall a \in F_1$.

Chứng minh. Ta chứng minh quy nạp theo bậc của f . Kết quả là hiển nhiên nếu $\deg(f) = 1$. Giả thiết $\deg(f) = n$ và mệnh đề đúng với đa thức có bậc nhỏ hơn n . Gọi $\alpha \in K_1$ là một nghiệm của f và kí hiệu $m \in F_1[x]$ là đa thức tối tiểu của α .

Rõ ràng τ_*m bất khả quy trên $F_2[x]$. Gọi $\beta \in K_2$ là một nghiệm của τ_*m . Đẳng cấu $F_1[x] \longrightarrow F_2[x]$, theo định lí phân tích đồng cấu, mở rộng thành đẳng cấu

$$\psi : F_1(\alpha) = F_1[x]/(m) \longrightarrow F_2[x]/(\tau_*m) = F_2(\beta)$$

thỏa $\psi(a) = \tau(a)$, $\forall a \in F_1$. Gọi $f = (x - \alpha_1)f_1$ với $f_1 \in F_1(\alpha)[x]$ có bậc $n - 1$. Ta có K_1, K_2 lần lượt là trường phân rã của f_1 và τ_*f_1 trên các trường tương ứng $F_1(\alpha)$ và $F_2(\beta)$. Theo giả thiết quy nạp, tồn tại đẳng cấu $\varphi : K_1 \longrightarrow K_2$ thỏa $\varphi(b) = \psi(b)$, $\forall b \in F_1(\alpha)$. Đặc biệt $\varphi(a) = \psi(a) = \tau(a)$, $\forall a \in F_1$. \square

Nhận xét 5.4. Nếu $F_1 = F_2$ và τ là phép đồng nhất thì mệnh đề trên có nghĩa là trường phân rã của một đa thức trên F_1 là duy nhất sai khác bởi F_1 -đẳng cấu.

Hệ quả 5.5. Cho $f \in F[x]$ và K là trường phân rã của f trên F . Cho $\alpha, \beta \in K$. Tồn tại một F -tự đẳng cấu của K biến α thành β khi và chỉ khi α và β có cùng một đa thức tối tiểu trên F .

Chứng minh. Nếu có $\varphi : K \longrightarrow K$ là F -tự đẳng cấu. Gọi $g \in F[x]$ là đa thức tối tiểu của α . Khi đó $\varphi(\alpha) = \beta$ cũng là nghiệm của g nên g cũng chính là đa thức

tối tiểu của β . Ngược lại nếu α và β đều có chung đa thức tối tiểu $g \in F[x]$. Khi đó tồn tại F -đẳng cấu ψ từ $F(\alpha)$ vào $F(\beta)$ thỏa $\psi(\alpha) = \psi(\beta)$. Khi đó K chính là trường phân rã của f trên $F(\alpha)$ và $F(\beta)$. Theo mệnh đề trên, đẳng cấu ψ mở rộng thành F -tự đẳng cấu của K , biến α thành β . \square

5.2 ĐA THỨC TÁCH ĐƯỢC

Bổ đề 5.6. Cho $F \subset K$ là một mở rộng trường và $f, g \in F[x]$. Gọi $d_1 = (f, g)$ trong $F[x]$ và $d_2 = (f, g)$ trong $K[x]$. Khi đó $d_1 \sim d_2$ trong $K[x]$, tức là $d_1 = ad_2$ với $a \in K$. Suy ra nếu f và g nguyên tố cùng nhau trong $F[x]$ thì chúng không có nghiệm chung trong bất cứ một mở rộng trường nào của F .

Chứng minh. Rõ ràng $d_1 | d_2$ trong $K[x]$. Mặt khác, tồn tại $k, h \in F[x]$ sao cho $fh + gk = d_1$. Suy ra $d_2 | d_1$ trong $K[x]$. \square

Định nghĩa.

Cho $f \in F[x]$ và $f = a \prod_{i=1}^n (x - u_i)^{m_i}$ với $u_i \neq u_j, m_i \geq 1$ trong một trường phân rã của f trên F . Do các trường phân rã của f trên F là đẳng cấu, tập các số mũ $\{m_1, \dots, m_n\}$ không phụ thuộc vào trường phân rã. Số mũ m_i được gọi là **số bội** của nghiệm u_i .

Định nghĩa.

Đa thức f gọi là **có nghiệm bội** nếu tồn tại $m_i > 1$. Nghiệm u_i ứng với $m_i > 1$ gọi là **nghiệm bội** của f . Nghiệm ứng với $m_i = 1$ gọi là **nghiệm đơn**.

Ví dụ 20. Cho F là trường có đặc số p và $a \in F$ thỏa điều kiện không có căn bậc p trong F (ví dụ $a = t$ trong trường các phân thức hữu tỉ $\mathbb{Z}_p(t)$). Ta có đa thức $f = x^p - a$ bất khả quy (Bài tập 5.10) trong $F[x]$. Gọi b là một nghiệm của f . Khi đó,

$$x^p - a = x^p - b^p = (x - b)^p$$

trong trường phân rã của f trên F . Như thế một đa thức bất khả quy có thể có nghiệm bội.

Định nghĩa. Cho $f = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$. Đạo hàm hình thức của f , kí hiệu f' , là đa thức định bởi

$$f' = n a_n x^{n-1} + \cdots + a_1 \in F[x].$$

Chú ý rằng từ định nghĩa trên, dễ dàng suy ra các công thức tính đạo hàm của đa thức tổng và tích quen thuộc

$$(f + g)' = f' + g'; \quad (fg)' = f'g + fg'.$$

Bổ đề 5.7. Đa thức f có nghiệm bội khi và chỉ khi $(f, f') \neq 1$.

Chứng minh. Nếu f có nghiệm bội α trong trường phân rã K của nó, thì dễ dàng thấy rằng α cũng là nghiệm của f' . Do đó $(f, f') \neq 1$ (xem 5.6). Ngược lại, nếu $(f, f') \neq 1$ thì f và f' có nghiệm chung α trong trường phân rã của f . Nếu α là nghiệm đơn thì dễ dàng chứng minh rằng α không phải là nghiệm của f' . Vô lí. □

Mệnh đề 5.8. Cho $f \in F[x]$ là một đa thức bất khả quy. Các phát biểu sau là tương đương :

- (i) f có nghiệm bội ;
- (ii) $(f, f') \neq 1$;
- (iii) F có đặc số $p > 0$ và f là một đa thức của x^p ;
- (iv) mọi nghiệm của f đều là nghiệm bội.

Chứng minh. (i) \implies (ii) Xem (5.7).

(ii) \implies (iii) Vì f bất khả quy và $(f, f') \neq 1$ ta có $f' = 0$. Do đó F có đặc số $p > 0$ và f là một đa thức của x^p .

(iii) \implies (iv) Ta có $f(x) = g(x^p)$ với $g(x) \in F[x]$. Đặt

$$g(x) = \prod (x - u_i)^{m_i}, m_i \geq 1.$$

Khi đó

$$f(x) = g(x^p) = \prod (x^p - u_i)^{m_i} = \prod (x - \alpha_i)^{pm_i},$$

với $\alpha_i^p = u_i$. Do $pm_i > 1$ nên tất cả các nghiệm của f đều là nghiệm bội.

(iv) \implies (i) Hiển nhiên. □

Định nghĩa.

Một đa thức $f \in F[x]$ gọi là **tách được** trên F nếu mọi nhân tử bất khả quy của f đều không có nghiệm bội. Một trường F gọi là **hoàn chỉnh** nếu mọi đa thức có hệ tử trong F đều tách được.

Mệnh đề 5.9. Một trường có đặc số 0 là hoàn chỉnh. Một trường có đặc số p là hoàn chỉnh khi và chỉ khi mọi phần tử của F đều có căn bậc p trong F .

Chứng minh. Kết quả hiển nhiên cho trường có đặc số 0 (xem 5.8). Xét trường hợp F có đặc số p . Nếu tồn tại một phần tử $a \in F$ không có căn bậc p trong F . Khi đó đa thức $x^p - a$ không tách được. Ngược lại, giả thiết mọi phần tử của F đều có căn bậc p . Nếu tồn tại một đa thức bất khả quy f không tách được thì

$$f = \sum a_i (x^p)^i = \sum b_i^p (x^p)^i = (\sum b_i x^i)^p.$$

Như vậy f không bất khả quy. Mâu thuẫn này kéo theo F hoàn chỉnh. □

Ví dụ 21. Mọi trường hữu hạn đều là trường hoàn chỉnh. Thật vậy, tự đồng cấu Frobenius:

$$\begin{aligned}\varphi : F &\longrightarrow F \\ a &\longmapsto a^p\end{aligned}$$

là một đẳng cấu vì nó là một đơn cấu. Do đó mọi phần tử của F đều có căn bậc p trong F .

Ví dụ 22. Mọi trường đóng đại số đều hoàn chỉnh.


Bài tập

 **5.1.** Chọn đúng, sai cho các mệnh đề sau :

- a) Mọi đa thức đều phân rã trong một mở rộng nào đó.
- b) Mọi đa thức có hệ tử thuộc một trong các trường \mathbb{Q} , \mathbb{R} , \mathbb{C} đều tách được.
- c) Mọi đa thức có hệ tử thuộc \mathbb{Z}_p đều tách được.
- d) Một đa thức có nghiệm bội thì không tách được.

- e) Mọi đa thức trên trường có đặc số p đều không tách được.
- f) Mọi đa thức bất khả quy đều tách được.
- g) Một đa thức bất khả quy $f \in F[x]$ không tách được thì F có đặc số p .
- h) Một đa thức bất khả quy $f \in F[x]$ không tách được khi và chỉ khi F có đặc số p và f là một đa thức của x^p .
- i) Mọi nghiệm của một đa thức trên một trường cho trước đều có cùng số bội.
- j) Mọi nghiệm của một đa thức bất khả quy trên một trường cho trước đều có cùng số bội.
- k) Đa thức $(x^3 + 5)^2$ tách được trên \mathbb{Z}_7 .
- l) Trường phân rã xác định duy nhất sai khác đẳng cấu.

(Xem HD 271)

 **5.2.** Cho $f \in F[x]$ có $\deg(f) = n > 0$ và $E = F(\alpha_1, \dots, \alpha_r)$ với $\alpha_1, \dots, \alpha_r$ là nghiệm của f với $r \leq n$. Cho K là một trường phân rã f . Chứng minh rằng :

- a) Tồn tại một F -đồng cấu từ E vào K .

b) Số các F -đồng cấu từ E vào K không vượt quá $[E : F]$ và bằng với $[E : F]$ nếu f có n nghiệm phân biệt trong K .

c) Suy ra tính duy nhất của trường phân rã của $f \in F[x]$ trên F .

(Xem HD 271)

👉 **5.3.** Chứng minh rằng nếu một trường viết được như hợp của các trường hoàn chỉnh là một trường hoàn chỉnh. Suy ra mọi mở rộng đại số trên \mathbb{Z}_p là một trường hoàn chỉnh. (Xem HD 272)

👉 **5.4.** Xây dựng trường phân rã của các đa thức

$$x^3 - 1, x^4 + 5x^2 + 6, x^6 - 8, x^5 - 2$$

trên \mathbb{Q} và tính bậc của các mở rộng tương ứng trên \mathbb{Q} .

👉 **5.5.** Xây dựng trường phân rã của các đa thức $x^3 + 2x + 1$ và $x^3 + x^2 + x + 2$ trên \mathbb{Z}_3 . Chúng có đẳng cấu với nhau không? (Xem HD 272)

👉 **5.6.** Cho $F \subset K \subset L$ trong đó L là trường phân rã của $f \in F[x]$ trên F . Chứng minh rằng L cũng là trường phân rã của f trên K .

- 👉 **5.7.** a) Cho F là trường có đặc số p và $a \in F$. Chứng minh rằng nếu đa thức $x^p - x - a$ khả quy trong $F[x]$ thì phân rã trong F .
- b) Với mọi số nguyên tố p , chứng minh rằng đa thức $x^p - x - 1$ bất khả quy trên \mathbb{Q} . (Xem HD 272)
- 👉 **5.8.** Cho F là trường có đặc số 0, cho $f, g \in F[x]$ và $d = (f, g)$. Chứng minh rằng tập nghiệm của f và $h = f/d$ là trùng nhau. (Xem HD 273)
- 👉 **5.9.** Cho F là trường có đặc số p và $f \in F[x]$ bất khả quy. Chứng minh rằng $f = g(x^{p^e})$ với $e \geq 0$ và $g \in F[x]$ là đa thức bất khả quy, tách được. Suy ra, mọi nghiệm của f đều có chung số bội trong trường phân rã của f . (Xem HD 273)
- 👉 **5.10.** Cho F là trường có đặc số p và $a \in F$ không có căn bậc p trong F . Chứng minh rằng $f = x^p - a$ bất khả quy trên F . (Xem HD 274)
- * **5.11.** (Tổng quát của Bài tập 5.2) Cho $\tau : F \longrightarrow K$ là một đồng cấu trường. Cho $E = F(\alpha_1, \dots, \alpha_r)$ với $\alpha_1, \dots, \alpha_r$ là các nghiệm của $f \in F[x]$ có bậc $n \geq r$.

Chứng minh rằng :

$$\#\{\varphi : E \longrightarrow K \mid \varphi \text{ là } F\text{-đồng cấu, } \varphi|_F = \tau\} \leq [E : F]$$

và đẳng thức xảy ra khi K chứa n nghiệm phân biệt của $\tau_* f$.

(Xem HD 274)

Chương 2

LÍ THUYẾT GALOIS



§ 6 TỰ ĐẲNG CẦU VÀ TRƯỜNG TRUNG GIAN CỦA MỞ RỘNG TRƯỜNG

Trong bài này, ta nghiên cứu nhóm $\text{Aut}(E/F)$ các tự đẳng cấu của mở rộng trường $E : F$, đặc biệt với trường hợp của trường phân rã của một đa thức trên F . Đồng thời, ta nghiên cứu tương ứng giữa tập các nhóm con của $\text{Aut}(E/F)$ và tập các trường con của E chứa F , gọi là các trường trung gian của mở rộng $E : F$.

6.1 NHÓM CÁC TỰ ĐẲNG CẤU CỦA MỞ RỘNG TRƯỜNG

Ta bắt đầu bằng một số bổ đề đơn giản sau đây :

Bổ đề 6.1. Cho $E : F$ là một mở rộng trường. Tập tất cả các F -tự đẳng cấu của E là nhóm con của nhóm $\text{Aut}(E)$, gọi là nhóm các F -tự đẳng cấu của $E : F$, kí hiệu $\text{Aut}(E/F)$.

Chứng minh. Tập $\text{Aut}(E/F) \neq \emptyset$ do chứa phép đồng nhất. Tích của hai F -đẳng cấu và nghịch đảo của F -đẳng cấu là F -đẳng cấu. Do đó $\text{Aut}(E/F)$ là nhóm con của $\text{Aut}(E)$. \square

Bổ đề 6.2. Cho $E : F$ là một mở rộng trường và $u \in E$ đại số trên F . Gọi $m \in F[x]$ là đa thức tối thiểu của u . Cho $\varphi : E \rightarrow E$ là một F -đồng cấu. Khi đó $\varphi(u)$ cũng là nghiệm của m .

Chứng minh. Đây chỉ là trường hợp đặc biệt của Mệnh đề 1.3. \square

Bổ đề 6.3. Cho $f \in F[x]$ có $\deg(f) = n > 0$ và $E = F(\alpha_1, \dots, \alpha_r)$ với $\alpha_1, \dots, \alpha_r$ là các nghiệm của f . Cho K là một trường phân rã f . Khi đó tồn tại một F -đồng

cầu từ E vào K ; số các F -đồng cấu từ E vào K không vượt quá $[E : F]$ và bằng với $[E : F]$ nếu f có n nghiệm phân biệt trong K .

Chứng minh. Xem Bài tập 5.2. □

Ta mở rộng kết quả trên bằng bổ đề sau đây.

Bổ đề 6.4. Cho $\tau : F \longrightarrow K$ là một đồng cấu trường. Cho $E = F(\alpha_1, \dots, \alpha_r)$ với $\alpha_1, \dots, \alpha_r$ là các nghiệm của $f \in F[x]$ có bậc $n \geq r$. Khi đó

$$\#\{\varphi : E \longrightarrow K \mid \varphi \text{ là } F\text{-đồng cấu}, \varphi|_F = \tau\} \leq [E : F]$$

và đẳng thức xảy ra khi K chứa n nghiệm phân biệt của $\tau_* f$.

Chứng minh. Xem Bài tập 5.11. □

Ví dụ 23. Cho $G = \text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. Nếu $\varphi \in G$ thì $\varphi(\sqrt{2}) = \sqrt{2}$ hay $\varphi(\sqrt{2}) = -\sqrt{2}$. Trường hợp thứ nhất kéo theo $\varphi(a + b\sqrt{2}) = a + b\sqrt{2}$ hay $\varphi = id$. Trường hợp thứ 2 tồn tại do $\pm\sqrt{2}$ đều có cùng một đa thức tối thiểu và các mở rộng đơn của chúng trên \mathbb{Q} chính là $\mathbb{Q}(\sqrt{2})$.

Ví dụ 24. Cho $G = \text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$. Đa thức tối tiểu của $\sqrt[3]{2}$ là $f = x^3 - 2$. Các nghiệm còn lại của f là $\xi\sqrt[3]{2}$ và $\xi^2\sqrt[3]{2}$, với $\xi = e^{\frac{2\pi i}{3}}$, đều không thuộc $\mathbb{Q}(\sqrt[3]{2})$. Do đó $G = 1$.

Nhận xét 6.5.

- (i) Cho $E = F(u_1, \dots, u_r)$ với u_i đại số trên F . Khi đó mỗi F -tự đồng cấu φ biến u_i thành một nghiệm của đa thức tối tiểu của u_i . Đặc biệt, $\text{Aut}(E/F)$ là một nhóm hữu hạn. Hơn thế, một F -tự đồng cấu φ hoàn toàn xác định khi biết tập ảnh của u_1, \dots, u_r .
- (ii) Đặc biệt, khi E là trường phân rã của một đa thức $f \in F[x]$ có $\deg(f) = n$ thì mỗi F -tự đồng cấu φ sẽ cảm sinh một hoán vị của các nghiệm của f . Do đó $\text{Aut}(E/F)$ là một nhóm con của nhóm đối xứng S_n .

Mệnh đề 6.6. Cho E_f là trường phân rã của $f \in F[x]$. Khi đó

$$(\text{Aut}(E_f/F) : 1) \leq [E_f : F].$$

Dấu “=” xảy ra khi f tách được.

Chú ý, ta kí hiệu $(G : 1)$ hay $|G|$ cho cấp của một nhóm nhân hữu hạn G .

Chứng minh. Chú ý rằng mỗi F -tự đồng cấu φ của E_f cũng là F -tự đẳng cấu vì φ hoán vị các nghiệm của f trong K nên φ biến cơ sở của $E_f : F$ thành cơ sở. Mặt khác, nếu $f = f_1^{m_1} \cdots f_r^{m_r}$ là dạng nhân tử hóa của f thì trường phân rã của f trên F cũng chính là trường phân rã của $g := f_1 \cdots f_r$ trên F . Do đó, từ Bổ đề 6.3, ta có $(\text{Aut}(E_f/F) : 1) \leq [E_f : F]$ và dấu “=” xảy ra khi f tách được. \square

Mệnh đề 6.7. Cho $E : F$ và $L : F$ là các mở rộng trường với E hữu hạn trên F . Khi đó

(i) Số F -đồng cấu từ E vào L không vượt quá $[E : F]$. Đặc biệt

$$(\text{Aut}(E/F) : 1) \leq [E : F].$$

(ii) Tồn tại một mở rộng hữu hạn K trên L và một F -đồng cấu từ E vào K .

Chứng minh. Gọi $E = F(u_1, \dots, u_n)$ với u_1, \dots, u_n đại số trên F . Gọi $m_1, \dots, m_n \in F[x]$ tương ứng là các đa thức tối tiểu của u_1, \dots, u_n . Đặt $f = m_1 \cdots m_n$ và gọi K là trường phân rã của f trên L . Theo Bổ đề 6.3, tồn tại một F -đồng cấu từ E vào K và số F -đồng cấu từ E vào K không quá $[E : F]$. Đặc biệt, số các F -đồng cấu từ E vào $L \subset K$ không quá $[E : F]$. \square

6.2 TRƯỜNG TRUNG GIAN CỦA MỞ RỘNG TRƯỜNG

Định nghĩa. Cho $E : F$ là mở rộng trường. Các trường con của E chứa F gọi là các trường trung gian của mở rộng $E : F$. Kí hiệu \mathcal{F} là tập tất cả các trường trung gian của $E : F$.

Bổ đề 6.8. Cho $\emptyset \neq H \subset \text{Aut}(E/F)$. Tập

$$\mathcal{T}(H) = \{b \in E \mid \varphi(b) = b, \forall \varphi \in H\}$$

là một trường trung gian của $E : F$, gọi là trường trung gian cố định bởi H .

Chứng minh. Rõ ràng $F \subset \mathcal{T}(H)$. Nếu $a, b \in \mathcal{T}(H)$ và $\forall \varphi \in H$, ta có $\varphi(a + b) = a + b$, $\varphi(ab) = ab$. Mặt khác, nếu $0 \neq a \in \mathcal{T}(H)$ thì $\varphi(a^{-1}) = a^{-1}$. Do đó $\mathcal{T}(H)$ là một trường trung gian của $E : F$. \square

Bổ đề 6.9. Cho K là trường trung gian của mở rộng $E : F$. Khi đó $\text{Aut}(E/K)$ là một nhóm con của $\text{Aut}(E/F)$, gọi là nhóm con cố định K , kí hiệu $\mathcal{N}(K)$.

Chứng minh. Sử dụng Bổ đề 6.1 và $\text{Aut}(E/K) \subset \text{Aut}(E/F)$. \square

Kí hiệu \mathcal{H} là tập tất cả các nhóm con của $\text{Aut}(E/F)$. Hai ánh xạ sau :

$$\begin{array}{ccc} \mathcal{N} : \mathcal{F} & \longrightarrow & \mathcal{H} \\ K & \mapsto & \mathcal{N}(K) \end{array} \quad \text{và} \quad \begin{array}{ccc} \mathcal{T} : \mathcal{H} & \longrightarrow & \mathcal{F} \\ H & \mapsto & \mathcal{T}(H) \end{array}$$

gọi là các **tương ứng Galois** của mở rộng $E : F$.

Nhận xét 6.10. Ta dễ dàng kiểm tra các tính chất sau đây :

- (i) $\mathcal{N}(F) = \text{Aut}(E/F)$, $\mathcal{N}(E) = \{1\}$ và $\mathcal{T}(\{1\}) = E$.
- (ii) Các ánh xạ \mathcal{N} và \mathcal{T} đảo ngược thứ tự bao hàm. Nghĩa là:
 - Nếu $F \subset K_1 \subset K_2 \subset E$ thì $\mathcal{N}(K_1) \supset \mathcal{N}(K_2)$.
 - Nếu $H_1 \subset H_2$ là 2 nhóm con của $\text{Aut}(E/F)$ thì $\mathcal{T}(H_1) \supset \mathcal{T}(H_2)$.
- (iii) $H \subset \mathcal{N}(\mathcal{T}(H))$, $\forall H \in \mathcal{H}$; tương tự $K \subset \mathcal{T}(\mathcal{N}(K))$, $\forall K \in \mathcal{F}$.

Ví dụ 25. Trong mở rộng $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$, ta biết rằng $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$. Suy ra $\mathcal{T}(\mathcal{N}(\mathbb{Q})) = \mathbb{Q}(\sqrt[3]{2})$. Do đó $\mathbb{Q} \subsetneq \mathcal{T}(\mathcal{N}(\mathbb{Q}))$.

Tuy nhiên, ta sẽ thấy rằng $H = \mathcal{N}(\mathcal{T}(H))$, với mọi H hữu hạn.

Định lí 6.11 (Artin). Cho $E : F$ là mở rộng trường và $H \subset \text{Aut}(E/F)$ là một nhóm con hữu hạn. Khi đó :

$$[E : \mathcal{T}(H)] \leq (H : 1).$$

Chứng minh. Gọi $H = \{\varphi_1, \dots, \varphi_m\}$ với $\varphi_1 = 1$. Cho $\alpha_1, \dots, \alpha_n$ với $n > m$ là n phần tử tùy ý của E . Ta chứng minh rằng $\alpha_1, \dots, \alpha_n$ phụ thuộc tuyến tính trên $\mathcal{T}(H)$. Xét hệ phương trình tuyến tính thuần nhất:

$$\begin{cases} \varphi_1(\alpha_1)x_1 + \dots + \varphi_1(\alpha_n)x_n = 0 \\ \vdots \\ \varphi_m(\alpha_1)x_1 + \dots + \varphi_m(\alpha_n)x_n = 0. \end{cases} \quad (2)$$

Do $n > m$, hệ phương trình trên có nghiệm không tầm thường trong E . Gọi $v = (c_1, \dots, c_n)$ là một nghiệm của (2) có số phần tử khác 0 nhỏ nhất. Sau khi hoán vị các c_i nếu cần, ta có thể giả thiết $c_1 \neq 0$. Ta có thể giả thiết $c_1 = 1 \in \mathcal{T}(H)$ bằng cách nhân v với một vô hướng thích hợp. Chú ý rằng do $\varphi_1 = 1$, nên phương trình đầu của (2) cho ta $c_1\alpha_1 + \dots + c_n\alpha_n = 0$. Ta cần chứng minh rằng tất cả thành phần c_j của v thuộc $\mathcal{T}(H)$.

Nếu tồn tại $c_i \notin \mathcal{T}(H)$ thì có $\varphi_k \in H$ sao cho $\varphi_k(c_i) \neq c_i$. Tác động φ_k vào tất cả các phương trình của hệ (2) với chú ý rằng

$$\{\varphi_k \varphi_1, \dots, \varphi_k \varphi_m\} = \{\varphi_1, \dots, \varphi_m\},$$

ta có $v' := (c_1, \varphi_k(c_2), \dots, \varphi_k(c_n))$ cũng là nghiệm của (2). Suy ra

$$v - v' = (0, \dots, c_i - \varphi_k(c_i), \dots, c_n - \varphi_k(c_n))$$

cũng là nghiệm của (2). Rõ ràng nghiệm $v - v'$ không tầm thường do $c_i - \varphi_k(c_i) \neq 0$ và có số phần tử khác 0 ít hơn số phần tử khác 0 của v . Vô lí! Như thế tất cả các c_i thuộc $\mathcal{T}(H)$, ta có điều phải chứng minh. \square

Hệ quả 6.12. Cho $H \subset \text{Aut}(E/F)$ là một nhóm con hữu hạn. Khi đó $[E : \mathcal{T}(H)] = (H : 1)$ và $H = \mathcal{N}(\mathcal{T}(H))$.

Chứng minh. Ta có $[E : \mathcal{T}(H)] \leq (H : 1)$ do định lí Artin. Mặt khác $(\mathcal{N}(\mathcal{T}(H)) : 1) \leq [E : \mathcal{T}(H)]$ do Mệnh đề 6.7. Suy ra

$$[E : \mathcal{T}(H)] \leq (H : 1) \leq (\mathcal{N}(\mathcal{T}(H)) : 1) \leq [E : \mathcal{T}(H)].$$

Do đó $[E : \mathcal{T}(H)] = (H : 1)$ và $H = \mathcal{N}(\mathcal{T}(H))$. \square

Từ kết quả trên, ta suy ra, nếu $E : F$ hữu hạn thì \mathcal{T} là đơn ánh và \mathcal{N} là toàn ánh. Ta sẽ xét một mở rộng trường trong đó các ánh xạ \mathcal{T} và \mathcal{N} đều là song ánh và do đó là nghịch đảo của nhau.

Ví dụ 26. Xét $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, là trường phân rã của đa thức $f = (x^2 - 2)(x^2 - 3)$. Cho $\varphi \in G = \text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ thì ta có $\varphi(\sqrt{2}) = \pm\sqrt{2}$, $\varphi(\sqrt{3}) = \pm\sqrt{3}$. Như thế có 4 trường hợp như sau :

$$\begin{aligned} & \left\{ \begin{array}{l} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{array} \right\}; \quad \left\{ \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{array} \right\}; \\ & \left\{ \begin{array}{l} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{array} \right\}; \quad \left\{ \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{array} \right\}. \end{aligned}$$

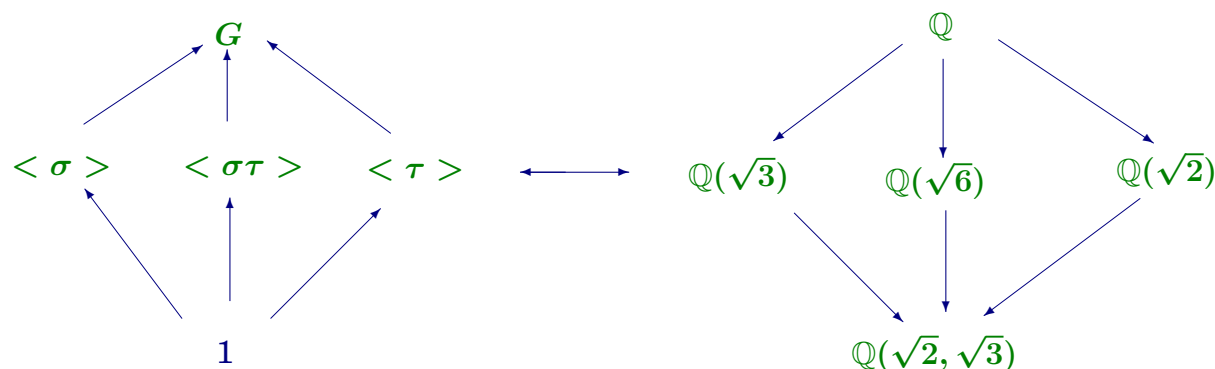
Theo Mệnh đề 6.6, ta có

$$(\text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) : 1) = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4.$$

Như thế 4 phần tử của G tương ứng với 4 trường hợp nêu trên. Đặt

$$\sigma : \left\{ \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{array} \right\}; \quad \tau : \left\{ \begin{array}{l} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{array} \right\}.$$

Ta có $\sigma^2 = \tau^2 = 1$ và $G = \langle \sigma, \tau \rangle$. Suy ra $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (gọi là *nhóm Klein*). Ta liệt kê các nhóm con và trường trung gian tương ứng cùng sơ đồ bao hàm của chúng như trong Hình 7. Ngoài ra, bằng cách chứng minh rằng nếu một trường trung



Hình 7: Tương ứng Galois của mở rộng $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

gian K có bậc 2 trên \mathbb{Q} , thì K là một trong các trường $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$. Do đó các ánh xạ \mathcal{N} và \mathcal{T} là song ánh và là nghịch đảo của nhau.

Bài tập

✎ 6.1. Xác định tính đúng, sai của các mệnh đề sau :

- a) Mọi F -tự đẳng cấu của mở rộng $E : F$ đều là một tự đẳng cấu của E .
- b) Mọi tự đẳng cấu của E đều là F -tự đẳng cấu của mở rộng $E : F$.
- c) Mọi F -tự đẳng cấu của F đều là ánh xạ đồng nhất.
- d) Nhóm $\text{Aut}(E/F)$ luôn là nhóm aben.
- e) Nhóm $\text{Aut}(\mathbb{C}/\mathbb{R})$ là nhóm cyclic.
- f) Các tương ứng Galois luôn là song ánh.
- g) Các tương ứng Galois bảo toàn thứ tự bao hàm.
- h) Nếu $\text{Aut}(E/F) = 1$ thì $E = F$.
- i) Nếu $E = F$ thì $\text{Aut}(E/F) = 1$.
- j) Trường $K(x)$ chỉ có một K -tự đẳng cấu.
- k) Nhóm $\text{Aut}(K(x)/K(x^2))$, với K có đặc số khác 2, đẳng cấu với $\text{Aut}(\mathbb{C}/\mathbb{R})$.

l) $H = \mathcal{N}(\mathcal{T}(H))$ với mọi nhóm con hữu hạn H của $\text{Aut}(E/F)$.

m) Cho mở rộng trường $E : F$ thì $\mathcal{T}(\mathcal{N}(F)) = F$.

n) Cho mở rộng trường $E : F$ thì $\mathcal{T}(\mathcal{N}(E)) = E$. (Xem HD 276)

✎ **6.2.** Vẽ sơ đồ bao hàm các nhóm tự đẳng cấu của các mở rộng trường sau đây và xét xem các tương ứng Galois \mathcal{N} và \mathcal{T} có phải là các song ánh không.

a) $\mathbb{C} : \mathbb{R}$;

b) $\mathbb{Q}(\omega) : \mathbb{Q}$ với $\omega = e^{2\pi i/5}$;

c) $E_f : \mathbb{Q}$ với E_f là trường phân rã của $f = x^4 - 2$;

d) $E_f : \mathbb{Q}(\theta)$ với $\theta = e^{\frac{2\pi i}{3}}$ và E_f là trường phân rã của $f = x^3 - 2$ trên $\mathbb{Q}(\theta)$;

e) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}$;

f) Trường phân rã của đa thức $(x^3 - 5)(x^3 - 7)$ trên \mathbb{Q} ;

g) Trường phân rã của đa thức $(x^6 - 5)$ trên \mathbb{Q} và trên \mathbb{R} . (Xem HD 276)

✎ **6.3.** Cho G là nhóm Galois của đa thức $x^5 - 2$ trên \mathbb{Q} . Xác định cấp của G và xét xem G có phải là nhóm aben hay không? (Xem HD 280)

👉 **6.4.** Xác định cấp của nhóm Galois của đa thức $(x^3 - 5)(x^3 - 2)$ trên \mathbb{Q} và \mathbb{R} .

(Xem HD 281)

👉 **6.5.** Chứng minh rằng $\text{Aut}(\mathbb{Q}(\xi)/\mathbb{Q})$ là nhóm aben với $\xi = e^{\frac{2\pi i}{n}}$ và $n \in \mathbb{N}$.

(Xem HD 281)

👉 **6.6.** Cho $f = x^p - a \in F[x]$ và gọi E_f là trường phân rã của f trên F . Xác định trường phân rã của f trên F trong các trường hợp :

a) $F = \mathbb{Q}$;

b) $F = \mathbb{Z}_p$.

(Xem HD 281)

👉 **6.7.** Chứng minh hoặc bác bỏ các mệnh đề sau đây :

a) Nếu $E : F$ là một mở rộng bậc 2 thì tồn tại $\sigma \in \text{Aut}(E)$ sao cho $\sigma(a) = a, \forall a \in F$.

b) Giống như trên với giả thuyết thêm là trường E hữu hạn.

(Xem HD 281)

👉 **6.8.** Cho K là trường phân rã của $x^5 - 1$ trên \mathbb{Q} . Mô tả nhóm $\text{Aut}(K/\mathbb{Q})$ và chỉ ra rằng $K : \mathbb{Q}$ chỉ có một trường trung gian thực sự là $\mathbb{Q}(\xi + \xi^4)$ với $\xi = e^{2\pi i/5}$.

Xác định đa thức tối thiểu của $\xi + \xi^4$. Xác định các trường phân rã của các đa thức sau trên \mathbb{Q} :

a) $(x^2 - 5)(x^5 - 1)$;

b) $(x^2 + 3)(x^5 - 1)$. (Xem HD 281)

✎ **6.9.** Cho K là trường phân rã của đa thức $x^3 - 5$ trên $\mathbb{Q}(\sqrt{7})$. Chứng minh rằng $\text{Aut}(K/\mathbb{Q}(\sqrt{7})) \cong S_3$. (Xem HD 282)

§ 7 MỞ RỘNG TÁCH ĐƯỢC, CHUẨN TẮC VÀ GALOIS

Trong bài này, ta xét các mở rộng trường đặc biệt hơn nhằm tìm điều kiện để các tương ứng Galois là các song ánh.

7.1 MỞ RỘNG TÁCH ĐƯỢC VÀ ĐỊNH LÝ PHẦN TỬ NGUYÊN THỦY

Định nghĩa. Một mở rộng đại số $E : F$ gọi là **tách được** nếu đa thức tối tiểu của mọi phần tử thuộc E đều tách được.

Như thế, mở rộng $E : F$ là không tách được nếu các trường có đặc số p và đa thức tối tiểu của một phần tử nào đó của E có dạng $g(x^p)$ với $g \in F[x]$.

Ví dụ 27. Mở rộng $\mathbb{Z}_2(t^2) \subset \mathbb{Z}_2(t)$ là không tách được vì đa thức tối tiểu $x^2 - t^2$ của t là không tách được.

Mệnh đề 7.1. Cho $F \subset M \subset E$ là các mở rộng trường. Nếu $F \subset E$ là mở rộng tách được thì $F \subset M$ và $M \subset E$ là các mở rộng tách được.

Chứng minh. Rõ ràng $F \subset M$ là mở rộng tách được. Cho $\alpha \in E$. Gọi $f \in F[x]$

và $g \in M[x]$ tương ứng là các đa thức tối tiểu của α trên F và M . Rõ ràng $g \mid f$. Do $F \subset E$ tách được, đa thức f là tách được. Suy ra g là tách được. \square

Mở rộng tách được có một tính chất rất đặc biệt được thể hiện sau đây.

Định lí 7.2 (Phần tử nguyên thủy). Cho $E = F(\alpha_1, \dots, \alpha_n)$ là một mở rộng hữu hạn của F sao cho $\alpha_2, \dots, \alpha_n$ tách được trên F . Khi đó tồn tại $\gamma \in E$ sao cho $E = F(\gamma)$.

Chứng minh. Nếu F là trường hữu hạn thì E hữu hạn và do đó nhóm nhân E^* các phần tử khác 0 là nhóm cyclic (xem Bài tập 0.18). Gọi u là một phần tử sinh của E^* . Rõ ràng $E = F(u)$.

Ta chỉ cần xét trường hợp F vô hạn. Ta chứng minh quy nạp trên n . Nếu $n = 1$, kết quả là hiển nhiên. Nếu kết quả đúng với $n = 2$ thì từ giả thiết quy nạp, ta có

$$F(\alpha_1, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) = F(t, \alpha_n)$$

và suy ra điều phải chứng minh. Do đó bài toán quy về việc chứng minh kết quả cho $n = 2$.

Xét $E = F(v, w)$ với w tách được trên F . Gọi $f, g \in F[x]$ lần lượt là đa thức tối tiểu của v, w . Gọi K là trường phân rã của fg . Khi đó f có các nghiệm trong K là v, v_1, \dots, v_r ; đa thức g có các nghiệm phân biệt trong K là w, w_1, \dots, w_s . Do F vô hạn, tồn tại $c \in F$ sao cho

$$c \neq \frac{v_i - v}{w - w_j}, \forall i = 1, \dots, r, \forall j = 1, \dots, s.$$

Đặt $u = v + cw$. Ta sẽ chỉ ra rằng $v, w \in F(u)$, do đó $F(v, w) = F(u)$.

Đặt $h = f(u - cx) \in F(u)[x]$. Ta có

$$h(w) = f(u - cw) = f(v) = 0.$$

Nếu có w_j với $1 \leq j \leq s$ nào đó là nghiệm của h thì

$$h(w_j) = f(u - cw_j) = 0.$$

Như thế tồn tại i thỏa $1 \leq i \leq r$ sao cho $u - cw_j = v_i$. Hay $c(w - w_j) = v_i - v$. Vô lý do cách chọn c . Vậy h chỉ có w là nghiệm duy nhất trong tập $\{w, w_1, \dots, w_s\}$. Suy ra $(h, g) = x - w$ trong $K[x]$. Suy ra $x - w \in F(u)[x]$ (xem Bổ đề 5.6), đặc biệt $w \in F(u)$. Ta có điều phải chứng minh. \square

Hệ quả 7.3. Mọi mở rộng hữu hạn, tách được là mở rộng đơn. Đặc biệt mọi mở rộng hữu hạn trên trường có đặc số 0 hoặc trường hữu hạn đều là mở rộng đơn.

7.2 TIÊU CHUẨN CỦA MỞ RỘNG GALOIS VÀ CHUẨN TẮC

Định nghĩa. Một mở rộng đại số $E : F$ gọi là **chuẩn tắc** nếu đa thức tối thiểu của mọi phần tử thuộc E phân rã trong E .

Nhận xét 7.4. Cho $E : F$ là một mở rộng chuẩn tắc và tách được. Cho $f \in F[x]$ là một đa thức bất khả quy bậc m . Nếu f có nghiệm trong E thì f có đúng m nghiệm phân biệt trong E .

Ta đã biết rằng với một mở rộng trường $E : F$ thì nói chung

$$F \subsetneq \mathcal{T}(\mathcal{N}(F)) = \mathcal{T}(\text{Aut}(E/F)).$$

Ta xét những mở rộng trường mà dấu đẳng thức xảy ra.

Định nghĩa. Một mở rộng hữu hạn $E : F$ được gọi là **mở rộng Galois** nếu $F = \mathcal{T}(\mathcal{N}(F))$. Khi đó $\text{Aut}(E/F)$ gọi là **nhóm Galois** của mở rộng trường và được kí hiệu là $\text{Gal}(E/F)$.

Định lí 7.5 (Tiêu chuẩn của mở rộng Galois). Cho mở rộng trường $E : F$. Các mệnh đề sau là tương đương :

- (i) E là trường phân rã của một đa thức tách được trên F ;
- (ii) $[E : F] = (\text{Aut}(E/F) : 1) < \infty$;
- (iii) $E : F$ là mở rộng Galois ;
- (iv) $F = \mathcal{T}(G)$ với G là một nhóm con hữu hạn của $\text{Aut}(E/F)$;
- (v) $E : F$ là mở rộng chuẩn tắc, tách được và hữu hạn trên F .

Chứng minh.

(i) \implies (ii) Xem Mệnh đề 6.6.

(ii) \implies (iii) Theo Định lí Artin, ta có

$$[E : \mathcal{T}(\mathcal{N}(F))] = (\mathcal{N}(F) : 1) = |\text{Aut}(E/F)|.$$

Suy ra $[E : \mathcal{T}(\mathcal{N}(F))] = [E : F]$. Do đó $F = \mathcal{T}(\mathcal{N}(F))$, hay $E : F$ là mở rộng Galois.

(iii) \implies (iv) Lấy $G = \text{Aut}(E/F)$.

(iv) \implies (v) Theo Định lí Artin (6.11), ta có $[E : F] \leq [G : 1]$. Suy ra $E : F$ hữu hạn. Lấy $\alpha \in E$. Gọi $f \in F[x]$ là đa thức tối tiểu của α . Ta chứng minh rằng f phân rã trong E thành các nhân tử phân biệt.

Đặt $N = \{\sigma\alpha \mid \sigma \in G\} = \{\alpha_1, \dots, \alpha_m\}$. Xét đa thức

$$g = \prod_{i=1}^m (x - \alpha_i) = x^m + a_1 x^{m-1} + \dots + a_m \in E[x].$$

Với mọi $\tau \in G$, ánh xạ τ hoán vị các phần tử trong N . Do các hệ tử a_i của g đều là các đa thức đối xứng của $\alpha_1, \dots, \alpha_m$, ta có $\tau(a_i) = a_i, \forall i = 1, \dots, m$. Suy ra $a_i \in F$ hay $g \in F[x]$. Vì f là đa thức tối tiểu của α , ta có $f \mid g$. Mặt khác, các phần tử α_i đều là nghiệm của f nên $g \mid f$. Vậy $g = f$, do đó f phân rã thành các nhân tử phân biệt.

(v) \implies (i) Vì $E : F$ là mở rộng hữu hạn, ta có $E = F(\alpha_1, \dots, \alpha_n)$ với α_i đại số trên F . Gọi m_i là đa thức tối tiểu của α_i với mọi $i = 1, \dots, n$. Do $E : F$ chuẩn tắc, các đa thức m_i phân rã trong E , do đó E là trường phân rã của $f = \prod m_i$

trên F . Hơn thế, do mở rộng $E : F$ là tách được, đa thức f là tách được.

□

Định nghĩa.

Nhóm Galois của một đa thức tách được $f \in F[x]$ là nhóm Galois của trường phân rã của f .

Hệ quả 7.6. Mọi mở rộng hữu hạn, tách được đều chứa trong một mở rộng Galois.

Chứng minh. Cho $F \subset E$ là mở rộng hữu hạn và tách được, ta có $E = F(\alpha_1, \dots, \alpha_n)$ với α_i đại số trên F . Gọi m_i là đa thức tối tiểu của α_i với mọi $i = 1, \dots, n$. Do m_i tách được, đa thức $f = \prod m_i$ là tách được. Trường E chứa trong trường phân rã của $f \in F[x]$.

□

Hệ quả 7.7. Cho $F \subset M \subset E$ là các mở rộng trường. Nếu $F \subset E$ là mở rộng Galois thì $M \subset E$ là mở rộng Galois.

Chứng minh. E là trường phân rã của đa thức $f \in F[x]$. Rõ ràng E cũng là trường phân rã của f trên M . Hơn thế $M \subset E$ là mở rộng tách được (xem Mệnh đề 7.1). Do đó $M \subset E$ là mở rộng Galois.

□

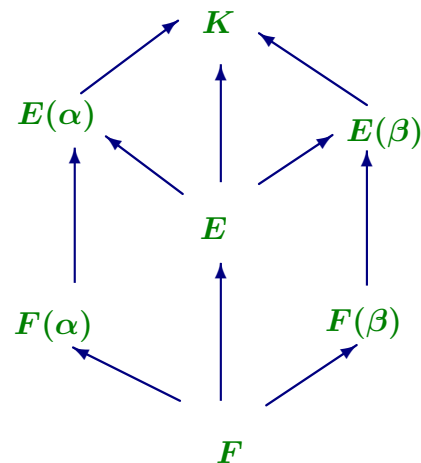
Định lí 7.5 cho ta tiêu chuẩn của một mở rộng Galois. Kết quả sau cho ta tiêu chuẩn của mở rộng chuẩn tắc.

Mệnh đề 7.8. Một mở rộng $E : F$ là hữu hạn và chuẩn tắc khi và chỉ khi E là trường phân rã của một đa thức trên F .

Chứng minh. Điều kiện cần của mệnh đề được chứng minh tương tự như trong Định lí 7.5. Ta chứng minh điều kiện đủ. Cho E là trường phân rã của đa thức $f \in F[x]$ trên F . Gọi $g \in F[x]$ là đa thức tối tiểu của $\alpha \in E$. Ta chứng minh rằng mọi nghiệm của g đều thuộc E .

Gọi K là trường phân rã của g trên E và β là một nghiệm của g trong K . Xét sơ đồ như trong Hình 8.

Ta sẽ chỉ ra rằng $[E(\alpha) : E] = [E(\beta) : E]$ và do $[E(\alpha) : E] = 1$, ta có $[E(\beta) : E] = 1$, nên $\beta \in E$. Do α và β đều là nghiệm của g bất khả quy trên F nên tồn tại F -đẳng cấu $F(\alpha) \longrightarrow F(\beta)$. Rõ ràng $E(\alpha)$ và $E(\beta)$ lần lượt là trường phân rã của f trên $F(\alpha)$ và $F(\beta)$ nên φ mở rộng thành F -đẳng cấu



Hình 8: Sơ đồ chỉ ra $E(\alpha)$ đẳng cấu với $E(\beta)$.

$\varphi' : E(\alpha) \longrightarrow E(\beta)$. Như thế $[E(\alpha) : F] = [E(\beta) : F]$. Suy ra

$$[E(\alpha) : E] = [E(\beta) : E].$$

Ta có điều cần chứng minh. □

Bài tập

✎ 7.1. Chọn đúng, sai cho các mệnh đề sau :

- a) Mọi mở rộng hữu hạn đều là mở rộng chuẩn tắc.
- b) Mọi mở rộng chuẩn tắc đều là mở rộng Galois.
- c) Mọi mở rộng tách được đều là mở rộng hữu hạn.
- d) Mọi mở rộng Galois đều là mở rộng chuẩn tắc và tách được.
- e) Mọi mở rộng tách được đều là mở rộng chuẩn tắc.
- f) Mọi mở rộng chuẩn tắc và hữu hạn đều là mở rộng Galois.
- g) Mọi mở rộng chuẩn tắc đều là trường phân rã của một đa thức.
- h) Mọi mở rộng Galois đều là trường phân rã của một đa thức.
- i) Một mở rộng hữu hạn là Galois khi và chỉ khi nó là trường phân rã của một đa thức tách được.
- j) Mọi mở rộng Galois đều là mở rộng đơn.
- k) Mọi mở rộng hữu hạn đều là mở rộng đơn.

- l) Nếu $F \subset M \subset E$ có $F \subset E$ là mở rộng tách được thì $F \subset M$ và $M \subset E$ tách được.
- m) Nếu $F \subset M \subset E$ có $F \subset E$ là mở rộng chuẩn tắc thì $F \subset M$ và $M \subset E$ chuẩn tắc.
- n) Nếu $F \subset M \subset E$ có $F \subset E$ là mở rộng Galois thì $F \subset M$ và $M \subset E$ Galois. (Xem HD 283)

👉 **7.2.** Cho $F \subset E \subset K$ là các mở rộng trường. Nếu $F \subset E$ và $E \subset K$ là các mở rộng Galois thì $F \subset K$ có phải là mở rộng Galois không?

(Xem HD 283)

👉 **7.3.** Chứng tỏ rằng mọi mở rộng bậc 2 trên trường có đặc số khác 2 đều là các mở rộng Galois. Khẳng định trên có đúng cho trường có đặc số 2 không?

(Xem HD 283)

👉 **7.4.** Cho F là trường có đặc số p và $f = x^p - x - a \in F[x]$. Xác định trường phân rã E_f của f trên F và xét xem nó có phải là mở rộng Galois trên F không? Xác định các phần tử của nhóm $\text{Aut}(E_f/F)$. (Xem HD 283)

👉 **7.5.** Cho $f = x^{p^n} - x \in \mathbb{Z}_p[x]$ và E_f là trường phân rã của f trên \mathbb{Z}_p . Xác định nhóm $\text{Aut}(E_f/\mathbb{Z}_p)$ và vẽ sơ đồ bao hàm của các nhóm con của nó.

(Xem HD 283)

👉 **7.6.** Tìm các mở rộng trường $\mathbb{Q} \subset F_1 \subset F_2 \subset F_3$ với F_1, F_3 Galois trên \mathbb{Q} nhưng F_2 không Galois trên \mathbb{Q} .

(Xem HD 284)

👉 **7.7.** Chứng minh rằng $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{2})$ là mở rộng Galois và xác định nhóm Galois của mở rộng đó.

(Xem HD 284)

👉 **7.8.** Trong các mở rộng ở Bài tập 6.2, mở rộng nào là mở rộng Galois, chuẩn tắc ?

👉 **7.9.** Mô tả nhóm Galois của các đa thức sau trên \mathbb{Q} .

a) $f = (x^2 - 2)(x^2 - 3)(x^2 - 5)$;

b) $g = x^p - 2$ với p nguyên tố ;

c) $h = x^4 - 14x^2 + 9$.

(Xem HD 284)

👉 **7.10.** Chứng minh rằng nhóm Galois của $x^p - 2$ trên \mathbb{Q} đẳng cấu với nhóm nhân các

ma trận $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ với $a, b \in \mathbb{Z}_p$ và $a \neq 0$. (Xem HD 285)

✎ **7.11.** Chứng minh rằng nếu nhóm Galois của một đa thức bậc 3 là một nhóm cyclic cấp 3 thì tất cả các nghiệm của f đều là nghiệm thực. (Xem HD 285)

§ 8 ĐỊNH LÍ CƠ BẢN CỦA LÍ THUYẾT GALOIS

Nhắc lại, với một mở rộng $F \subset E$ cho trước, kí hiệu \mathcal{F} là tập các trường trung gian của mở rộng và \mathcal{H} là tập các nhóm con của $\text{Aut}(E/F)$. Giữa \mathcal{F} và \mathcal{H} có các ánh xạ \mathcal{N} và \mathcal{T} , gọi là các tương ứng Galois.

Định lí 8.1. Cho $F \subset E$ là mở rộng Galois với $G = \text{Gal}(E/F)$. Khi đó các tương ứng Galois $\mathcal{N} : \mathcal{F} \longrightarrow \mathcal{H}$ và $\mathcal{T} : \mathcal{H} \longrightarrow \mathcal{F}$ là các song ánh và là nghịch đảo của nhau. Hơn thế :

$$(i) \ H_1 \subset H_2 \iff \mathcal{T}(H_1) \supset \mathcal{T}(H_2), \forall H_1, H_2 \in \mathcal{H};$$

(ii) chỉ số của nhóm bằng bậc của mở rộng trường, nghĩa là với mọi $H_1, H_2 \in \mathcal{H}$,

$$H_1 \subset H_2 \implies (H_2 : H_1) = [\mathcal{T}(H_1) : \mathcal{T}(H_2)];$$

(iii) $\mathcal{T}(\sigma H \sigma^{-1}) = \sigma \mathcal{T}(H)$ và

$$\mathcal{N}(\sigma M) = \sigma \mathcal{N}(M) \sigma^{-1}, \forall \sigma \in G, \forall H \in \mathcal{H}, \forall M \in \mathcal{F};$$

(iv) $H \triangleleft G$ khi và chỉ khi $\mathcal{T}(H) : F$ là mở rộng chuẩn tắc (do đó Galois) và $\text{Gal}(\mathcal{T}(H)/F) \cong G/H$.

Chứng minh. Do $E : F$ là mở rộng hữu hạn nên G hữu hạn. Khi đó $\forall H \in \mathcal{H}$, ta có $\mathcal{N}(\mathcal{T}(H)) = H$. Mặt khác $\forall M \in \mathcal{F}$, ta có $E : M$ là mở rộng Galois, do đó $\mathcal{T}(\mathcal{N}(M)) = M$. Suy ra \mathcal{N} và \mathcal{T} là các song ánh và là nghịch đảo của nhau.

(i) Ta có

$$\mathcal{T}(H_1) \supset \mathcal{T}(H_2) \implies H_1 = \mathcal{N}(\mathcal{T}(H_1)) \subset \mathcal{N}(\mathcal{T}(H_2)) = H_2.$$

(ii) Với $H \in \mathcal{H}$, ta có $E : \mathcal{T}(H)$ là mở rộng Galois. Do đó

$$[E : \mathcal{T}(H)] = (H : 1).$$

Cho $H_1 \subset H_2$ là các nhóm con của G . Suy ra

$$F \subset \mathcal{T}(H_2) \subset \mathcal{T}(H_1) \subset E.$$

Ta có $(H_2 : 1) = (H_2 : H_1)(H_1 : 1)$. Suy ra

$$\begin{aligned} [E : \mathcal{T}(H_2)] &= (H_2 : H_1)[E : \mathcal{T}(H_1)] \\ &= [E : \mathcal{T}(H_1)][\mathcal{T}(H_1) : \mathcal{T}(H_2)]. \end{aligned}$$

Do đó $(H_2 : H_1) = [\mathcal{T}(H_1) : \mathcal{T}(H_2)]$.

(iii) Cho $y = \sigma x \in \sigma \mathcal{T}(H)$. Với mọi $\sigma \varphi \sigma^{-1} \in \sigma H \sigma^{-1}$, ta có

$$\sigma \varphi \sigma^{-1}(y) = \sigma \varphi(x) = \sigma x = y.$$

Suy ra $y \in \mathcal{T}(\sigma H \sigma^{-1})$. Do đó $\sigma \mathcal{T}(H) \subset \mathcal{T}(\sigma H \sigma^{-1})$.

Ngược lại, cho $y \in \mathcal{T}(\sigma H \sigma^{-1})$. Khi đó, với mọi $\varphi \in H$, ta có $(\sigma \varphi \sigma^{-1})(y) = y$.

Đặt $x = \sigma^{-1}(y)$, ta có

$$(\sigma \varphi \sigma^{-1})(y) = \sigma \varphi(x) = y = \sigma x.$$

Như thế $\varphi(x) = x, \forall \varphi \in H$. Suy ra $x \in \mathcal{T}(H)$, do đó $y = \sigma x \in \sigma \mathcal{T}(H)$.

Vậy $\mathcal{T}(\sigma H \sigma^{-1}) = \sigma \mathcal{T}(H)$.

Ta chứng minh $\sigma \mathcal{N}(M) \sigma^{-1} = \mathcal{N}(\sigma M)$. Với mọi $\sigma \varphi \sigma^{-1} \in \sigma \mathcal{N}(M) \sigma^{-1}$, cho $y = \sigma x \in \sigma M$, ta có

$$\sigma \varphi \sigma^{-1}(y) = \sigma \varphi \sigma^{-1}(\sigma x) = \sigma \varphi(x) = \sigma x = y.$$

Suy ra $\sigma \varphi \sigma^{-1} \in \mathcal{N}(\sigma M)$.

Ngược lại, với mọi $\psi \in \mathcal{N}(\sigma M)$, đặt $\varphi = \sigma^{-1}\psi\sigma$. Ta chứng minh $\varphi \in \mathcal{N}(M)$.
Thật vậy, với mọi $x \in M$, ta có

$$\varphi(x) = \sigma^{-1}\psi\sigma(x) = \sigma^{-1}\psi(\sigma x) = \sigma^{-1}\sigma(x) = x.$$

Do đó $\varphi \in \mathcal{N}(M)$. Vậy $\psi = \sigma\varphi\sigma^{-1} \in \sigma\mathcal{N}(M)\sigma^{-1}$.

(iv) Giả thiết $F \subset \mathcal{T}(H)$ là mở rộng chuẩn tắc. Gọi $\mathcal{T}(H) = F(\alpha_1, \dots, \alpha_m)$.
Với mọi $\sigma \in G$, ta có $\sigma(\alpha_i)$ cũng là nghiệm của đa thức tối tiểu của α_j ,
nên $\sigma(\alpha_i) \in \mathcal{T}(H)$. Do đó $\sigma\mathcal{T}(H) \subset \mathcal{T}(H)$. Do σ là đẳng cấu, ta có
 $\sigma\mathcal{T}(H) = \mathcal{T}(H)$. Suy ra

$$\sigma\mathcal{N}(\mathcal{T}(H))\sigma^{-1} = \mathcal{N}(\sigma\mathcal{T}(H)) = \mathcal{N}(\mathcal{T}(H)) = H.$$

Hay $\sigma H\sigma^{-1} = H$, nghĩa là $H \triangleleft G$.

Ngược lại, giả thiết $H \triangleleft G$. Do $\sigma H\sigma^{-1} = H$, $\forall \sigma \in G$, suy ra

$$\sigma\mathcal{T}(H) = \mathcal{T}(\sigma H\sigma^{-1}) = \mathcal{T}(H).$$

Ta có đồng cấu nhóm :

$$\begin{aligned} g : G &\longrightarrow \text{Aut}(\mathcal{T}(H)/F) \\ \sigma &\longmapsto \sigma|_{\mathcal{T}(H)}. \end{aligned}$$

Ta có

$$\text{Ker}(g) = \{\sigma \in G \mid \sigma|_{\mathcal{T}(H)} = id\} = \mathcal{N}(\mathcal{T}(H)) = H.$$

Đặt $H' = \text{Im}(g) \subset \text{Aut}(\mathcal{T}(H)/F)$. Kí hiệu \mathcal{T}' và \mathcal{N}' là các tương ứng Galois của mở rộng $F \subset \mathcal{T}(H)$. Ta có $\mathcal{T}'(H') = \mathcal{T}(G) = F$ do $g : G \longrightarrow H'$ là toàn cấu. Vì H' hữu hạn, theo tiêu chuẩn của mở rộng Galois, ta có $\mathcal{T}(H) : F$ là mở rộng Galois. Mặt khác, tương ứng Galois ứng với mở rộng Galois $\mathcal{T}(H) : F$ cho ta

$$H' \mapsto F \mapsto \text{Gal}(\mathcal{T}(H)/F) = H'.$$

Như thế, $\text{Gal}(\mathcal{T}(H)/F) \cong G/H$.

□

Ví dụ 28. Xét nhóm Galois của đa thức $f = x^4 - 2 \in \mathbb{Q}[x]$. Các nghiệm của f là $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}$ và $-i\sqrt[4]{2}$. Trường phân rã của f trên \mathbb{Q} là $\mathbb{Q}(i, \sqrt[4]{2})$.

- 1) Dễ dàng kiểm tra $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$.
- 2) Đặt $G = \text{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$. Ta có $(G : 1) = 8$.
- 3) Tồn tại các phần tử σ, τ trong G xác định bởi

$$\sigma : \begin{cases} \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\ i \mapsto i \end{cases} \quad \text{và} \quad \tau : \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto -i \end{cases}.$$

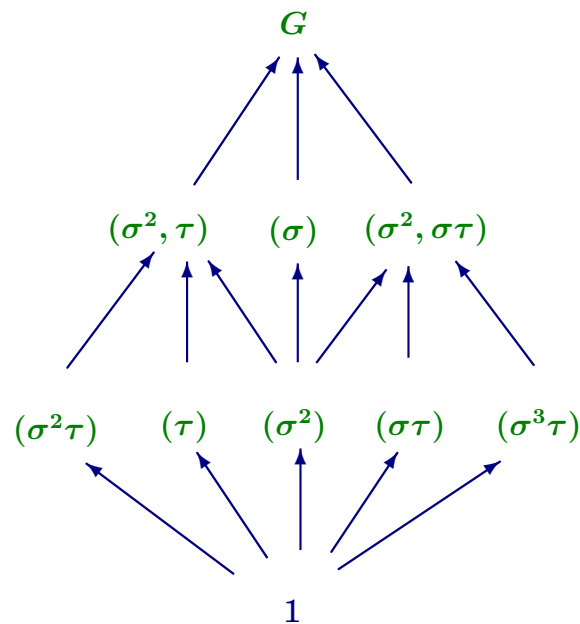
Dễ dàng thấy rằng $\sigma^4 = \tau^2 = 1$. Ngoài phần tử đơn vị 1 và σ, τ , các phần tử còn lại của G là :

$$\begin{aligned} \sigma^2 : \begin{cases} \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ i \mapsto i \end{cases}; & \quad \sigma^3 : \begin{cases} \sqrt[4]{2} \mapsto -i\sqrt[4]{2} \\ i \mapsto i \end{cases}; \\ \sigma\tau : \begin{cases} \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\ i \mapsto -i \end{cases}; & \quad \sigma^2\tau : \begin{cases} \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ i \mapsto -i \end{cases}; \end{aligned}$$

và

$$\sigma^3\tau : \begin{cases} \sqrt[4]{2} \mapsto -i\sqrt[4]{2} \\ i \mapsto -i \end{cases}.$$

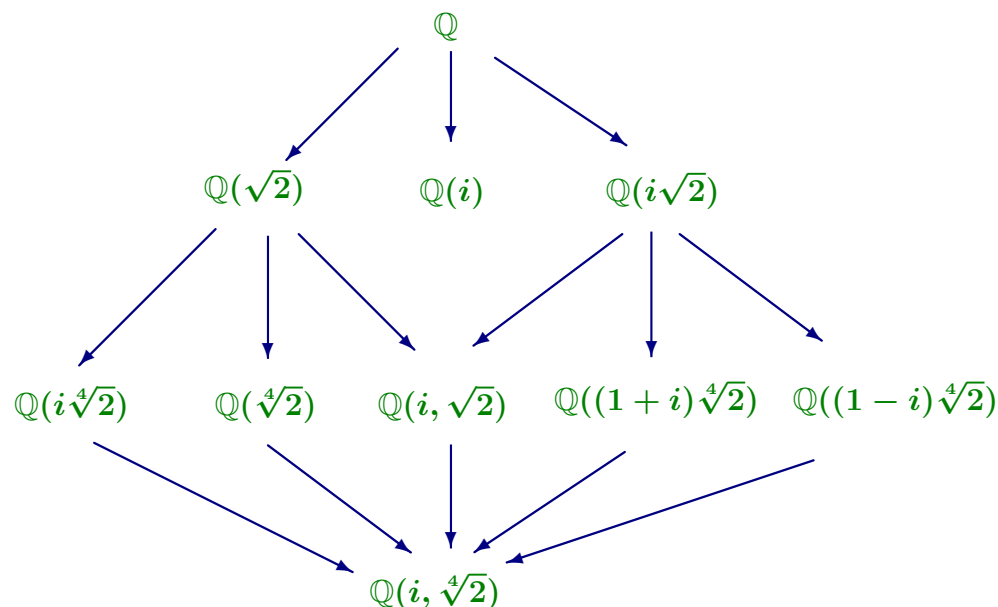
4) Sơ đồ bao hàm các nhóm con của G như trong Hình 9.



Hình 9: Sơ đồ các nhóm con của $\text{Aut}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$.

5) Do các tương ứng Galois là song ánh, ta có sơ đồ tất cả các trường trung gian của mở rộng như trong Hình 10.

6) Trong sơ đồ bao hàm các trường trung gian, dễ thấy rằng các mở rộng bậc 2



Hình 10: Sơ đồ các trường trung gian tương ứng.

của \mathbb{Q} là các mở rộng Galois. Các nhóm con cấp 4 tương ứng (σ^2, τ) , (σ) và $(\sigma^2, \sigma\tau)$ là các nhóm con chuẩn tắc. Mặt khác, mở rộng $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt{2})$ là mở rộng Galois nên nhóm con tương ứng (σ^2) cũng là một nhóm con chuẩn tắc của G . Các mở rộng còn lại đều không phải là mở rộng Galois do các nhóm con

tương ứng của nó không phải là nhóm con chuẩn tắc.

Định nghĩa. Cho M_1, \dots, M_r là các trường trung gian của mở rộng trường $E : F$. Trường hợp thành của M_1, \dots, M_r , kí hiệu $M_1 \cdots M_r$ hay $\prod_1^r M_i$, là trường con nhỏ nhất của E chứa M_1, \dots, M_r (nói cách khác nó là trường con của E sinh ra bởi $\cup_1^r M_i$).

Nhận xét 8.2. Các tương ứng Galois của một mở rộng Galois $E : F$ cho ta các tính chất sau :

- (i) Cho M_1, \dots, M_r là các trường trung gian. Khi đó trường hợp thành $M_1 \cdots M_r$ ứng với nhóm con lớn nhất chứa trong các $\mathcal{N}(M_i)$, tức là ứng với nhóm $\cap_1^r \mathcal{N}(M_i)$.
- (ii) Cho H là một nhóm con của $G = \text{Gal}(E/F)$. Gọi $M = \mathcal{T}(H)$. Khi đó nhóm con chuẩn tắc lớn nhất của G chứa trong H là $N = \bigcap_{\sigma \in G} \sigma H \sigma^{-1}$. Trường trung gian tương ứng với N là mở rộng Galois nhỏ nhất của F chứa tất cả σM , với $\sigma \in G$, tức là $\prod_{\sigma \in G} \sigma M$. Sau này, (xem Định nghĩa 11.1) ta thấy rằng $\prod_{\sigma \in G} \sigma M$

chính là *bao đóng chuẩn tắc* của M .

Các kết quả sau cho ta tính chất của các trường hợp thành.

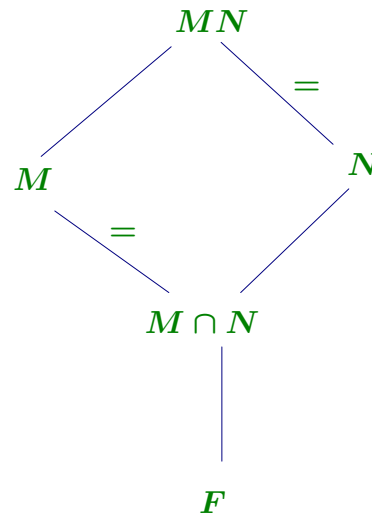
Mệnh đề 8.3. Cho M, N là các trường trung gian của $E : F$. Nếu $M : F$ là mở rộng Galois thì các mở rộng $MN : N$ và $M : (M \cap N)$ cũng Galois. Hơn thế, ánh xạ

$$\begin{array}{ccc} \text{Gal}(MN/N) & \longrightarrow & \text{Gal}(M/M \cap N) \\ \sigma & \longmapsto & \sigma|_M \end{array}$$

là một đẳng cấu nhóm.

Chứng minh. Xét sơ đồ như Hình 11. Vì $M : F$ là mở rộng Galois, ta có M là trường phân rã của một đa thức f tách được trên F . Do đó MN là trường phân rã của đa thức f trên N . Tương tự M là trường phân rã của f trên $M \cap N$. Vì thế, $MN : N$ và $M : M \cap N$ là các mở rộng Galois.

Mọi đồng cấu $\sigma \in \text{Gal}(MN/N)$ biến nghiệm của f thành nghiệm của f , vì thế



Hình 11:

$\sigma M = M$. Do đó, ta có đồng cấu nhóm :

$$\begin{array}{ccc} \psi : \text{Gal}(MN/N) & \longrightarrow & \text{Gal}(M/F) \\ \sigma & \longmapsto & \sigma|_M. \end{array}$$

Xét $\sigma \in \text{Gal}(MN/N)$ thỏa $\sigma|_M = 1$. Khi đó σ cố định mọi phần tử của M và N nên cố định mọi phần tử của MN . Do đó đồng cấu ψ là một đơn cấu.

Kí hiệu H' là ảnh của ψ . Gọi $M_{H'}$ là trường con của M cố định bởi H' . Rõ ràng $M \cap N \subset M_{H'}$. Theo tương ứng Galois, trường hợp thành $M_{H'}N$ ứng với nhóm

Galois $\text{Gal}(MN/N)$. Do đó $M_{H'}N = N$. Hay $M_{H'} \subset N$. Do đó $M_{H'} = M \cap N$. Tương ứng Galois trong $M : F$ cho ta $H' = \text{Gal}(M/M \cap N)$. Ta có điều phải chứng minh. \square

Hệ quả 8.4. Với giả thiết như mệnh đề trên và $N : F$ là mở rộng hữu hạn. Khi đó :

$$[MN : F] = \frac{[M : F][N : F]}{[(M \cap N) : F]}.$$

Chứng minh. Ta có

$$[MN : F] = [MN : N][N : F] = [M : (M \cap N)][N : F].$$

Thay $[M : (M \cap N)] = \frac{[M : F]}{[M \cap N : F]}$, ta có điều phải chứng minh. \square

Mệnh đề 8.5. Cho M, N là các trường trung gian của mở rộng trường trên F thỏa $M : F$ và $N : F$ là các mở rộng Galois. Khi đó MN và $M \cap N$ là các mở rộng Galois của F . Hơn thế :

$$\begin{array}{ccc} \text{Gal}(MN/F) & \longrightarrow & \text{Gal}(M/F) \times \text{Gal}(N/F) \\ \sigma & \longmapsto & (\sigma|_M, \sigma|_N) \end{array}$$

là một đẳng cấu từ $\text{Gal}(MN/F)$ vào nhóm con

$$H = \{(\sigma_1, \sigma_2) \mid \sigma_1|_{M \cap N} = \sigma_2|_{M \cap N}\}$$

của nhóm $\text{Gal}(M/F) \times \text{Gal}(N/F)$.

Chứng minh. Cho $\alpha \in M \cap N$, gọi $f \in F[x]$ là đa thức tối tiểu của α . Gọi $n = \deg(f)$. Vì M và N Galois trên F , đa thức f có đúng n nghiệm phân biệt trong M và N . Trong trường hợp thành MN , đa thức f có tối đa n nghiệm, do đó f có đúng n nghiệm phân biệt trong $M \cap N$. Như thế $M \cap N$ Galois trên F .

Mặt khác, trường M (tương ứng N) là trường phân rã của một đa thức g (tương ứng h) tách được trên F . Khi đó MN là trường phân rã của gh trên F . Do đó MN Galois trên F .

Xét đồng cấu

$$\begin{aligned} \phi : \text{Gal}(MN/F) &\longrightarrow \text{Gal}(M/F) \times \text{Gal}(N/F) \\ \sigma &\longmapsto (\sigma|_M, \sigma|_N). \end{aligned}$$

Nếu $\sigma \in \text{Gal}(MN/F)$ cố định mọi phần tử của M và N thì cố định mọi phần tử của MN . Do đó ϕ là đơn ánh.

Rõ ràng $\text{Im}(\phi) \subset H$, với $H = \{(\sigma_1, \sigma_2) \mid \sigma_1|_{M \cap N} = \sigma_2|_{M \cap N}\}$. Ta chứng minh chúng trùng nhau bằng cách chỉ ra rằng số phần tử của chúng bằng nhau. Ta có theo định lý cơ bản:

$$\frac{|\text{Gal}(N/F)|}{|\text{Gal}(N/(M \cap N))|} \cong |\text{Gal}(M \cap N/F)|.$$

Suy ra, với một đồng cấu $\sigma \in \text{Gal}(M/F)$ cho trước, đồng cấu hạn chế $\sigma|_{M \cap N}$ có đúng $[N : (M \cap N)]$ mở rộng trong $\text{Gal}(N/F)$. Do đó

$$(H : 1) = [M : F][N : (M \cap N)].$$

Mặt khác, theo hệ quả trên, ta có

$$\begin{aligned} [M : F][N : (M \cap N)] &= \frac{[M : F][N : F]}{[M \cap N : F]} = [MN : F] \\ &= |\text{Gal}(MN/F)|. \end{aligned}$$

□

Hệ quả 8.6. (i) Cho M, N như trong hệ quả trên. Nếu $M \cap N = F$ thì

$$\text{Gal}(MN/F) \cong \text{Gal}(M/F) \times \text{Gal}(N/F).$$

(ii) Ngược lại, cho một mở rộng $E : F$ có $\text{Gal}(E/F) = G_1 \times G_2$ với G_1, G_2 là 2 nhóm con của $\text{Gal}(E/F)$. Khi đó tồn tại các trường trung gian M, N của $E : F$ sao cho M, N là các mở rộng Galois trên F và $E = MN$.

Chứng minh. Phần thứ nhất suy ra ngay từ hệ quả trên. Gọi M và N tương ứng là các trường trung gian cố định bởi G_1 và G_2 . Khi đó trường trung gian $M \cap N$ ứng với nhóm con nhỏ nhất chứa G_1 và G_2 . Nhóm đó chính là G . Do đó $M \cap N = F$. Theo hệ quả trên, ta có MN Galois trên F và có nhóm Galois đẳng cấu với $G_1 \times G_2 = \text{Gal}(E/F)$. Suy ra $MN = E$. \square

Bài tập

 **8.1.** Chọn đúng, sai cho các mệnh đề sau :

- Nếu mở rộng là Galois thì các tương ứng Galois là các song ánh, bảo toàn quan hệ bao hàm.
- Một mở rộng hữu hạn là Galois khi và chỉ khi các tương ứng Galois là song ánh.

- c) Trong một mở rộng Galois $F \subset E$, trường cố định bởi một nhóm con của nhóm Galois là một mở rộng Galois trên F .
- d) Trong một mở rộng Galois $F \subset E$, trường cố định bởi một nhóm con chuẩn tắc của nhóm Galois là một mở rộng Galois trên F .
- e) Trong một mở rộng Galois $F \subset E$ có nhóm Galois G , trường trung gian M ứng với nhóm con H của G có bậc trên F là $(H : 1)$.
- f) Trong một mở rộng Galois $F \subset E$ có nhóm Galois G , trường trung gian M ứng với nhóm con H của G có bậc trên F là $(G : H)$.
- g) Trong một mở rộng Galois $F \subset E$ có nhóm Galois G , gọi M là trường trung gian ứng với nhóm con H của G . Khi đó $[E : M] = (H : 1)$.
- h) Nhóm Galois của một đa thức bậc 3 luôn là nhóm aben.
- i) Nhóm Galois của một mở rộng Galois bậc 4 luôn là nhóm aben.
- j) Trường hợp thành của 2 trường trung gian là trường con nhỏ nhất chứa chúng. (Xem HD 285)

 **8.2.** Chỉ ra các tương ứng Galois của mở rộng trường $\mathbb{Q}(\xi) : \mathbb{Q}$ với $\xi = e^{2\pi i/7}$. Chỉ

ra các trường trung gian nào là Galois trên \mathbb{Q} . Trong trường hợp trường trung gian M là Galois trên \mathbb{Q} , tìm đa thức tương ứng $g \in \mathbb{Q}[x]$ sao cho M là trường phân rã của g trên \mathbb{Q} (Xem HD 285)

👉 8.3. Chứng minh các kết luận ở Nhận xét 8.2. (Xem HD 286)

👉 8.4. Phân tích các tương ứng Galois của trường phân rã của đa thức $x^3 - 2$ trên \mathbb{Q} và chỉ ra các trường trung gian là mở rộng Galois trên \mathbb{Q} . (Xem HD 287)

👉 8.5. Phân tích tương ứng Galois của mở rộng ở các Bài tập 6.2, 7.7 và 7.9. (Xem HD 287)

👉 8.6. Cho K là trường phân rã của đa thức $x^3 - 5$ trên $\mathbb{Q}(\sqrt{7})$. Chứng minh rằng tồn tại trường con M của K chứa $\mathbb{Q}(\sqrt{7})$, sao cho $\text{Gal}(K/M) \cong \mathbb{Z}_3$. (xem bài tập 6.9) (Xem HD 288)

👉 8.7. Xác định nhóm Galois của đa thức $f = x^5 - 6x^4 + 3$ trên F với

a) $F = \mathbb{Q}$;

b) $F = \mathbb{Z}_2$.

Trong mỗi trường hợp, gọi K là trường phân rã của f , xác định có bao nhiêu trường trung gian M của $F \subset K$ sao cho $[M : F] = 2$. (Xem HD 288)

✎ 8.8. Cho $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$ và L là trường phân rã của $f = x^3 - 2$.

a) Xác định nhóm Galois của $K : \mathbb{Q}$ và $L : \mathbb{Q}$.

b) Trường K có chứa nghiệm nào của f hay không?

c) Xác định bậc của mở rộng $\mathbb{Q} \subset K \cap L$. (Xem HD 288)

✎ 8.9. Cho F là trường có đặc số khác 2.

a) Cho $a, b \in F$ sao cho a, b và ab không có căn bậc 2 trong F . Chứng minh rằng trường $F(\sqrt{a}, \sqrt{b})$ là một mở rộng Galois trên F và $\text{Gal}(K/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

b) Đảo lại, cho $F \subset K$ là một mở rộng bậc 4 có $\text{Aut}(K/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Chứng minh rằng $K = F(\sqrt{a}, \sqrt{b})$ với a, b và ab không có căn bậc 2 trong F .

(Xem HD 289)

✎ **8.10.** Cho $E = \mathbb{Q}(\sqrt[8]{2}, i)$, $M_1 = \mathbb{Q}(i)$, $M_2 = \mathbb{Q}(\sqrt{2})$, $M_3 = \mathbb{Q}(\sqrt{-2})$. Xác định các nhóm $\text{Aut}(E/M_i)$ với $1 \leq i \leq 3$. (Xem HD 289)

✎ **8.11.** Cho $f = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$.

a) Chứng tỏ f bất khả quy trên \mathbb{Q} .

b) Đặt $\alpha = \sqrt{1 + \sqrt{3}}$ và $\beta = \sqrt{1 - \sqrt{3}}$. Chứng tỏ α và β đều là nghiệm của f . Tìm các nghiệm còn lại của f .

c) Đặt $K_1 = \mathbb{Q}(\alpha)$, $K_2 = \mathbb{Q}(\beta)$. Chứng tỏ $K_1 \neq K_2$ và

$$K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F.$$

d) Chứng minh rằng K_1, K_2 và K_1K_2 là các mở rộng Galois trên F . Mô tả nhóm Galois $\text{Gal}(K_1K_2/F)$, vẽ sơ đồ bao hàm các nhóm con và các trường trung gian tương ứng.

e) Chứng minh rằng nhóm Galois của f đẳng cấu với nhóm các phép đối xứng của hình vuông. (Xem HD 290)

§ 9 MỘT SỐ ỨNG DỤNG CỦA LÝ THUYẾT GALOIS

9.1 TRƯỜNG HỮU HẠN

Định nghĩa. Một trường có hữu hạn phần tử thì gọi là trường hữu hạn.

Nhận xét 9.1.

- (i) Trường hữu hạn E có đặc số p nguyên tố. Do đó trường con nguyên tố của E , kí hiệu \mathbb{F}_p , đẳng cấu với \mathbb{Z}_p .
- (ii) Trường hữu hạn E có đặc số p thì có $q = p^n$ phần tử, với $n = [E : \mathbb{F}_p]$.

Mệnh đề 9.2. Mọi trường hữu hạn đều là mở rộng đơn trên trường con nguyên tố của nó.

Chứng minh. Cho E là một trường hữu hạn có trường con nguyên tố \mathbb{F}_p . Ta biết rằng nhóm nhân $E^* = E \setminus \{0\}$ là một nhóm cyclic. Gọi α là phần tử sinh. Rõ ràng $E = \mathbb{F}_p(\alpha)$. □

Mệnh đề 9.3. Một trường hữu hạn E có p^n phần tử (p nguyên tố) đẳng cấu với trường phân rã của $x^{p^n} - x$ trên \mathbb{F}_p , có nhóm Galois là nhóm cyclic cấp n sinh bởi

ánh xạ Frobenius $\sigma : a \mapsto a^p$. Suy ra với mọi $n \in \mathbb{N}$, tồn tại duy nhất (sai khác đẳng cấu) một trường hữu hạn có p^n phần tử, kí hiệu \mathbb{F}_{p^n} .

Chứng minh. Do $E^* = E \setminus \{0\}$ là nhóm nhân cấp $p^n - 1$ nên $a^{p^n-1} = 1$, với mọi $a \in E^*$. Suy ra, mọi phần tử của E đều là nghiệm của đa thức $x^{p^n} - x$. Hơn nữa, đa thức $x^{p^n} - x$ không thể có quá p^n nghiệm, do đó E là trường phân rã của $x^{p^n} - x$ trên \mathbb{F}_p . Vì đa thức $x^{p^n} - x$ tách được trên \mathbb{F}_p nên E là mở rộng Galois trên \mathbb{F}_p và nhóm Galois G của nó có cấp n . Gọi $\alpha \in E^*$ là phần tử có cấp $p^n - 1$ trong nhóm cyclic E^* . Do $\sigma^i(\alpha) = \alpha^{p^i} \neq \alpha \forall i < n$ và $\sigma^n(\alpha) = \alpha$ nên σ có cấp là n . Do đó G là nhóm cyclic sinh ra bởi σ . \square

Hệ quả 9.4. Cho \mathbb{F}_{p^n} là trường có p^n phần tử. Mọi trường trung gian của $\mathbb{F}_{p^n} : \mathbb{F}_p$ đều là mở rộng Galois của \mathbb{F}_p và tương ứng 1-1 với tập các ước của n .

Chứng minh. Vì mở rộng là Galois, các trường trung gian của $\mathbb{F}_{p^n} : \mathbb{F}_p$ tương ứng 1-1 với các nhóm con của nhóm cyclic (σ) cấp n . Do đó chúng tương ứng 1-1 với các ước của n . Với $d \mid n$, trường trung gian duy nhất bậc d trên \mathbb{F}_p (đẳng cấu với \mathbb{F}_{p^d}) là trường cố định bởi nhóm cyclic (σ^d) . \square

Hệ quả 9.5. Cho $f \in \mathbb{F}_p[x]$ bất khả quy bậc $d \leq n$. Khi đó f là một nhân tử của $x^{p^n} - x$ khi và chỉ khi $d \mid n$.

Chứng minh. Gọi α là một nghiệm của f . Vì f là nhân tử của $x^{p^n} - x$ nên α nằm trong trường phân rã của $x^{p^n} - x$. Do đó $d = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ là một ước của n .

Ngược lại, ta có $\mathbb{F}_p(\alpha)$ đẳng cấu với \mathbb{F}_{p^d} là trường phân rã của $x^{p^d} - x$ trên \mathbb{F}_p . Suy ra α là nghiệm của $x^{p^d} - x$. Do đó f là ước của $x^{p^d} - x$ nên là ước của $x^{p^n} - x$. □

Sử dụng Maple 4. Hệ quả trên cho ta xác định tất cả các đa thức chuẩn tắc, bất khả quy bậc d (và bậc $d' \mid d$) trên \mathbb{Z}_p bằng cách tìm dạng nhân tử hóa của $x^{p^d} - x$. Với Maple, ta dễ dàng thực hiện điều đó.

Ví dụ sau tìm tất cả các đa thức bất khả quy chuẩn tắc bậc 1, bậc 2 và 4 trên trường \mathbb{Z}_3 .

```
> Factor(x^(3^4)-x)mod 3 ;
```

$$\begin{aligned}
& (x^4 + x^2 + x + 1) x (x^4 + x^3 + x^2 + x + 1) (x + 1) (x^2 + 1) \\
& (x^4 + 2x^3 + x^2 + 1) (x^4 + 2x + 2) (x^4 + 2x^3 + x^2 + x + 2) \\
& (x^4 + 2x^3 + 2) (x^4 + x^3 + 2x + 1) (x^4 + 2x^2 + 2) \\
& (x^4 + 2x^3 + x + 1) (x^4 + x^2 + 2) (x^4 + x^3 + x^2 + 2x + 2) \\
& (x^4 + 2x^3 + 2x^2 + x + 2) (x^2 + x + 2) (x^4 + x^3 + 2) (x + 2) \\
& (x^4 + x^2 + 2x + 1) (x^4 + x + 2) (x^4 + x^3 + 2x^2 + 2x + 2) \\
& (x^2 + 2x + 2) (x^4 + x^3 + x^2 + 1) (x^4 + 2x^3 + x^2 + 2x + 1)
\end{aligned}$$

Hệ quả 9.6. Mọi đa thức bất khả quy f trên trường hữu hạn E đều phân rã trong mở rộng $E(\alpha)$ với α là một nghiệm của f .

Chứng minh. Trường $E(\alpha)$ là mở rộng Galois trên \mathbb{F}_p nên là mở rộng Galois trên E . Suy ra đa thức tối tiểu của α (do đó f) phân rã trong $E(\alpha)$. \square

Mệnh đề 9.7. Cho E là một trường hữu hạn. Tồn tại bao đóng đại số của E .

Chứng minh. Gọi p là đặc số của E . Khi đó E đẳng cấu với \mathbb{F}_{p^n} . Đặt $\overline{\mathbb{F}}_p = \bigcup_{r \geq 1} \mathbb{F}_{p^r}$. Khi đó $\overline{\mathbb{F}}_p$ là một trường. Dễ thấy rằng nó là một mở rộng đại số của \mathbb{F}_p , và do đó là mở rộng đại số của E . Cuối cùng nó là một trường đóng đại số

vì với mọi $f \in \overline{\mathbb{F}_p}[x]$, tồn tại l để $f \in \mathbb{F}_{p^l}[x]$. Trường phân rã của f trên \mathbb{F}_{p^l} là mở rộng hữu hạn của \mathbb{F}_p do đó có dạng \mathbb{F}_{p^m} nên chứa trong $\overline{\mathbb{F}_p}$. \square

Việc tồn tại bao đóng đại số của một trường bất kì, xem Định lý C.1 trong Phụ lục.

9.2 TRƯỜNG VÀ ĐA THỨC CHIA ĐƯỜNG TRÒN

Định nghĩa. Cho F là một trường và $n \in \mathbb{N}^*$ không chia hết cho đặc số của F . Trường phân rã E_n của $x^n - 1$ trên F được gọi là trường chia đường tròn bậc n (trên F).

Nhận xét 9.8. Một nghiệm của $x^n - 1$ gọi là căn bậc n của đơn vị. Tập tất cả các căn bậc n của đơn vị tạo thành một nhóm nhân C_n trong trường chia đường tròn bậc E_n . Nhóm C_n có n phần tử do $x^n - 1$ tách được. Như thế nhóm C_n là nhóm cyclic (xem Bài tập 0.18). Một phần tử sinh của C_n gọi là căn nguyên thủy bậc n của đơn vị. Số các căn nguyên thủy bậc n của đơn vị bằng $\varphi(n)$ với φ là hàm Euler.

Mệnh đề 9.9. Trường chia đường tròn E_n là mở rộng đơn Galois trên F .

Chứng minh. Gọi ξ_n là một căn nguyên thủy bậc n của đơn vị. Khi đó $E_n = F(\xi_n)$. Đa thức $x^n - 1$ tách được trên F nên E_n Galois trên F . \square

Cho $\sigma \in \text{Gal}(E_n/F)$. Khi đó σ cảm sinh một tự đẳng cấu của nhóm C_n . Do đó $\sigma(\xi_n)$ cũng là một phần tử sinh của C_n . Suy ra, tồn tại duy nhất $i \in \{1, \dots, n-1\}$, thỏa $(i, n) = 1$ để $\sigma(\xi_n) = \xi_n^i$. Như thế, ta có một ánh xạ từ $\text{Gal}(F(\xi_n)/F)$ vào \mathbb{Z}_n^\times , nhóm nhân các phần tử khả nghịch của \mathbb{Z}_n , xác định bởi $\sigma \mapsto \bar{i}$. Dễ dàng thấy rằng ánh xạ này là một đơn cấu nhóm. Do đó ta có kết quả sau.

Mệnh đề 9.10. Ánh xạ từ $\text{Gal}(F(\xi_n)/F)$ vào \mathbb{Z}_n^\times xác định bởi $\sigma \mapsto \bar{i}$ là một đơn cấu nhóm. Suy ra nhóm Galois $\text{Gal}(F(\xi_n)/F)$ đẳng cấu với một nhóm con của \mathbb{Z}_n^\times .

Nhận xét 9.11. Đơn cấu nhóm $\text{Gal}(F(\xi_n)/F) \longrightarrow \mathbb{Z}_n^\times$ nêu trên không nhất thiết phải là một toàn cấu. Ví dụ nếu $F = \mathbb{R}$, nhóm $\text{Gal}(\mathbb{R}(\xi_n)/\mathbb{R})$ hoặc là nhóm tầm thường hoặc chỉ có 2 phần tử. Mặt khác, nếu $F = \mathbb{Q}$ và $n = p$, nhóm $\text{Gal}(\mathbb{Q}(\xi_p)/F)$ có $p - 1$ phần tử, bằng với cấp của \mathbb{Z}_p^\times , nên đơn cấu trên là một đẳng cấu. Ta sẽ thấy rằng điều đó đúng với mọi n khi $F = \mathbb{Q}$.

Định nghĩa.

Cho $\xi_1, \dots, \xi_{\varphi(n)}$ là $\varphi(n)$ căn nguyên thủy bậc n của đơn vị trong trường chia đường tròn bậc n trên F . Đa thức chia đường tròn thứ n là đa thức định bởi

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \xi_i).$$

Ta có các tính chất đơn giản sau đây liên quan đến $\Phi(n)$:

Mệnh đề 9.12.

- (i) $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
- (ii) Nếu F có đặc số 0 và đồng nhất \mathbb{Z} với ảnh của nó trong F qua đơn cấu định bởi $n \mapsto n \cdot 1_F$ thì $\Phi_n(x) \in \mathbb{Z}[x]$.
- (iii) Nếu F có đặc số p và đồng nhất \mathbb{Z}_p với trường con nguyên tố của F thì $\Phi_n(x) \in \mathbb{Z}_p[x]$, bằng với đa thức nhận được ở (ii) modulo p .

Chứng minh. (i) Hiển nhiên.

(ii) Ta chứng minh bằng quy nạp theo n . Nếu $n = 1$ kết quả là hiển nhiên. Ta có

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \prod_{d||n} \Phi_d(x).$$

Theo giả thiết quy nạp $\Phi_d(x) \in \mathbb{Z}[x]$, $\forall d||n$ (nghĩa là d là ước của n và $d < n$).
Đặt

$$G = \prod_{d||n} \Phi_d(x) \in \mathbb{Z}[x].$$

Ta có

$$\Phi_n(x) = \frac{x^n - 1}{G}$$

là thương của hai đa thức có hệ tử thuộc \mathbb{Z} nên $\Phi_n(x) \in \mathbb{Z}[x]$.

(iii) Hiển nhiên từ chứng minh của (ii).

□

Ví dụ 29. (i) Với mọi p nguyên tố, ta có

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1.$$

(ii) Từ mệnh đề trên, ta dễ dàng tính được $\Phi(n)$, chẳng hạn :

- $\Phi_1(x) = x - 1 ;$
- $\Phi_2(x) = \frac{x^2 - 1}{x - 1} = x + 1 ;$
- $\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1 ;$
- $\Phi_4(x) = \frac{x^4 - 1}{(x - 1)(x + 1)} = x^2 + 1 ;$
- $\Phi_6(x) = \frac{x^6 - 1}{(x - 1)(x + 1)(x^2 + x + 1)} = x^2 - x + 1 ;$
- $\Phi_8(x) = \frac{x^8 - 1}{(x - 1)(x + 1)(x^2 + 1)} = x^4 + 1 ;$
- $\Phi_9(x) = \frac{x^9 - 1}{(x - 1)(x^2 + x + 1)} = x^6 + x^3 + 1 ;$
- $\Phi_{10}(x) = \frac{x^{10} - 1}{(x - 1)(x + 1)\Phi_5(n)} = x^4 - x^3 + x^2 - x + 1 ;$

$$\bullet \Phi_{12}(x) = \frac{x^{12} - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)} = x^4 - x^2 + 1 ;$$

Nhận xét 9.13. Để tính đa thức chia đường tròn, ta có thể dùng công thức đảo ngược Möbius sau đây. Gọi $\mu : \mathbb{N}^* \longrightarrow \mathbb{N}$ là hàm Möbius định bởi :

$$\mu(n) = \begin{cases} 1 & \text{nếu } n = 1, \\ 0 & \text{nếu } n \text{ chứa một ước chính phương,} \\ (-1)^r & \text{nếu } n = p_1 \cdots p_r, p_i \neq p_j \text{ nguyên tố.} \end{cases}$$

Đặt f là hàm xác định trên \mathbb{N} và lấy giá trị trong 1 nhóm nhân aben. Cho $F(n) = \prod_{d|n} f(d)$. Khi đó công thức đảo ngược Möbius cho bởi :

$$f(n) = \prod_{d|n} F(d)^{\mu(\frac{n}{d})}.$$

Áp dụng cho hàm $f(n) = \Phi_n(x)$ có giá trị trong nhóm nhân $F(x)^*$ và $F(n) = x^n - 1$. Ta có $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$.

Sử dụng Maple 5. Maple cung cấp cho ta lệnh để tính đa thức chia đường tròn như sau :

> with(numtheory):

> cyclotomic(n,x); với n là một số tự nhiên xác định.

Ví dụ, Maple cho lại ta các đa thức chia đường tròn đã biết:

> for i to 12 do Phi[i]:=cyclotomic(i,x) od;

$$\Phi_1 := x - 1$$

$$\Phi_2 := x + 1$$

$$\Phi_3 := x^2 + x + 1$$

$$\Phi_4 := x^2 + 1$$

$$\Phi_5 := x^4 + x^3 + x^2 + x + 1$$

$$\Phi_6 := x^2 - x + 1$$

$$\Phi_7 := x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_8 := x^4 + 1$$

$$\Phi_9 := x^6 + x^3 + 1$$

$$\Phi_{10} := x^4 - x^3 + x^2 - x + 1$$

$$\Phi_{11} := x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_{12} := x^4 - x^2 + 1$$

Ta có kết quả đơn giản sau đây :

Mệnh đề 9.14. Cho F là trường có đặc số 0 hoặc không chia hết n . Gọi $F(\xi_n)$ là trường chia đường tròn bậc n trên F , với ξ_n là một căn nguyên thủy bậc n của đơn vị. Các mệnh đề sau là tương đương :

- (i) đa thức chia đường tròn $\Phi_n(x)$ bất khả quy trên F ;
- (ii) $[F(\xi_n) : F] = \varphi(n)$;
- (iii) đơn cấu $\text{Gal}(F(\xi_n)/F) \longrightarrow \mathbb{Z}_n^\times$ xác định như trong (9.10) là một đẳng cấu.

Chứng minh. Đa thức tối tiểu của ξ_n trên F là ước của $\Phi_n(x)$, và $\Phi_n(x)$ có bậc là $\varphi(n)$. Do đó $\Phi_n(x)$ bất khả quy khi và chỉ khi $[F(\xi_n) : F] = \varphi(n)$. Chú ý rằng cấp của $\text{Gal}(F(\xi_n)/F)$ bằng với $[F(\xi_n) : F]$, nên $[F(\xi_n) : F] = \varphi(n)$ khi và chỉ khi đơn cấu $\text{Gal}(F(\xi_n)/F) \longrightarrow \mathbb{Z}_n^\times$ là đẳng cấu. \square

Định lí 9.15. Đa thức chia đường tròn $\Phi_n(x)$ bất khả quy trên \mathbb{Q} .

Chứng minh. Gọi $f \in \mathbb{Z}[x]$ là một ước bất khả quy của $\Phi_n(x)$. Ta có $\Phi_n(x) = fg$, với $g \in \mathbb{Z}[x]$. Gọi ξ_n là một nghiệm của f . Rõ ràng ξ_n là một căn nguyên thủy bậc n của đơn vị. Ta chứng minh $\Phi_n(x) = f$ bằng cách chỉ ra rằng với mọi m nguyên tố cùng nhau với n thì ξ_n^m cũng là một nghiệm của f . Thực ra, ta chỉ cần chỉ ra rằng với mọi p nguyên tố không chia hết n , phân tử ξ_n^p cũng là một nghiệm của f .

Giả sử có p nguyên tố không chia hết n sao cho ξ_n^p không phải là nghiệm của f . Suy ra ξ_n^p là nghiệm của g . Nói cách khác ξ_n là nghiệm của $g(x^p)$. Như vậy ξ_n là nghiệm chung của f và $g(x^p)$. Như thế $(f, g(x^p)) \neq 1$ trong $\mathbb{Q}[x]$. Gọi $\bar{f}, \overline{g(x^p)}$ là ảnh của f và $g(x^p)$ trong vành $\mathbb{Z}_p[x]$. Suy ra $(\bar{f}, \overline{g(x^p)}) \neq 1$ trong $\mathbb{Z}_p[x]$. Trong $\mathbb{Z}_p[x]$, ta có $\overline{g(x^p)} = \overline{g(x)}^p$. Như thế $(\bar{f}, \bar{g}) \neq 1$ trong $\mathbb{Z}_p[x]$. Nói cách khác, $\overline{\Phi_n(x)}$ có nghiệm bội trong trường phân rã của nó trên \mathbb{Z}_p . Điều này vô lí. \square

Nhận xét 9.16. Trên trường có đặc số lớn hơn 0, đa thức $\Phi_n(x)$ không nhất thiết bất khả quy. Ví dụ

$$\Phi_{12}(x) = x^4 - x^2 + 1 = (x^2 + 6x + 1)(x^2 + 5x + 1)$$

trong $\mathbb{Z}_{11}[x]$.

9.3 ĐA GIÁC ĐỀU DỰNG ĐƯỢC BẰNG THƯỚC KẼ VÀ COMPA

Trong Bài 4, ta đã chứng minh rằng nếu $\alpha \in \mathbb{R}$ dựng được bằng thước kẻ và compa thì $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$ với $r \in \mathbb{N}$. Ngược lại, ta có :

Bổ đề 9.17. Cho $\alpha \in E \subset \mathbb{R}$ với E là một mở rộng Galois của \mathbb{Q} . Nếu $[E : \mathbb{Q}] = 2^r$ thì α dựng được bằng thước kẻ và compa.

Chứng minh. Giả sử ta có $[E : \mathbb{Q}] = 2^r$. Gọi $G = \text{Gal}(E/\mathbb{Q})$. Ta có $(G : 1) = 2^r$. Tồn tại dãy chuyển các nhóm con (A.17)

$$\{1\} = G_0 \subset G_1 \cdots \subset G_r = G$$

thỏa $(G_i : G_{i-1}) = 2$, với mọi $i = 1, \dots, r$. Ta có dãy chuyển các trường trung gian tương ứng:

$$E = \mathcal{T}(G_0) \supset \mathcal{T}(G_1) \cdots \supset \mathcal{T}(G_r) = \mathbb{Q}$$

với $[\mathcal{T}(G_{i-1}) : \mathcal{T}(G_i)] = 2$, với mọi $i = 1, \dots, r$. Suy ra

$$\mathcal{T}(G_{i-1}) = \mathcal{T}(G_i)(\sqrt{d}),$$

với $d \in \mathcal{T}(G_i)$. Do đó nếu mọi phần tử của $\mathcal{T}(G_i)$ dựng được thì mọi phần tử của $\mathcal{T}(G_{i-1})$ cũng dựng được, với mọi $i = 1, \dots, r$. Suy ra α dựng được. \square

Định lí 9.18. Đa giác đều n cạnh dựng được khi và chỉ khi $n = 2^r p_1 \cdots p_s$ với p_1, \dots, p_s là các số nguyên tố Fermat khác nhau.

Chứng minh. Đa giác đều dựng được khi và chỉ khi

$$\xi_n = e^{2\pi i/n} \in \mathbb{C} = \mathbb{R}^2$$

là một điểm dựng được. Tương đương với số $\alpha = \cos(\frac{2\pi}{n})$ dựng được. Ta có $\alpha = (\xi_n + \xi_n^{-1})/2$. Suy ra $\xi_n^2 - 2\alpha\xi_n + 1 = 0$. Do đó $[\mathbb{Q}(\xi_n) : \mathbb{Q}(\alpha)] = 2$.

Mặt khác ta biết rằng $\mathbb{Q}(\xi_n) : \mathbb{Q}$ là mở rộng Galois có nhóm Galois G đẳng cấu với \mathbb{Z}_n^\times . Trường trung gian $\mathbb{Q}(\alpha)$ cũng là một mở rộng Galois trên \mathbb{Q} . Do đó α dựng được khi và chỉ khi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{\varphi(n)}{2}$ là một lũy thừa của 2. Tương đương $\varphi(n)$ là một lũy thừa của 2. Điều đó xảy ra khi và chỉ khi n có dạng như đã chỉ ra (xem Mệnh đề 0.22). \square

9.4 ĐỊNH LÝ CƠ BẢN CỦA ĐẠI SỐ

Ta sẽ áp dụng Lí thuyết Galois để đưa ra một chứng minh cho Định lý cơ bản của đại số.

Định lý 9.19 (Định lý cơ bản của đại số). Mọi đa thức bậc lớn hơn 0 trên trường số phức \mathbb{C} có một nghiệm trong \mathbb{C} .

Chứng minh. Ta dùng 2 tính chất cơ bản sau về trường số thực và phức.

Tính chất 1. Mọi đa thức hệ số thực có bậc lẻ đều có một nghiệm thực. Suy ra \mathbb{R} không có một mở rộng thực sự bậc lẻ. Tính chất này suy ra dễ dàng từ Định lý giá trị trung bình. Một đa thức $f(x)$ trên \mathbb{R} chuẩn tắc bậc lẻ thì có giá trị âm với x đủ bé và có giá trị dương với x đủ lớn. Vì thế f có ít nhất một nghiệm thực. Với một mở rộng $E : \mathbb{R}$ bậc lẻ, do E là mở rộng đơn của \mathbb{R} nên $E = \mathbb{R}(\alpha)$. Gọi f là đa thức tối tiểu của α thì f bất khả quy và có nghiệm trong \mathbb{R} , nên f có bậc 1. Suy ra $E = \mathbb{R}$.

Tính chất 2. Mọi đa thức bậc 2 trên \mathbb{C} có nghiệm trong \mathbb{C} . Tính chất này được suy ra nếu ta chỉ ra rằng mọi số phức đều có một căn bậc 2. Thật vậy, nếu $z = re^{i\alpha}$ với

$0 \leq r \in \mathbb{R}$. Khi đó số phức $a = \sqrt{r}e^{\alpha/2}$ thỏa $a^2 = z$.

Bây giờ ta chứng minh định lí. Gọi $\tau \in \text{Aut}(\mathbb{C})$ là phép lấy liên hợp. Cho $f \in \mathbb{C}[x]$ có bậc n lớn hơn 0. Gọi \bar{f} là đa thức nhận được bằng tác động τ lên các hệ số của f . Đa thức $f\bar{f}$ có các hệ số bất biến bởi τ nên thuộc vào $\mathbb{R}[x]$. Do đó, để chứng minh f có nghiệm phức, ta chỉ cần chứng minh cho $f \in \mathbb{R}[x]$. Xét $n = 2^m k$ với k lẻ và $m \geq 0$. Ta chứng minh bằng quy nạp trên m . Nếu $m = 0$ thì n lẻ, nên định lí được chứng minh. Xét $m > 0$. Gọi $\alpha_1, \dots, \alpha_n$ là các nghiệm của f và đặt $K = \mathbb{R}(\alpha_1, \dots, \alpha_n, i)$. Khi đó K là mở rộng Galois của \mathbb{R} và $\mathbb{C} \subset K$. Với mọi $t \in \mathbb{R}$, xét đa thức :

$$L_t = \prod_{1 \leq i < j \leq n} [x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)].$$

Rõ ràng, với mọi $\sigma \in \text{Gal}(K/\mathbb{R})$, khi tác động σ_* lên f , các nhân tử của L hoán vị cho nhau nên $\sigma_*(L_t) = L_t$. Nói cách khác $L_t \in \mathbb{R}[x]$. Bậc của L_t là

$$\frac{n(n-1)}{2} = 2^{m-1}k(2^m k - 1) = 2^{m-1}k'$$

với k' lẻ. Do số mũ của 2 nhỏ hơn m nên theo giả thuyết quy nạp, đa thức L_t có

nghiệm phức. Như thế với mỗi $t \in \mathbb{R}$, tồn tại i, j thỏa $0 \leq i < j \leq n$ sao cho $\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$. Do t có thể lấy vô hạn trong khi số cặp (i, j) hữu hạn, nên tồn tại $s \neq r$ trong \mathbb{R} và cặp i, j để

$$\alpha_i + \alpha_j + t\alpha_i\alpha_j, \alpha_i + \alpha_j + s\alpha_i\alpha_j \in \mathbb{C}.$$

Suy ra $(s - t)\alpha_i\alpha_j \in \mathbb{C}$. Nên $\alpha_i\alpha_j$ và do đó cả $\alpha_i + \alpha_j$ thuộc \mathbb{C} . Như thế α_i và α_j là 2 nghiệm của cùng một đa thức bậc 2 trên \mathbb{C} do đó thuộc \mathbb{C} . Ta có điều phải chứng minh.

□

Bài tập

👉 **9.1.** Chọn đúng, sai cho các mệnh đề sau :


- a) Mọi trường hữu hạn đều là mở rộng Galois trên trường nguyên tố của nó.
- b) Có duy nhất (sai khác đẳng cấu) một trường hữu hạn có n phần tử.
- c) Có duy nhất (sai khác đẳng cấu) một trường hữu hạn có p^n phần tử với p

nguyên tố.


- d) Mọi đa thức bất khả quy bậc d trên \mathbb{Z}_p đều là ước của $x^{p^d} - x$.
- e) Có hữu hạn đa thức bất khả quy bậc n trên một trường hữu hạn cho trước.
- f) Có trường hữu hạn gồm 124 phần tử.
- g) Có trường hữu hạn mà nhóm nhân các phần tử khác 0 gồm 124 phần tử.
- h) Mọi trường có 121 phần tử đều đẳng cấu.
- i) Mọi tự đẳng cấu của trường hữu hạn đều là tự đẳng cấu.
- j) Nhóm cộng các phần tử trong trường hữu hạn là nhóm cyclic.
- k) Nhóm con hữu hạn của nhóm nhân các phần tử khác 0 của một trường hữu hạn là một nhóm cyclic.
- l) Mọi trường chia đường tròn đều là mở rộng Galois.
- m) Nhóm Galois của trường chia đường tròn là nhóm cyclic.
- n) Nhóm Galois của trường chia đường tròn là nhóm aben.
- o) Có đúng $\varphi(n)$ căn nguyên thủy bậc $n > 0$ của đơn vị trên trường F có đặc số không chia hết n .

- p) Đa thức chia đường tròn luôn luôn bất khả quy trên trường nguyên tố của nó.
- q) Đa thức chia đường tròn luôn tách được.
- r) Đa giác đều có $2^{2006} \cdot 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$ cạnh dựng được bằng thước kẻ và compa.
- s) Đa giác đều có 30 cạnh dựng được bằng thước kẻ và compa.
- t) Đa giác đều có 18 cạnh dựng được bằng thước kẻ và compa.
- u) Đa giác đều có 14 cạnh dựng được bằng thước kẻ và compa.

(Xem HD 291)


 **9.2.** Tìm tất cả đa thức bất khả quy bậc 2, 3, 4, 5 trên trường $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$ (có thể sử dụng Maple).

(Xem HD 291)

 **9.3.** Cho f, g là 2 đa thức bất khả quy cùng bậc trên trường hữu hạn E . Gọi α, β lần lượt là nghiệm của f và g . Chứng minh rằng các trường $E(\alpha)$ và $E(\beta)$ đẳng cấu với nhau.

(Xem HD 291)

- 🍰 **9.4.** Chứng minh rằng với mọi số nguyên dương n , tồn tại một đa thức bất khả quy bậc n trên \mathbb{F}_p . (Xem HD 292)
- 🍰 **9.5.** Chứng minh rằng đa thức $x^4 + 1$ là khả quy trên \mathbb{Z}_p với mọi p nguyên tố. (Xem HD 292)
- 🍰 **9.6.** Xác định các tương ứng Galois của trường chia đường tròn $\mathbb{Q}(\xi_{12})$ trên \mathbb{Q} . (Xem HD 292)
- 🍰 **9.7.** Làm tương tự cho $\mathbb{Q}(\xi_{13})$. (Xem HD 293)
- 🍰 **9.8.** Cho $E : F$ là một mở rộng hữu hạn. Chứng minh rằng $E = F(\gamma)$ khi và chỉ khi $E : F$ chỉ có hữu hạn các trường trung gian. Suy ra mọi mở rộng hữu hạn và tách được đều là mở rộng đơn. (xem Bài tập 3.8) (Xem HD 293)
- 🍰 **9.9.** Ký hiệu $\overline{\mathbb{F}}_p$ là bao đóng đại số của \mathbb{F}_p . Chứng minh rằng mở rộng $\overline{\mathbb{F}}_p(x, y)$ không phải là mở rộng đơn của $\overline{\mathbb{F}}_p(x^p, y^p)$ bằng cách chỉ ra rằng có vô hạn trường trung gian, (xem bài tập 9.8). (Xem HD 293)

 **9.10.** Cho F là trường có 16 phần tử. Xác định số nghiệm trong F của các đa thức sau đây :


a) $x^3 - 1$;


b) $x^4 - 1$;


c) $x^{15} - 1$;

d) $x^{17} - 1$.

(Xem HD 294)

 **9.11.** Cho F là trường có đặc số khác 2. Chứng minh rằng phương trình $x^2 = -1$ có nghiệm trong F khi và chỉ khi $|F| = 4k + 1$ với $k \in \mathbb{N}$. (Xem HD 294)

 **9.12.** Gọi ζ là một căn nguyên thủy bậc 12 của đơn vị trên \mathbb{Q} . Có bao nhiêu trường trung gian thực sự của mở rộng $\mathbb{Q}(\zeta^3) \subset \mathbb{Q}(\zeta)$? (Xem HD 294)

 **9.13.** Cho F là trường có 81 phần tử. Xác định số nghiệm trong F của các đa thức sau :

a) $x^{80} - 1$;

b) $x^{81} - 1$;

c) $x^{88} - 1$.

(Xem HD 294)

✎ **9.14.** Tìm dạng nhân tử hóa của đa thức $f = x^4 + 1$ trên $\mathbb{F}_5, \mathbb{F}_{25}$ và F_{125} . Xác định trường phân rã của f trong các trường hợp trên.

(Xem HD 294)

§ 10 NHÓM GALOIS CỦA ĐA THỨC

Trong bài này, ta sẽ tính toán nhóm Galois của một số lớp đa thức đặc biệt trên một trường F tùy ý.

10.1 BIỆT THỨC

Cho $f = x^n + a_1x^{n-1} + \cdots + a_0 \in F[x]$ là một đa thức tách được. Gọi $\alpha_1, \dots, \alpha_n$ là tất cả các nghiệm của f . Đặt :

$$D_f = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

gọi là *biệt thức* của f . Kí hiệu

$$\sqrt{D_f} = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

Chú ý rằng $D_f \neq 0$ khi và chỉ khi f không có nghiệm bội. Gọi G_f là nhóm Galois của f trên F và xem G_f là nhóm con của nhóm đối xứng S_n .

Bổ đề 10.1. Cho f xác định như trên và không có nghiệm bội. Với mọi $\sigma \in G_f$,

$$(i) \sigma(\sqrt{D_f}) = \text{sign}(\sigma)\sqrt{D_f};$$

$$(ii) \sigma(D_f) = D_f.$$

Chứng minh. Suy ra trực tiếp từ định nghĩa của đồng cấu sign . □

Mệnh đề 10.2. Cho f như trong bổ đề trên. Gọi E_f là trường phân rã của f trên F . Khi đó :

(i) Biệt thức D_f là một phần tử của F ;

(ii) Trường con của E_f cố định bởi $G_f \cap A_n$ là $F(\sqrt{D_f})$, trong đó A_n là nhóm thay phiên. Suy ra

$$G_f \subset A_n \iff \sqrt{D_f} \in F \iff D_f \text{ chính phương trong } F.$$

Chứng minh. (i) Do D_f cố định bởi mọi phần tử của G_f và $E_f : F$ Galois nên $D_f \in F$.

(ii) Do f chỉ có nghiệm đơn nên $\sqrt{D_f} \neq 0$. Từ bổ đề trên, ta có $\sigma \in G_f$ cố định $\sqrt{D_f}$ khi và chỉ khi $\sigma \in A_n$. Do đó $G_f \cap A_n$ chính là nhóm cố định $F(\sqrt{D_f})$. □

Ví dụ 30. Cho đa thức bậc hai $f = x^2 + bx + c \in F[x]$ tách được. Gọi α_1, α_2 là 2 nghiệm của f . Ta có

$$D_f = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4c.$$

Biệt thức $D_f = 0$ khi và chỉ khi f có nghiệm kép. Nhóm Galois G_f đẳng cấu với nhóm con của S_2 . Nếu D_f chính phương trong F thì $G_f = 1 = A_2$ và $G_f = S_2$ nếu D_f không chính phương trong F .

10.2 NHÓM GALOIS CỦA ĐA THỨC BẬC 3

Trong mục này và mục (10.3) sau, để đơn giản trong biện luận, ta giả thiết F có đặc số khác 2, 3. Khi đó mọi đa thức bậc 2, 3, 4 trên F đều tách được.

Cho $f = x^3 + ax^2 + bx + c \in F[x]$. Thay $x = y - a/3$, ta có đa thức theo y

$$g = y^3 + py + q \in F[y] \tag{3}$$

với

$$p = \frac{1}{3}(3b - a^2), \quad q = \frac{1}{27}(2a^3 - 9ab + 27c).$$

Rõ ràng trường phân rã của f và g trên F là như nhau và biệt thức của chúng cũng trùng nhau. Gọi $\alpha_1, \alpha_2, \alpha_3$ là 3 nghiệm của g . Ta có

$$g = (y - \alpha_1)(y - \alpha_2)(y - \alpha_3).$$

Đạo hàm hình thức của g là :

$$g' = (y - \alpha_1)(y - \alpha_2) + (y - \alpha_2)(y - \alpha_3) + (y - \alpha_1)(y - \alpha_3).$$

Do đó

$$\begin{aligned} g'(\alpha_1) &= (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \\ g'(\alpha_2) &= (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3) \\ g'(\alpha_3) &= (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2). \end{aligned}$$

Như thế

$$D_g = [(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)]^2 = -g'(\alpha_1)g'(\alpha_2)g'(\alpha_3).$$

Mặt khác, từ (3), ta có $g' = 3y^2 + p$. Do đó

$$\begin{aligned} -D_g &= (3\alpha_1^2 + p)(3\alpha_2^2 + p)(3\alpha_3^2 + p) \\ &= 27\alpha_1^2\alpha_2^2\alpha_3^2 + 9p(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) \\ &\quad + 3p^2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + p^3. \end{aligned}$$

Biểu diễn D_g qua các đa thức đối xứng sơ cấp s_1, s_2, s_3 của $\alpha_1, \alpha_2, \alpha_3$ với chú ý rằng $s_1 = 0, s_2 = p, s_3 = -q$, ta có

$$D_g = -4p^3 - 27q^2.$$

Do D_g cũng là biệt thức của f , biểu diễn D_g theo các hệ tử của f , ta có

$$D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc. \quad (4)$$

Nếu f khả quy trên F thì nhóm Galois G_f của nó trùng với nhóm Galois của một đa thức bậc 2 trên F . Ta chỉ cần xét khi f bất khả quy trên F . Khi đó $(G_f : 1) \geq 3$ do đó G_f đẳng cấu với A_3 hoặc với S_3 . Nếu D_f chính phương trong F thì do $G_f \subset A_3$, suy ra $G_f = A_3$. Khi đó trường phân rã $E_g = F(\alpha_i)$ với $i \in \{1, 2, 3\}$. Nếu D_f không chính phương trong F thì $G_f = S_3$ và $E_f = F(\alpha_i, \sqrt{D_f})$ với $i \in \{1, 2, 3\}$.

Ví dụ 31. Cho đa thức $g = x^3 - 4x + 2 \in \mathbb{Q}[x]$. Rõ ràng g bất khả quy và biệt thức $D_g = 4 \cdot 4^3 - 27 \cdot 2^2 = 4 \cdot 37$ không chính phương trong \mathbb{Q} . Do đó nhóm Galois của g là S_3 . Trường phân rã của g trên \mathbb{Q} là $\mathbb{Q}(\sqrt{37}, \alpha)$ với α là một nghiệm của g .

Ví dụ 32. Cho $f = x^3 - 6x^2 + 9x - 1 \in \mathbb{Q}[x]$. Dễ dàng kiểm tra f bất khả quy trên \mathbb{Q} . Biệt thức $D_f = 81 = 9^2$. Do đó nhóm Galois của f là A_3 . Trường phân rã của f là $\mathbb{Q}(\alpha)$ với α là một nghiệm của f . Sử dụng Maple, ta dễ dàng tìm được dạng nhân tử hóa của f trong $\mathbb{Q}(\alpha)$ là

$$f = (x - 4 + 4\alpha - \alpha^2)(x - 2 - 3\alpha + \alpha^2)(x - \alpha).$$

10.3 ĐA THỨC BẬC 4

Cho đa thức $f = x^4 + ax^3 + bx^2 + cx + d \in F[x]$. Bằng cách thay $x = y - a/4$, ta có đa thức theo y

$$g = y^4 + py^2 + qy + r \in F[y],$$

với

$$\begin{aligned} p &= \frac{1}{8}(-3a^2 + 8b) ; \\ q &= \frac{1}{8}(a^3 - 4ab + 8c) ; \\ r &= \frac{1}{256}(-3a^4 + 16a^2b - 64ac + 256d). \end{aligned}$$

Gọi các nghiệm của g là $\alpha_1, \alpha_2, \alpha_3$ và α_4 . Gọi G là nhóm Galois của g (cũng là của f). Nếu g là tích của một đa thức bậc 1 và bậc 3 trên F thì nhóm G đẳng cấu với nhóm Galois của một đa thức bậc 3 đã xác định ở trên. Nếu g là tích của 2 đa thức bất khả quy bậc 2 trên F thì trường phân rã E_g của g trên F là $F(\sqrt{d_1}, \sqrt{d_2})$ với $d_1, d_2 \in F^*$. Nếu $d_1 = a^2 d_2$ với $a \in F$ thì E_g là mở rộng bậc 2 trên F và $G \cong \mathbb{Z}_2$. Nếu không thì $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Bây giờ, ta xét trường hợp g bất khả quy trên F . Khi đó, ta biết rằng, với 2 nghiệm tùy ý α_i, α_j cho trước của g , tồn tại một phần tử $\sigma \in G$ biến α_i thành α_j

(xem 5.5). Những nhóm con của S_4 thỏa mãn tính chất đó là :

$$S_4;$$

$$A_4;$$

$$D_8 = \{1, (1324), (12)(34), (1423), (13)(24), (14)(23), (12), (34)\}$$

và các nhóm con liên hợp $\sigma^{-1}D_8\sigma$ của D_8 (xem Phụ lục A) ;

$$V = \{1, (12)(34), (13)(24), (14)(23)\};$$

$$C_4 = \{1, (1234), (13)(24), (1432)\} \text{ và các nhóm con liên hợp } \sigma^{-1}C_4\sigma \text{ của } C_4.$$

Nhóm Galois G sẽ đẳng cấu với một trong các nhóm trên. Đặt

$$\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$

$$\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$

$$\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3).$$

Ta có

$$\theta_1 + \theta_2 + \theta_3 = 2p$$

$$\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 = p^2 - 4r$$

$$\theta_1\theta_2\theta_3 = -q^2.$$

Suy ra θ_1, θ_2 và θ_3 là 3 nghiệm của

$$h(X) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2. \quad (5)$$

Đa thức (5) gọi là *giải thức bậc 3* của g . Chú ý rằng

$$\begin{aligned} \theta_1 - \theta_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4 \\ &= -(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3). \end{aligned}$$

Tương tự ta có :

$$\begin{aligned} \theta_1 - \theta_3 &= -(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4) \\ \theta_2 - \theta_3 &= -(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4). \end{aligned}$$

Suy ra biệt thức của giải thức (5) trùng với biệt thức của g (do đó trùng với biệt thức của f). Từ công thức tính biệt thức (4), ta có biệt thức của giải thức (5) là :

$$D_h = 16p^4r - 128p^2r^2 + 256r^3 - 4p^3q^2 - 27q^4 + 144pq^2r. \quad (6)$$

Thay các giá trị của p, q, r trong (6), ta có

$$\begin{aligned} D_f &= -6a^2c^2d + b^2a^2c^2 + 144a^2bd^2 - 4a^2b^3d + 144bdc^2 \\ &\quad + 18abc^3 - 192acd^2 + 16b^4d - 128b^2d^2 - 80b^2acd \\ &\quad + 18a^3bcd - 27a^4d^2 + 256d^3 - 4a^3c^3 - 4b^3c^2 - 27c^4. \end{aligned}$$

Sử dụng Maple 6. Trong Maple, ta dễ dàng tính được biệt thức của một đa thức tùy ý với lệnh :

```
>discrim(f,x);
```

Ví dụ, biệt thức của $f = x^4 + ax^3 + bx^2 + cx + d$ có thể tính trực tiếp bằng lệnh :

```
>discrim(x^4+a*x^3+b*x^2+c*x+d,x);
```

$$\begin{aligned} & -6a^2c^2d + b^2a^2c^2 + 144a^2bd^2 - 4a^2b^3d + 144bdc^2 \\ & + 18abc^3 - 192acd^2 + 16b^4d - 128b^2d^2 - 80b^2acd \\ & + 18a^3bcd - 27a^4d^2 + 256d^3 - 4a^3c^3 - 4b^3c^2 - 27c^4 \end{aligned}$$

Trường phân rã của giải thức $h(X)$ chứa trong trường phân rã của f . Do đó nhóm Galois của h là nhóm thương của G . Ta có các trường hợp như sau :

- Nếu h bất khả quy và D_f không chính phương trong F . Khi đó G không chứa trong A_4 và nhóm Galois của h đẳng cấu với S_3 . Do đó cấp của G chia hết cho 6. Suy ra $G = S_4$.
- Nếu h bất khả quy và D_f chính phương trong F . Khi đó $G \subset A_4$ và nhóm Galois của h đẳng cấu với A_3 . Suy ra G có cấp chia hết cho 3. Suy ra $G = A_4$.

- Nếu h khả quy và phân rã thành 3 nhân tử tuyến tính trong $F[X]$. Khi đó θ_1, θ_2 và θ_3 thuộc F . Do đó mọi phần tử G phải cố định chúng. Suy ra $G \subset V$. Vì g bất khả quy nên $G = V$.
- Nếu h phân tích thành 1 đa thức bậc 2 và một đa thức bậc nhất trong $F[X]$. Khi đó có đúng 1 phần tử trong $\{\theta_1, \theta_2, \theta_3\}$ thuộc F . Ta có thể giả thiết $\theta_1 \in F$. Như thế mọi phần tử của G cố định θ_1 nhưng không cố định θ_2 và θ_3 . Suy ra $G \subset D_8$ và $G \not\subset V$. Như thế $G = D_8$ hay $G = C_4$. Chú ý rằng $F(\sqrt{D_f})$ là trường cố định bởi $G \cap A_4$. Ta có $D_8 \cap A_4 = V$ và $C_4 \cap A_4 = \{1, (13)(24)\}$. Chú ý rằng $G \cap A_4$ là nhóm Galois của g trên $F(\sqrt{D_f})$. Do đó nếu g bất khả quy trên $F(\sqrt{D_f})$ thì $G \cap A_4$ có cấp không nhỏ hơn 4, do đó $G = D_8$. Ngược lại, nếu g khả quy trên $F(\sqrt{D_f})$ thì $G = C_4$.

Ví dụ 33. Cho đa thức $f = x^4 + 5x^2 + 5x - 5$. Rõ ràng f bất khả quy trên \mathbb{Q} . Giải thức của f là $h = x^3 - 10x^2 + 45x + 25$ bất khả quy trên \mathbb{Q} . Hơn thế biệt thức của f là -281375 không chính phương. Do đó nhóm Galois của f là S_4 .

Ví dụ 34. Cho đa thức $f = x^4 - 5x^2 - 4 \in \mathbb{Q}[x]$. Kiểm tra f bất khả quy trên \mathbb{Q} .

Giải thức của f là

$$h(x) = x^3 + 10x^2 + 41x = x(x^2 + 10x + 41)$$

khả quy trên \mathbb{Q} . Mặt khác biệt thức của f là $-107584 = -328^2$ không chính phương. Có thể tính trực tiếp nghiệm của f và thấy rằng f không khả quy trên $\mathbb{Q}(i)$. Do đó nhóm Galois của f đẳng cấu với D_8 .

Sử dụng Maple 7. Trong Maple, ta có thể tính trực tiếp nhóm Galois của một đa thức bất khả quy có bậc không quá 9 trên \mathbb{Q} . Cú pháp như ví dụ sau đây :

```
> restart;
```

```
> f:=x^4-5*x^2-4;
```

$$f := x^4 - 5x^2 - 4$$

```
> galois(f);
```

```
“4T3”, {“D(4)”}, “-”, 8, {“(1 3)”, “(1 2 3 4)”}
```

Kết quả tính toán của Maple cho thấy nhóm Galois của $x^4 - 5x^2 - 4$ đẳng cấu với nhóm D_8 , có 8 phần tử và sinh bởi các phép thế $(1\ 3)$ và $(1\ 2\ 3\ 4)$ như nhóm con của nhóm S_4 (trong Maple kí hiệu $D(n)$ cho nhóm đối xứng của n -giác đều).

10.4 ĐA THỨC TỔNG QUÁT

Trong mục này, ta sẽ xét lớp đặc biệt các đa thức gọi là *đa thức tổng quát* và chứng minh rằng nhóm Galois của chúng đẳng cấu với nhóm đối xứng.

Định nghĩa. Một mở rộng E của F gọi là **hữu hạn sinh** nếu $E = F(\alpha_1, \dots, \alpha_n)$.

Định nghĩa. Cho $E : F$ là một mở rộng trường và $t_1, \dots, t_n \in E$. Các phần tử t_1, \dots, t_n gọi là **độc lập đại số** trên F nếu không tồn tại đa thức $f \in F[x_1, \dots, x_n]$ khác 0 sao cho $f(t_1, \dots, t_n) = 0$. Chú ý rằng, khi đó các phần tử t_1, \dots, t_n là siêu việt trên F .

Ví dụ 35. Trong mở rộng $\mathbb{Q}(x, y) : \mathbb{Q}$ các phần tử siêu việt x, y là độc lập đại số trên \mathbb{Q} , trong khi x và x^2 không độc lập đại số.

Bổ đề 10.3. Cho $E : F$ là một mở rộng hữu hạn sinh. Khi đó tồn tại một trường trung gian M sao cho :

- (i) $M = F(\alpha_1, \dots, \alpha_r)$ với $\alpha_1, \dots, \alpha_r$ độc lập đại số trên F ,
- (ii) $E : M$ là mở rộng hữu hạn.

Chứng minh. Gọi $E = F(\beta_1, \dots, \beta_n)$. Nếu tất cả β_1, \dots, β_n đại số trên F thì lấy $M = F$. Nếu tồn tại β_i siêu việt trên F thì ký hiệu nó là α_1 . Nếu $E : F(\alpha_1)$ không hữu hạn thì tồn tại β_j siêu việt trên $F(\alpha_1)$. Đặt $\alpha_2 = \beta_j$. Tiếp tục như vậy cho đến khi tìm được $F(\alpha_1, \dots, \alpha_r) \subset E$ là mở rộng hữu hạn. Khi đó đặt $M = F(\alpha_1, \dots, \alpha_r)$. \square

Bổ đề 10.4 (Stienitz). Với các kí hiệu như trong bổ đề trên, nếu tồn tại một trường trung gian $N = F(\gamma_1, \dots, \gamma_s)$ khác sao cho $\gamma_1, \dots, \gamma_s$ độc lập đại số trên F và $E : N$ hữu hạn thì $r = s$. Số r xác định như thế được gọi là bậc siêu việt của mở rộng trường.

Chứng minh. Do $E : M$ là mở rộng hữu hạn, ta có γ_1 đại số trên $M = F(\alpha_1, \dots, \alpha_r)$. Do đó tồn tại đa thức $f \in F[x_0, \dots, x_r]$ khác 0 sao cho

$$f(\gamma_1, \alpha_1, \dots, \alpha_r) = 0. \quad (7)$$

Không mất tính tổng quát, giả sử α_1 xuất hiện trong biểu diễn (7). Như thế α_1 đại số trên $F(\gamma_1, \alpha_2, \dots, \alpha_r)$ và $E : F(\gamma_1, \alpha_2, \dots, \alpha_r)$ là mở rộng hữu hạn. Nếu $s > r$ thì tiếp tục quá trình trên, các α_i được thay bởi γ_i và mở rộng $E : F(\gamma_1, \dots, \gamma_r)$

hữu hạn. Tuy nhiên điều đó kéo theo γ_{r+1} đại số trên $F(\gamma_1, \dots, \gamma_r)$, vô lí. Vậy $s \leq r$. Tương tự, thay đổi vai trò của s và r , ta có $r \leq s$. Vậy $r = s$. \square

Nhận xét 10.5. Bằng qui nạp ta dễ dàng chứng minh rằng nếu t_1, \dots, t_n độc lập đại số trên F thì $F(t_1, \dots, t_n)$ đẳng cấu với trường các phân thức hữu tỷ r biến $F(x_1, \dots, x_n)$.

Cho F là một trường và t_1, \dots, t_n là các phần tử độc lập đại số trên F . Xét

$$\begin{aligned} E &:= F(t_1, \dots, t_n) \\ &= \left\{ \frac{P(t_1, \dots, t_n)}{Q(t_1, \dots, t_n)} \mid P, Q \in F[t_1, \dots, t_n], Q \neq 0 \right\}. \end{aligned}$$

Mỗi $\sigma \in S_r$ xác định một F -tự đẳng cấu của E định bởi :

$$\frac{P(t_1, \dots, t_n)}{Q(t_1, \dots, t_n)} \mapsto \frac{P(\sigma(t_1), \dots, \sigma(t_n))}{Q(\sigma(t_1), \dots, \sigma(t_n))}.$$

Tương ứng trên là một đơn cấu từ S_n vào $\text{Aut}(E/F)$. Xem S_n như một nhóm con của $\text{Aut}(E/F)$. Ký hiệu N là trường con cố định bởi S_n . Rõ ràng N chứa các đa thức đối xứng, đặc biệt chứa các đa thức đối xứng sơ cấp s_1, \dots, s_n . Nhắc lại,

các đa thức đối xứng sơ cấp được định nghĩa như sau :

$$\begin{aligned} s_1 &= t_1 + \cdots + t_n ; \\ s_2 &= \sum_{1 \leq i < j \leq n} t_i t_j = t_1 t_2 + \cdots + t_{n-1} t_n ; \\ s_3 &= \sum_{1 \leq i < j < k \leq n} t_i t_j t_k ; \\ &\dots \\ s_n &= t_1 \cdots t_n. \end{aligned}$$

Ta có kết quả sau :

Định lí 10.6. $N = F(s_1, \dots, s_n)$.

Chứng minh. Ta có $[F(t_1, \dots, t_n) : N] = (S_n : 1) = n!$ theo Định lí Artin. Ta chứng minh rằng

$$[F(t_1, \dots, t_n) : F(s_1, \dots, s_n)] \leq n!$$

và từ nhận xét $F(s_1, \dots, s_n) \subset N$, suy ra điều phải chứng minh.

Xét các mở rộng:

$$F(s_1, \dots, s_n) \subset F(s_1, \dots, s_n, t_n) \subset F(t_1, \dots, t_n).$$

Ta có t_n là nghiệm của

$$X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n \in F(s_1, \dots, s_n)[X].$$

Do đó $[F(s_1, \dots, s_n, t_n) : F(s_1, \dots, s_n)] \leq n$.

Gọi s'_1, \dots, s'_{n-1} là các đa thức đối xứng sơ cấp của các biến t_1, \dots, t_{n-1} . Rõ ràng $s_j = s'_{j-1} t_n + s'_j$ với mọi $1 \leq j \leq n$. Do đó

$$F(s_1, \dots, s_n, t_n) = F(s'_1, \dots, s'_{n-1}, t_n).$$

Bằng quy nạp, ta có

$$\begin{aligned} [F(t_1, \dots, t_n) : F(s_1, \dots, s_n, t_n)] \\ = [F(t_n)(t_1, \dots, t_{n-1}) : F(t_n)(s'_1, \dots, s'_{n-1})] \leq (n-1)! \end{aligned}$$

và suy ra điều phải chứng minh. \square

Mệnh đề 10.7. Với các kí hiệu như trên, các phần tử s_1, \dots, s_n là độc lập đại số trên F .

Chứng minh. Do $[F(t_1, \dots, t_n) : F(s_1, \dots, s_n)] = n!$ nên bậc siêu việt của chúng trên F là như nhau. Do đó s_1, \dots, s_n độc lập đại số trên F . \square

Cho F là một trường và s_1, \dots, s_n là các phần tử độc lập đại số trên F . Đa thức

Định nghĩa.

$$g = t^n - s_1 t^{n-1} + \dots + (-1)^n s_n \in F(s_1, \dots, s_n)[t] \quad (8)$$

gọi là **đa thức tổng quát bậc n trên F** .

Định lý 10.8. Cho F là một trường và g là đa thức tổng quát (8) trên F . Gọi E_g là trường phân rã của g trên $F(s_1, \dots, s_n)$. Khi đó các nghiệm t_1, \dots, t_n của g độc lập đại số trên F và nhóm Galois của $E_g : F(s_1, \dots, s_n)$ là S_n .

Chứng minh. Ta có $E_g = F(t_1, \dots, t_n)$. Do $E_g : F(s_1, \dots, s_n)$ là mở rộng hữu hạn nên bậc siêu việt của E_g trên F bằng với bậc siêu việt của $F(s_1, \dots, s_n)$ trên F , tức bằng n . Suy ra đa thức (8) tách được nên mở rộng $E_g : F(s_1, \dots, s_n)$ là mở rộng Galois. Mặt khác, các phần tử t_1, \dots, t_n là độc lập đại số và s_1, \dots, s_n là các đa thức đối xứng sơ cấp của chúng. Theo Định lý 10.6 và tương ứng Galois, nhóm Galois của mở rộng $E_g : F(s_1, \dots, s_n)$ chính là S_n . \square

Bài tập

 **10.1.** Chọn đúng, sai cho các mệnh đề sau :

- a) Biệt thức của một đa thức $f \in F[x]$ là một phần tử của F .
- b) Nhóm Galois của một đa thức bậc $n > 0$ là một nhóm con của S_n .
- c) Nhóm Galois của một đa thức bậc 2 tách được trên F là một nhóm cyclic.
- d) Nhóm Galois của đa thức bậc 3 khả quy, tách được trên F là một nhóm cyclic.
- e) Nhóm Galois của một đa thức bậc 3 tách được có biệt thức chính phương là một nhóm cyclic.
- f) Nhóm Galois của một đa thức bậc 3 tách được có biệt thức không chính phương đẳng cấu với S_3 .
- g) Nhóm Galois của một đa thức bậc 3 bất khả quy, tách được có biệt thức không chính phương đẳng cấu với S_3 .

- h) Tồn tại đa thức bậc 4 trên \mathbb{Q} có nhóm Galois đẳng cấu với một nhóm con của S_4 .
- i) Tồn tại một đa thức bậc 3 bất khả quy trên \mathbb{Q} có 3 nghiệm thực.
- j) Một đa thức bậc 3 trên \mathbb{Q} có nhóm Galois đẳng cấu với A_3 thì có 3 nghiệm thực.
- k) Biệt thức của đa thức bậc 4 và của giải thức bậc 3 của nó là như nhau.
- l) Đa thức tổng quát bậc n trên F có các hệ tử thuộc F .
- m) Mọi mở rộng hữu hạn sinh đều là mở rộng hữu hạn.
- n) Mọi mở rộng đại số, hữu hạn sinh đều là mở rộng hữu hạn.
- o) Mọi mở rộng hữu hạn sinh đều là mở rộng đại số.
- p) Các phần tử độc lập đại số trên F thì siêu việt trên F .
- q) Các phần tử siêu việt trên F thì độc lập đại số. (Xem HD 295)

✎ **10.2.** Hãy tìm dạng nhân tử hóa của đa thức $f = x^3 - 4x + 2 \in \mathbb{Q}[x]$ (xem Ví dụ 31) trong $\mathbb{Q}(\alpha, \sqrt{37})$ bằng Maple, với α là một nghiệm của f . (Xem HD 295)

✎ **10.3.** Xác định nhóm Galois của các đa thức sau đây trên trường \mathbb{Q} :

- a) $-x^3 - 3x^2 + 4x - 1$; b) $x^3 + 2x^2 - 2x - 2$;
 c) $7x^3 + 10x^2 + 5x + 1$; d) $x^3 + x - 1$;
 e) $x^3 - 2x - 2$; f) $3x^3 - 3x + 1$;
 g) $x^3 - 3x + 1$; h) $x^3 + 2x^2 - 2x - 2$. (Xem HD 295)

✎ **10.4.** Xác định nhóm Galois của các đa thức sau đây trên trường \mathbb{Q} .

- a) $x^4 - x^2 + 4x + 5$; b) $x^4 + x^2 + 3x + 5$;
 c) $x^4 + 3x + 1$; d) $x^4 - 4x^2 - 4x - 2$;
 e) $x^4 - 4x - 2$; f) $x^4 + 2x^2 - 4$;
 g) $x^4 - x^3 - 3x + 4$; h) $x^4 + 2x^3 + 2x^2 - 4x + 2$;
 i) $x^4 - 4x^3 + 5x^2 - 2x + 1$; j) $x^4 + 2x^2 + 4$. (Xem HD 296)

✎ **10.5.** Có thể nói gì về nhóm Galois của đa thức $f = x^4 + ax^2 + b \in F[x]$ bất khả quy và F có đặc số khác 2, 3 ? (Xem HD 298)

✎ **10.6.** Cho $f \in F[x]$ bất khả quy và F là trường có đặc số khác 2,3. Gọi h là giải thức bậc 3 của f và M là trường phân rã của h trên F . Kí hiệu D_f là biệt thức của

f và G_f là nhóm Galois của f . Chứng minh rằng :

- a) $G_f = S_4$ khi và chỉ khi h bất khả quy trên F và D_f không chính phương trong F ;
- b) $G_f = A_4$ khi và chỉ khi h bất khả quy trên F và D_f chính phương trong F ;
- c) $G_f = D_8$ khi và chỉ khi h khả quy trên F , D_f không chính phương trong F và f bất khả quy trên M ;
- d) $G_f = V$ khi và chỉ khi h khả quy và D_f chính phương trong F ;
- e) $G_f = C_4$ khi và chỉ khi h khả quy trên F , D_f không chính phương trong F và f khả quy trên M . (Xem HD 298)

✎ **10.7.** Cho F là trường hữu hạn và $f = x^3 + ax + b \in F[x]$. Chứng minh rằng nếu f bất khả quy trên F thì $-4a^3 - 27b^2$ chính phương trong F . (Xem HD 298)

§ 11 TIÊU CHUẨN GIẢI ĐƯỢC BẰNG CĂN THỨC CỦA ĐA THỨC

11.1 MỞ RỘNG CĂN VÀ TIÊU CHUẨN GIẢI ĐƯỢC

Ta biết rằng các nghiệm của đa thức $f = x^2 + px + q \in \mathbb{Q}[x]$ là $\frac{-p \pm \sqrt{p^2 - 4q}}{2}$ nằm trong mở rộng trường $\mathbb{Q}(\sqrt{\Delta})$ với $\Delta = p^2 - 4q$.

Cho đa thức bậc ba $g = x^3 + px + q \in \mathbb{Q}[x]$. Nghiệm của g cho bởi công thức Cardano. (Ta sẽ kiểm chứng công thức Cardano ở phần cuối của tiết này).

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

Xét các mở rộng $\mathbb{Q} = E_0 \subset E_1 \subset E_2 \subset E_3$, trong đó:

- $E_1 := E_0(\alpha_1)$ với $\alpha_1^2 = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 \in E_0$;
- $E_2 := E_1(\alpha_2)$ với $\alpha_2^3 = -\frac{q}{2} + \alpha_1 \in E_1$;
- $E_3 := E_2(\alpha_3) = E(\alpha_1, \alpha_2, \alpha_3)$ với $\alpha_3^3 = -\alpha_2^3 - q \in K_2$.

Khi đó $\alpha = \alpha_2 + \alpha_3 \in E_3$. Ta nói rằng $E_3 : \mathbb{Q}$ là một mở rộng căn. Ta có định nghĩa sau đây :

Định nghĩa. Một mở rộng $F \subset E$ gọi là một mở rộng căn nếu $E = F(\alpha_1, \dots, \alpha_m)$ sao cho với mọi $i = 1, \dots, m$ tồn tại n_i thỏa $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$. Khi đó ta cũng nói E là một mở rộng căn của F . Ta nói các phần tử α_i tạo ra một chuỗi căn cho mở rộng $F \subset E$.

Định nghĩa. Một phần tử α thuộc vào một mở rộng căn $E : F$ thì gọi là biểu diễn được bằng căn thức (trên F).

Định nghĩa. Một đa thức f trên F được gọi là giải được bằng căn thức (trên F) nếu trường phân rã của f nằm trong một mở rộng căn của F .

Như thế, một đa thức giải được bằng căn thức trên F nếu mọi nghiệm của nó được biểu diễn qua hữu hạn các phép toán cộng, trừ, nhân, chia và lấy căn các phần tử của F . Khi đó ta cũng nói các nghiệm của f là nghiệm căn thức trên F .

Ta nhắc lại kết quả đã biết trong § 9.

Bổ đề 11.1. Cho $f = x^n - 1 \in F[x]$ với n không chia hết cho đặc số của F . Gọi E_f là trường phân rã của f trên F . Khi đó $E_f : F$ là mở rộng Galois và $\text{Gal}(E_f/F)$ là một nhóm aben.

Chứng minh. Xem Mệnh đề 9.10 □

Định nghĩa. Một mở rộng Galois $E : F$ gọi là mở rộng aben (cyclic) nếu nhóm $\text{Gal}(E/F)$ là nhóm aben (cyclic).

Kết quả trên cho thấy rằng mọi trường chia đường tròn là một mở rộng aben.

Bổ đề 11.2. Cho $0 \neq n \in \mathbb{N}$, cho F là trường có đặc số không chia hết n và F chứa một căn nguyên thủy bậc n của đơn vị. Cho $a \in F$ và E là trường phân rã của đa thức $x^n - a$ trên F . Khi đó nhóm Galois của $E : F$ là một nhóm cyclic có cấp là ước của n .

Chứng minh. Gọi $\xi_n \in F$ là một căn nguyên thủy bậc n của đơn vị. Gọi α là một nghiệm của $x^n - a$. Khi đó tất cả các nghiệm của $x^n - a$ là $\xi_n^i \alpha$ với $i = 1, \dots, n$. Như thế trường phân rã của $x^n - a$ trên F là $E = F(\alpha)$. Gọi $C_n \subset E$ là nhóm

cyclic các căn bậc n của đơn vị. Xét đồng cấu

$$\begin{aligned} \psi : \text{Gal}(F(\alpha)/F) &\longrightarrow C_n \\ \sigma &\longmapsto \frac{\sigma(\alpha)}{\alpha}. \end{aligned}$$

Dễ dàng thấy rằng ψ là đơn cấu, do đó $\text{Gal}(E/F)$ là nhóm cyclic có cấp là ước của n . □

Định nghĩa.

Cho $E : F$ là một mở rộng đại số. Một bao đóng chuẩn tắc của $E : F$ là một mở rộng N của E sao cho :

- $N : F$ là mở rộng chuẩn tắc;
- Nếu $E \subset M \subset N$ và $M : F$ chuẩn tắc thì $M = N$.

Có thể nói bao đóng chuẩn tắc N chính là mở rộng chuẩn tắc nhỏ nhất của F chứa E .

Bổ đề 11.3. Mọi mở rộng hữu hạn đều tồn tại duy nhất (sai khác đẳng cấu) một bao đóng chuẩn tắc.

Chứng minh. Gọi $\{\alpha_1, \dots, \alpha_r\}$ là một cơ sở của $E : F$. Lấy N là trường phân rã của $\prod_1^r m_i$ trên F với m_i là đa thức tối tiểu của α_i với $i = 1, \dots, r$. Rõ ràng $N : F$ là mở rộng chuẩn tắc và $E \subset N$. Nếu có $E \subset M$ sao cho $M : F$ chuẩn tắc, khi đó $\prod_1^r m_i$ phân rã trong M nên $N \subset M$. Suy ra nếu M là một bao đóng chuẩn tắc của $E : F$ thì $M \cong N$. \square

Ví dụ 36. Bao đóng chuẩn tắc của một mở rộng hữu hạn, tách được là một mở rộng Galois.

Ví dụ 37. Cho $E : F$ là một mở rộng Galois và M là một trường trung gian của mở rộng. Khi đó bao đóng chuẩn tắc của M là trường hợp thành của σM , với mọi $\sigma \in G$, tức là $\prod_{\sigma \in G} \sigma M$ (xem Nhận xét 8.2).

Định lí 11.4. Nếu đa thức f giải được bằng căn thức trên trường F có đặc số 0 thì nhóm Galois của f là nhóm giải được.

Chứng minh. Do f giải được bằng căn thức trên F nên tồn tại chuỗi các mở rộng

$$F = E_0 \subset E_1 \subset \dots \subset E_m$$

sao cho $E_i = E_{i-1}(\alpha_i)$ thỏa $\alpha_i^{n_i} \in E_{i-1}$, $\forall i = 1, \dots, m$ và E_m chứa trường phân rã của f . Đặt $n = n_1 \cdots n_m$. Gọi Ω là một mở rộng Galois của F chứa E_m và chứa một căn nguyên thủy ξ_n của đơn vị. (Một mở rộng Ω như thế tồn tại. Chẳng hạn, biểu diễn $E_m = F(\gamma)$, gọi $g \in F[x]$ là đa thức tối tiểu của γ . Lấy Ω là trường phân rã của $g(x^n - 1)$ trên F).

Gọi $G = \{\sigma_1, \dots, \sigma_r\}$ là nhóm Galois của $\Omega : F$ và $K \subset \Omega$ là bao đóng chuẩn tắc của $E_m(\xi_n) : F$. Khi đó (xem Ví dụ 37), ta có K là trường hợp thành của $\sigma_i E_m(\xi_n)$ với mọi $\sigma_i \in G$. Như thế K là trường sinh bởi

$$\xi_n, \alpha_1, \dots, \alpha_m, \sigma_1 \alpha_1, \dots, \sigma_2 \alpha_1, \dots, \sigma_r \alpha_1, \dots$$

trên F . Ghép thêm các phần tử của dãy trên vào F theo thứ tự, ta có chuỗi các mở rộng trường

$$F \subset F(\xi_n) \subset F(\xi_n, \alpha_1) \subset \dots \subset L \subset L' \subset \dots \subset K.$$

Ta nhận thấy rằng mỗi mở rộng $L \subset L'$ của chuỗi trên thỏa mãn L' được sinh ra trên L bởi một phần tử β_i thỏa $\beta_i^r \in L$, với $r \in \{n_1, \dots, n_m, n\}$. Do đó theo (11.1) và (11.2), chúng là các mở rộng aben. Theo tương ứng Galois, chuỗi các mở rộng

trên ứng với chuỗi các nhóm con của nhóm Galois $G' = \text{Gal}(K/F)$

$$1 = G_0 \subset G_1 \subset \dots \subset G_t = G'$$

sao cho $G_i \triangleleft G_{i+1}$ và G_{i+1}/G_i aben. Do đó G' là nhóm giải được. Xét các mở rộng $F \subset E_f \subset K$ với E_f là trường phân rã của f trên F . Vì nhóm Galois của f là nhóm thương của G' , theo tính chất của nhóm giải được (A.4), nhóm G_f cũng giải được. \square

Để chứng minh điều ngược lại của định lí trên, ta cần một số bổ đề như sau :

Bổ đề 11.5. Cho $f \in F$ tách được và $F \subset E$ là mở rộng trường. Khi đó nhóm Galois của f trên E là nhóm con của nhóm Galois của f trên F .

Chứng minh. Gọi $R = \{\alpha_1, \dots, \alpha_n\}$ là tập các nghiệm của f . Kí hiệu $K = F(\alpha_1, \dots, \alpha_n)$ và $L = E(\alpha_1, \dots, \alpha_n)$ lần lượt là trường phân rã của f trên F và trên E . Rõ ràng $K \subset L$. Mỗi $\sigma \in \text{Gal}(L/E)$ hoán vị các phần tử trong R , do đó biến K thành K . Nói cách khác, phép hạn chế $\sigma \mapsto \sigma|_K$ là một đồng cấu từ $\text{Gal}(L/E)$ vào $\text{Gal}(K/F)$. Rõ ràng phép hạn chế đó là một đơn cấu nên $\text{Gal}(L/E)$ là một nhóm con của $\text{Gal}(K/F)$. \square

Bổ đề sau chỉ ra một phần tính đảo ngược của (11.2) :

Bổ đề 11.6. Cho p là một số nguyên tố, cho F là trường có đặc số khác p và F chứa một căn nguyên thủy bậc p của đơn vị. Nếu $E : F$ là mở rộng cyclic bậc p thì $E = F(\alpha)$ với $\alpha^p \in F$.

Chứng minh. Gọi $z_1, \dots, z_p \in F$ là các căn bậc p phân biệt của đơn vị. Lấy $\beta \in E \setminus F$, ta có $E = F(\beta)$. Gọi σ là phần tử sinh của nhóm cyclic $G = \text{Gal}(E/F)$. Đặt $\beta_i = \sigma^{i-1}(\beta)$, với $i = 1, \dots, p$. Ta có $\beta_i \neq \beta_j$ với mọi $i \neq j$. Khi đó $\beta_1 = \beta$, $\beta_{i+1} = \sigma(\beta_i)$ nếu $i = 1, \dots, p-1$ và $\sigma(\beta_p) = \beta_1$. Đặt

$$d_i(\beta) = \beta_1 + z_i\beta_2 + \dots + z_i^{p-1}\beta_p, \quad i = 1, \dots, p.$$

gọi là *giải thức Lagrange*. Khi đó

$$\sigma(d_i) = \beta_2 + z_i\beta_3 + \dots + z_i^{p-1}\beta_1 = z_i^{-1}d_i.$$

Do đó $\sigma(d_i^p) = \sigma(d_i)^p = d_i^p$. Suy ra $d_i^p \in F$.

Mặt khác, xét hệ phương trình tuyến tính

$$d_i = x_1 + z_ix_2 + \dots + z_i^{p-1}x_p, \quad i = 1, \dots, p.$$

Ma trận hệ số

$$\begin{pmatrix} 1 & z_1 & \cdots & z_1^{p-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & z_p & \cdots & z_p^{p-1} \end{pmatrix}$$

có định thức $\prod_{0 < i < j \leq p} (z_j - z_i) \neq 0$, do đó β_i , với $1 \leq i \leq p$, là một tổ hợp tuyến tính của d_1, \dots, d_p với hệ tử trong F (chú ý rằng F chứa z_1, \dots, z_p). Suy ra $E = F(\beta) = F(d_1, \dots, d_p)$. Rõ ràng tồn tại $d_i \in E \setminus F$. Khi đó $E = F(d_i)$ và $d_i^p \in F$. \square

Bây giờ ta chứng minh kết quả ngược lại của (11.4).

Định lý 11.7. Nếu nhóm Galois của đa thức f trên trường có đặc số 0 giải được thì f giải được bằng căn thức trên F .

Chứng minh. Gọi G_f là nhóm Galois của f trên F . Gọi $n = \deg(f)$ và kí hiệu $E = F(\xi_n)$ với ξ_n là một căn nguyên thủy bậc n của đơn vị. Theo (11.5), nhóm Galois G của f trên E là nhóm con của G_f , do đó G giải được.

Theo (A.7), tồn tại chuỗi các nhóm con

$$G = G_m \supset \dots \supset G_0 = 1 \quad (9)$$

sao cho $G_i \triangleleft G_{i+1}$ và G_{i+1}/G_i cyclic có cấp nguyên tố p_i , với mọi $i = 0, \dots, m-1$. Gọi K là trường phân rã của f trên E . Khi đó K chứa trường phân rã của f trên F .

Chuỗi các nhóm con (9) cho ta chuỗi các mở rộng

$$F \subset F(\xi_n) = E = E_0 \subset E_1 \subset \dots \subset E_m = K$$

với $E_i : E_{i-1}$ cyclic bậc p_i , với mọi $i = 0, \dots, m$. Theo Bổ đề 11.6, ta có $E_i = E_{i-1}(\alpha_i)$ với $\alpha_i^{p_i} \in E_{i-1}$, với mọi $i = 0, \dots, m$. Như thế $K : F$ là một mở rộng căn chứa trường phân rã của f trên F , nên f giải được bằng căn thức trên F . \square

Hệ quả 11.8. Cho F là trường có đặc số 0. Một đa thức trên F giải được bằng căn thức khi và chỉ khi nhóm Galois của nó là giải được.

Hệ quả 11.9. Cho F là trường có đặc số 0. Đa thức tổng quát (8) không giải được bằng căn thức trên $F(s_1, \dots, s_n)$ khi và chỉ khi $n \geq 5$.

11.2 TÍNH KHÔNG GIẢI ĐƯỢC CỦA ĐA THỨC CÓ BẬC LỚN HƠN BỐN

Ta cần một kết quả của nhóm đối xứng, tương tự như (0.18).

Bổ đề 11.10. Nếu một nhóm con của nhóm đối xứng S_p với p nguyên tố chứa một vòng xích độ dài p và một phép chuyển trí thì trùng với S_p .

Chứng minh. Gọi G là nhóm con của S_p sinh bởi $\sigma = (a_1 \cdots a_p)$ là một vòng xích có độ dài p và $\tau = (i j)$ là một phép chuyển trí. Bằng cách đánh số lại nếu cần thiết, ta có thể giả thiết $\tau = (1 2)$. Viết lại σ dưới dạng $\sigma = (1 a_2 \cdots a_p)$. Lấy lũy thừa thích hợp của σ , ta có được kết quả là $(1 2 b_3 \cdots b_p)$, đó cũng là một vòng xích độ dài p do p nguyên tố. Giữ nguyên 1 và 2, đánh số lại các phần tử của tập $\{3, 4, \dots, p\}$, suy ra nhóm con G chứa $\tau = (1 2)$ và vòng xích $(1 2 \cdots p)$. Theo (0.18), ta có $G = S_p$. \square

Mệnh đề 11.11. Cho một đa thức $f \in \mathbb{Q}[x]$ bất khả quy có bậc p nguyên tố. Nếu f có đúng 2 nghiệm không thực trong \mathbb{C} thì nhóm Galois của f là nhóm đối xứng S_p .

Chứng minh. Gọi E_f là trường phân rã của f trên \mathbb{Q} và $G = \text{Gal}(E_f : \mathbb{Q})$ xem như nhóm con của S_p . Gọi $\alpha \in E_f$ là một nghiệm của f . Do $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset E_f$ và

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$, ta có p là ước của $[E_f : \mathbb{Q}] = (G : 1)$. Suy ra G chứa một phần tử cấp p , xem (B.2). Trong S_p chỉ có các vòng xích độ dài p có cấp p , (xem 0.16). Như thế G chứa một vòng xích độ dài p . Mặt khác E_f là một trường con của \mathbb{C} . Trong $\text{Aut}(\mathbb{C}/\mathbb{Q})$, xét phép liên hợp $a + bi \mapsto a - bi$. Vì f có đúng 2 nghiệm không thực r_1, r_2 , chúng là các số phức liên hợp. Khi đó phép liên hợp hoán vị 2 nghiệm r_1, r_2 và cố định các nghiệm còn lại của f . Do đó hạn chế của phép liên hợp trên E_f xác định một phép chuyển trí của G . Theo (11.10), ta có $G = S_p$. \square

Hệ quả 11.12. Đa thức $f = x^5 - 4x^2 + 2 \in \mathbb{Q}[x]$ không giải được bằng căn thức.

Chứng minh. Đa thức f bất khả quy trên \mathbb{Q} do tiêu chuẩn Eisenstein cho $p = 2$. Ta có

$$f(-1) = -3; f(0) = 2; f(1) = -1; f(2) = 18.$$

Do đó f có ít nhất 3 nghiệm thực nằm trong $(-1, 0), (0, 1)$ và $(1, 2)$. Mặt khác, do $f' = 5x^4 - 8x = x(5x^3 - 8)$, có đúng 2 nghiệm thực là $x = 0$ và $x = \sqrt[3]{8/5}$. Do đó f có đúng 3 nghiệm thực. Theo (11.11), đa thức f có nhóm Galois đẳng cấu với S_5 là một nhóm không giải được (A.9). Do đó f không giải được bằng căn thức trên \mathbb{Q} . \square

11.3 NGHIỆM CĂN THỨC CỦA CÁC ĐA THỨC TỔNG QUÁT CÓ BẬC KHÔNG QUÁ 4

Trong phần này, ta trình bày nghiệm căn thức của đa thức tổng quát (8) (xem trang 196) với $n \leq 4$. Hiển nhiên, khi s_1, \dots, s_n lấy giá trị trong F thì ta sẽ có nghiệm căn thức của các đa thức trên F . Để đơn giản, ta giả thiết F có đặc số 0.

Đa thức tổng quát bậc 2

Cho $g = t^2 - s_1 t + s_2$ có nhóm Galois trên $F(s_1, s_2)$ là $S_2 = \{1, (12)\}$. Phần tử $(1, 2)$ hoán vị t_1, t_2 nên cố định $(t_1 - t_2)^2$. Do đó $(t_1 - t_2)^2 \in F(s_1, s_2)$. Cụ thể $(t_1 - t_2)^2 = s_1^2 - 4s_2$. Kí hiệu $\sqrt{s_1^2 - 4s_2}$ là một nghiệm của $x^2 - (s_1^2 - 4s_2)$, ta có $t_1 - t_2 = \sqrt{s_1^2 - 4s_2}$ và $t_1 + t_2 = s_1$. Suy ra công thức nghiệm quen thuộc:

$$\begin{cases} t_1 = \frac{1}{2}(s_1 + \sqrt{s_1^2 - 4s_2}) \\ t_2 = \frac{1}{2}(s_1 - \sqrt{s_1^2 - 4s_2}). \end{cases}$$

Đa thức tổng quát bậc 3

Cho $g = t^3 - s_1 t^2 + s_2 t - s_3$ có nhóm Galois trên $F(s_1, s_2, s_3)$ là S_3 . Ta có dãy các nhóm con chuẩn tắc $1 \triangleleft A_3 \triangleleft S_3$ có thương là các nhóm cyclic. Đặt $\omega = e^{2\pi i/3}$

và $y = t_1 + \omega t_2 + \omega^2 t_3$, với t_1, t_2, t_3 là các nghiệm của g . Với mọi $\sigma \in A_3$, tồn tại $0 \leq i \leq 2$ sao cho $\sigma(y) = \omega^i y$. Nên $\sigma(y^3) = y^3$. Tương tự, đặt $z = t_1 + \omega^2 t_2 + \omega t_3$ thì ta có $\sigma(z^3) = z^3$, $\forall \sigma \in A_3$. Mặt khác, với σ là một phép thế lẻ thì $\sigma(y^3) = z^3$. Nói cách khác các phần tử $y^3 + z^3$ và $y^3 z^3$ bất biến với S_3 . Do đó $y^3 + z^3$ và $y^3 z^3$ thuộc $F(s_1, s_2, s_3)$. Như thế y^3 và z^3 là nghiệm của cùng một đa thức bậc 2 trên $F(s_1, s_2, s_3)$. Mặt khác, dễ dàng thấy rằng:

$$\begin{cases} t_1 = \frac{1}{3}(s_1 + y + z) \\ t_2 = \frac{1}{3}(s_1 + \omega^2 y + \omega z) \\ t_3 = \frac{1}{3}(s_1 + \omega y + \omega^2 z). \end{cases}$$

Do đó, khi đã giải được y^3 và z^3 , ta có nghiệm của g . Thực ra, ta có thể tính toán trực tiếp $yz = s_1^2 - 3s_2$ và $y^3 + z^3 = 2s_1^3 - 9s_1 s_2 + 27s_3$.

Trong thực hành, ta thường giải bằng cách đặt $u = t - \frac{1}{3}s_1$. Khi đó ta có đa thức bậc 3 theo u là $f = u^3 + pu + q$ với

$$p = s_2 - \frac{1}{3}s_1^2, \quad q = -\frac{2}{27}s_1^3 + \frac{1}{3}s_1 s_2 - s_3 \in F(s_1, s_2, s_3).$$

Do đó $y^3 + z^3 = -27q$ và $y^3 z^3 = -27p^3$. Khi đó y^3 và z^3 là 2 nghiệm của

$X^2 + 27qX - 27p^3 = 0$. Từ đó,

$$y = 3\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}, \quad z = 3\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

sao cho $yz = -3p$. Ta nhận lại công thức nghiệm Cardano

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} \quad (10)$$

và 3 nghiệm của f cho bởi

$$\begin{cases} u_1 = \frac{1}{3}(y + z) \\ u_2 = \frac{1}{3}(\omega^2 y + \omega z) \\ u_3 = \frac{1}{3}(\omega y + \omega^2 z). \end{cases}$$

Nhận xét 11.13. Trong công thức (10), thay $D = -4p^3 - 27q^2$ là biệt thức của $f = u^3 + pu + q$, ta có công thức nghiệm cho bởi

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{-D}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{-D}{27}}}. \quad (11)$$

Ví dụ 38. Tìm nghiệm căn thức của $f = x^3 - x + 1 \in \mathbb{Q}[x]$. Ta có $D = -23$. Do đó một nghiệm của f là

$$\sqrt[3]{-\frac{1}{2} + \frac{1}{18}\sqrt{69}} + \sqrt[3]{-\frac{1}{2} - \frac{1}{18}\sqrt{69}}.$$

Hai nghiệm còn lại là 2 số phức liên hợp.

Ví dụ 39. Cho đa thức $f = x^3 - 6x^2 + 9x - 1$. Thay $x = u + 2$, ta có đa thức theo u là $g = u^3 - 3u + 1$. Biệt thức của nó là $D = 81$. Một nghiệm biểu diễn bằng căn thức của g là

$$\sqrt[3]{-\frac{1}{2} + \frac{1}{2}\sqrt{-3}} + \sqrt[3]{-\frac{1}{2} - \frac{1}{2}\sqrt{-3}}.$$

Chú ý rằng trong trường hợp này, đa thức g cũng như f đều có 3 nghiệm thực. Tuy nhiên để biểu diễn bằng căn thức, các biểu diễn nghiệm cần phải dùng đến các căn của số phức.

Sử dụng Maple 8. Maple cho chúng ta nghiệm căn thức của một đa thức bậc 3 tùy ý bằng lệnh `> solve(f);` với f là một đa thức bậc 3.

Đa thức tổng quát bậc 4

Cho $g = t^4 - s_1 t^3 + s_2 t^2 - s_3 t + s_4$. Nhóm Galois S_4 của g có dãy các nhóm con chuẩn tắc

$$1 \triangleleft V \triangleleft A_4 \triangleleft S_4 \text{ với } V = \{1, (12)(34), (13)(24), (14)(23)\}.$$

Đặt

$$y_1 = (t_1 + t_2)(t_3 + t_4),$$

$$y_2 = (t_1 + t_3)(t_2 + t_4),$$

$$y_3 = (t_1 + t_4)(t_2 + t_3).$$

Vì các đa thức đối xứng sơ cấp của y_1, y_2, y_3 thuộc $F(s_1, s_2, s_3, s_4)$ nên y_1, y_2, y_3 là nghiệm của một đa thức bậc 3 trên $F(s_1, s_2, s_3, s_4)$, gọi là **giải thức bậc 3** của g .

Khi đã giải được y_1, y_2, y_3 , cùng với $t_1 + t_2 + t_3 + t_4 = s_1$, suy ra các cặp $(t_1 + t_2, t_3 + t_4); (t_1 + t_3, t_2 + t_4); (t_1 + t_4, t_2 + t_3)$ là nghiệm của các đa thức bậc 2 có hệ tử trong $F(s_1, s_2, s_3, s_4, y_1, y_2, y_3)$. Từ đó giải được t_1, t_2, t_3, t_4 .

Trong thực hành, ta đặt $u = t - \frac{1}{4}s_1$ thì ta có một đa thức bậc 4 theo u :

Từ đó tính được :

$$\begin{aligned}y_1 + y_2 + y_3 &= 2p ; \\ y_1y_2 + y_1y_3 + y_2y_3 &= p^2 - 4r ; \\ y_1y_2y_3 &= -q^2.\end{aligned}$$

Suy ra giải thức của $f(u)$ là

$$X^3 - 2pX^2 + (p^2 - 4r)X + q^2.$$

Các nghiệm của f cho bởi :

$$\left\{ \begin{array}{l} u_1 = \frac{1}{2}(\sqrt{-y_1} + \sqrt{-y_2} + \sqrt{-y_3}) \\ u_2 = \frac{1}{2}(\sqrt{-y_1} - \sqrt{-y_2} - \sqrt{-y_3}) \\ u_3 = \frac{1}{2}(-\sqrt{-y_1} + \sqrt{-y_2} - \sqrt{-y_3}) \\ u_4 = \frac{1}{2}(-\sqrt{-y_1} - \sqrt{-y_2} - \sqrt{-y_3}) \end{array} \right.$$

với các căn thức được chọn sao cho $\sqrt{-y_1} \cdot \sqrt{-y_2} \cdot \sqrt{-y_3} = -q$.

Sử dụng Maple 9. Trong Maple, nghiệm căn thức của một đa thức bậc 4, theo ngầm định, không được hiển thị trên màn hình, do tính phức tạp của công thức nghiệm.


```
> restart;  
> solve(x^4+x^3-9);
```

Maple hiển thị nghiệm dưới dạng `RootOf` và dễ dàng nhận được nghiệm gần đúng.

```
> evalf(%);
```

$$1.527117219, -.2396103081 + 1.679403718 I, \\ -2.047896603, -.2396103081 - 1.679403718 I$$

Như thế đa thức $x^4 + x^3 - 9$ có 2 nghiệm thực và 2 nghiệm phức liên hợp. Muốn hiển thị nghiệm căn thức của đa thức bậc 4, cần dùng như sau :

```
> _EnvExplicit:=true:  
> solve(x^4+x^3-9);
```

Sau khi nhấn Enter để thực hiện lệnh cuối cùng, 4 nghiệm căn thức của f sẽ được hiển thị.

Bài tập

✎ **11.1.** Xác định tính đúng, sai cho các mệnh đề sau :

- a) Nhóm Galois của đa thức tổng quát bậc n là giải được.
- b) Nhóm S_3 chỉ có hai nhóm con thực sự là 1 và A_3 .
- c) Đa thức tổng quát bậc n trên F là một đa thức có một biến siêu việt trên F .
- d) Bậc siêu việt của trường phân thức $\mathbb{Q}(t)$ trên \mathbb{Q} bằng 1.
- e) Một đa thức bậc nhỏ hơn 5 trên \mathbb{Q} luôn luôn giải được bằng căn thức trên \mathbb{Q} .
- f) Tồn tại đa thức bậc lớn hơn 4 trên \mathbb{R} không giải được bằng căn thức trên \mathbb{R} .
- g) Mọi đa thức bậc 2 trên trường đặc số 0 giải được bằng căn thức.
- h) Mọi mở rộng căn thức đều hữu hạn.
- i) Mọi mở rộng hữu hạn đều là mở rộng căn thức.
- j) Cấp của nhóm Galois của một đa thức cấp n chia hết $n!$.
- k) Tồn tại một đa thức bậc 4 có nhóm Galois là S_4 .

l) Một đa thức bất khả qui trên \mathbb{Q} bậc 11 có đúng 2 nghiệm không thực thì không giải được bằng căn thức.

m) Nhóm A_5 có 60 phần tử. (Xem HD 299)

 **11.2.** Tìm nghiệm căn thức của các đa thức sau :

a) $t^3 - 3t + 5$;

b) $t^3 - 7t + 6$;

c) $x^3 + x^2 - 2$. Suy ra $\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} = 4$.

d) $x^3 - 5x^2 + 4x + 5$;

e) $t^4 - t^3 - 2t - 1$;

f) $t^4 + 4t + 2$;

g) $t^6 + 2t^5 - 5t^4 + 9t^3 - 5t^2 + 2t + 1$. (Xem HD 299)

 **11.3.** Chứng minh rằng $\mathbb{C} : \mathbb{Q}$ và $\mathbb{R} : \mathbb{Q}$ không phải là mở rộng hữu hạn sinh.

(Xem HD 300)

 **11.4.** Tính bậc siêu việt của các mở rộng sau :

a) $\mathbb{Q}(t, u, v, w) : \mathbb{Q}$ với $t^2 = 2$, u siêu việt trên $\mathbb{Q}(t)$; $v^3 = t + 5$ và w siêu việt trên $\mathbb{Q}(t, u, v)$.

b) $\mathbb{Q}(t, u, v) : \mathbb{Q}$ với $t^2 = u^3 = v^4 = 7$. (Xem HD 300)

✎ **11.5.** Cho $f = x^3 - 3x + 1 \in F[x]$. Chứng minh rằng f hoặc là bất khả qui hoặc phân rã trong F . (Xem HD 300)

✎ **11.6.** Chứng minh các đa thức sau không giải được bằng căn thức trên \mathbb{Q} :

a) $t^5 - 4t + 2$;

c) $t^5 - 6t^2 + 3$;

b) $t^5 - 6t + 3$;

d) $t^7 - 10t^5 + 15t + 5$. (Xem HD 301)

PHỤ LỤC

A NHÓM GIẢI ĐƯỢC VÀ NHÓM ĐƠN

Mục này trình bày các kiến thức cơ bản về nhóm giải được và nhóm đơn. Các kết quả chính trong phần này là A.4, A.7, A.9 và A.17.

1. Nhóm giải được

Cho G là một nhóm nhân. Chuỗi chuẩn tắc của G là một chuỗi hữu hạn các nhóm con phân biệt

Định nghĩa.
$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G, \quad (12)$$

nghĩa là G_i là nhóm con chuẩn tắc của G_{i+1} với mọi $i = 0, \dots, n-1$. Các nhóm thương G_{i+1}/G_i , với $i = 0, \dots, n-1$, gọi là các thành phần của chuỗi chuẩn tắc (12).

Định nghĩa. Chuỗi (12) gọi là **chuỗi hợp thành** của G nếu G_i là nhóm con chuẩn tắc tối đại của G_{i+1} , nghĩa là nếu có $N \triangleleft G_{i+1}$ và N chứa G_i thì $G_i = N$ hay $N = G_{i+1}$, với mọi $i = 0, \dots, n-1$.

Nhận xét A.1. Chú ý rằng, trong chuỗi chuẩn tắc (12), không kéo theo $G_i \triangleleft G$ ngoại trừ $i = n-1$.

Định nghĩa. Một nhóm G gọi là **giải được** nếu tồn tại chuỗi chuẩn tắc (12) sao cho G_{i+1}/G_i là nhóm aben, với mọi $i = 0, \dots, n-1$.

Ví dụ A.2. (i) Mọi nhóm aben đều giải được.

(ii) Nhóm đối xứng S_3 giải được vì có chuỗi $1 \triangleleft A_3 \triangleleft S_3$, trong đó A_3 là nhóm cyclic và S_3/A_3 là nhóm cyclic cấp 2.

(iii) Nhóm đối xứng S_4 giải được vì có chuỗi chuẩn tắc

$$1 \triangleleft V \triangleleft A_4 \triangleleft S_4,$$

trong đó $V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Ta nhắc lại kết quả đơn giản sau của lý thuyết nhóm.

Bổ đề A.3. Cho G là một nhóm nhân.

(i) Nếu $H \triangleleft G$ và A là nhóm con của G thì $H \cap A \triangleleft A$ và

$$\frac{A}{H \cap A} \cong \frac{HA}{H}.$$

(ii) Nếu $H \triangleleft G$ và $H \subset A \triangleleft G$ thì $H \triangleleft A$, $A/H \triangleleft G/H$ và

$$\frac{G/H}{A/H} \cong \frac{G}{A}.$$

Các kết quả trong bổ đề trên tương ứng gọi là **định lý đẳng cấu thứ nhất** và **định lý đẳng cấu thứ hai**.

Ta có kết quả quan trọng đầu tiên về nhóm giải được.

Mệnh đề A.4. Cho G là một nhóm.

(i) Nếu G giải được thì mọi nhóm con H của G giải được.

(ii) Nếu $N \triangleleft G$ và G giải được thì G/N giải được.

(iii) Nếu tồn tại nhóm con chuẩn tắc $N \triangleleft G$ sao cho N và G/N giải được thì G giải được.

Chứng minh.

(i) Cho chuỗi chuẩn tắc

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

sao cho G_{i+1}/G_i aben, với mọi $i = 0, \dots, n-1$. Đặt $H_i = G_i \cap H$. Khi đó ta có chuỗi chuẩn tắc :

$$1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = H.$$

Ta chứng minh các thành phần H_{i+1}/H_i là aben. Ta có

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{G_i(G_{i+1} \cap H)}{G_i}.$$

Nhóm cuối cùng là nhóm aben vì nó là nhóm con của nhóm aben G_{i+1}/G_i . Vì thế H là nhóm giải được.

(ii) Từ chuỗi hợp thành của G như trên, nhóm thương G/N có chuỗi các nhóm con sau

$$1 = G_0N/N \subset G_1N/N \subset \cdots \subset G_nN/N = G/N.$$

Ta có $\frac{G_{i+1}N/N}{G_iN/N} \cong \frac{G_{i+1}N}{G_iN}$ theo định lí đẳng cấu thứ hai. Mặt khác

$$\begin{aligned} \frac{G_{i+1}N}{G_iN} &\cong \frac{G_{i+1}(G_iN)}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \\ &\cong \frac{G_{i+1}}{G_{i+1}/G_i} \\ &\cong \frac{G_{i+1}}{(G_{i+1} \cap (G_iN))/G_i}. \end{aligned}$$

Nhóm cuối cùng là nhóm thương của G_{i+1}/G_i nên là nhóm aben. Vậy G/N giải được.

(iii) Tồn tại 2 chuỗi chuẩn tắc

$$1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = N$$

$$1 = G_0/N \triangleleft G_1/N \triangleleft \cdots \triangleleft G_s/N = G/N$$

với các thành phần aben. Xét chuỗi

$$1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = N = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_s = G/N$$

có các thành phần đẳng cấu với N_{i+1}/N_i hay đẳng cấu với

$$G_{i+1}/G_i \cong (G_{i+1}/N)/(G_i/N),$$

chúng đều là nhóm aben. Vậy G giải được.

□

2. Nhóm đơn

Định nghĩa. Một nhóm $G \neq 1$ gọi là **nhóm đơn** nếu G không có nhóm con chuẩn tắc nào khác 1 và chính nó.

Như thế chuỗi (12) là chuỗi hợp thành của G khi và chỉ khi mọi thành phần G_{i+1}/G_i là các nhóm đơn.

Nhận xét A.5. Nếu G là nhóm hữu hạn thì trong $G = G_1$ có nhóm con chuẩn tắc tối đại G_2 , nhóm G_2 chứa một nhóm con chuẩn tắc tối đại G_3, \dots . Tiếp tục quá trình này, ta thấy rằng mọi nhóm hữu hạn đều có một chuỗi hợp thành.

Mệnh đề A.6. Mọi nhóm đơn giải được đều là nhóm cyclic có cấp nguyên tố.

Chứng minh. Gọi G là nhóm đơn giải được. Khi đó có chuỗi chuẩn tắc

$$1 = G_0 \triangleleft \cdots \triangleleft G_r = G$$

với các thành phần aben. Vì G đơn nên $r = 1$ và $G = G/G_0$ aben. Trong nhóm aben, mọi nhóm con đều là nhóm con chuẩn tắc, do đó để G đơn, nó trùng với nhóm con cyclic sinh ra bởi một phần tử bất kì khác 1 của G . Do đó G là nhóm cyclic có cấp nguyên tố. \square

Hệ quả A.7. Một nhóm hữu hạn G là giải được khi và chỉ khi tồn tại chuỗi hợp thành $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$ sao cho với mọi $1 \leq i \leq n$, ta có G_i/G_{i-1} cyclic có cấp nguyên tố.

Chứng minh. Gọi $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$ là chuỗi hợp thành của nhóm giải được G . Khi đó nhóm con G_{i+1} giải được nên nhóm thương G_{i+1}/G_i giải được, với mọi $i = 0, \dots, n-1$. Do chuỗi trên là chuỗi hợp thành nên G_{i+1}/G_i là nhóm đơn. Từ (A.6), ta có các thành phần G_{i+1}/G_i là các nhóm cyclic cấp nguyên tố. Chiều ngược lại là hiển nhiên vì mọi nhóm cyclic đều aben. \square

Bổ đề A.8. Cho G là nhóm nhân và $H \triangleleft G$ sao cho G/H aben. Khi đó $\forall a, b \in G$, ta có $a^{-1}b^{-1}ab \in H$.

Chứng minh. Với mọi $a, b \in G$, ta có

$$\overline{ab} = \overline{a}b = b\overline{a} = \overline{ba}.$$

Suy ra $(ba)^{-1}(ab) = a^{-1}b^{-1}ab \in H.$ □

Định lí A.9. Nhóm đối xứng S_n với $n \geq 5$ không giải được.

Chứng minh. Giả sử ngược lại, nhóm S_n với $n \geq 5$ giải được. Khi đó tồn tại chuỗi chuẩn tắc

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = S_n,$$

sao cho G_i/G_{i-1} aben với mọi $i = 1, \dots, r$. Gọi $(a b c)$ là một vòng xích bậc 3 bất kì của S_n . Lấy

$$u, v \in \{1, \dots, n\} \setminus \{a, b, c\}$$

sao cho $u \neq v$ (chú ý u, v tồn tại do $n \geq 5$). Bổ đề trên kéo theo:

$$(u b a)^{-1}(v c a)^{-1}(u b a)(v c a) = (a b c) \in G_{r-1},$$

do S_n/G_{r-1} aben. Vậy G_{r-1} chứa tất cả các vòng xích độ dài 3. Tiếp tục lí luận như trên, do G_{i-1}/G_{i-2} aben, nhóm G_{r-2} chứa tất cả các vòng xích độ dài 3. Bằng

quy nạp, nhóm G_0 chứa tất cả các vòng xích độ dài 3. Vô lí ! Vậy S_n không giải được. \square

Mệnh đề A.10. Với mọi $n \geq 5$, nhóm thay phiên A_n là nhóm đơn.

Chứng minh. Giả sử có $1 \neq N \triangleleft A_n$. Ta cần chỉ ra $N = A_n$. Trước hết ta chứng tỏ rằng nếu N chứa một vòng xích độ dài 3 thì $N = A_n$. Ta có thể giả thiết N chứa vòng xích $(1\ 2\ 3)$. Khi đó với mọi $k > 3$, ta có $(3\ 2\ k) \in A_n$. Do đó

$$(3\ 2\ k)(1\ 2\ 3)(3\ 2\ k)^{-1} = (1\ k\ 2) \in N.$$

Như thế N chứa các phần tử $(1\ k\ 2)^2 = (1\ 2\ k)$ với mọi $k \geq 3$.

Chú ý rằng $(m\ r) = (1\ m)(1\ r)(1\ m)$ với mọi m, r . Do đó S_n được sinh bởi các chuyển trí $(1\ i)$ với $i = 2, \dots, n$. Suy ra, mọi phép thế chẵn đều là tích của một số chẵn các chuyển trí loại này. Nên A_n được sinh bởi các phần tử $(1\ j)(1\ i) = (1\ i\ j)$, với $i, j = 2, \dots, n$. Ta có

$$(1\ i\ j) = (1\ 2\ j)^{-1}(1\ 2\ i)(1\ 2\ j),$$

với $i, j \neq 2$. Như thế A_n được sinh bởi các phần tử $(1\ 2\ k)$. Do đó $N = A_n$.

Ta còn phải chứng minh N chứa một vòng xích bậc 3. Ta chia ra các trường hợp như sau :

- Nhóm con N chứa một phần tử $x = a b c \dots$ với a, b, c, \dots là các vòng xích độc lập và

$$a = (a_1 a_2 \dots a_m) \text{ với } m \geq 4.$$

Đặt $t = (a_1 a_2 a_3)$. Khi đó N chứa phần tử $z := t^{-1} x t$. Chú ý rằng t giao hoán với các vòng xích a, b, \dots , nên

$$z = t^{-1} x t = (t^{-1} a t) b c \dots$$

Cuối cùng, ta thấy rằng N chứa phần tử $z x^{-1} = t^{-1} a t a^{-1} = (a_1 a_2 a_4)$.

- Xét N chứa 1 phần tử có phân tích vòng xích độc lập chứa 2 vòng xích độ dài 3. Không mất tính tổng quát, giả sử N chứa

$$x = (123)(456)y.$$

Đặt $t = (234)$. Khi đó N chứa

$$x^{-1}(t x t^{-1}) = (12436).$$

Từ trường hợp đầu tiên, ta suy ra N chứa một vòng xích độ dài 3.

- Nếu N chứa một phần tử x có dạng phân tích vòng xích là $(ijk)\sigma$ với σ là tích của các phép chuyển trí độc lập. Khi đó N chứa $x^2 = (ijk)$.
- Trường hợp còn lại là mọi phần tử của N đều là tích của các phép chuyển trí độc lập. Vì $n \geq 5$, ta có thể giả thiết N chứa phần tử x với phân tích vòng xích

$$x = (12)(34)\sigma$$

trong đó σ là tích các phép chuyển trí độc lập. Đặt $t = (234)$. Khi đó N chứa phần tử

$$x^{-1}(txt^{-1}) = (23)(14).$$

Lấy $u = (145)$, khi đó N chứa

$$ux^{-1}(txt^{-1})u^{-1} = (23)(45).$$

Như thế N chứa

$$(23)(14)(23)(45) = (145).$$

Mâu thuẫn !

Vậy A_n là nhóm đơn với mọi $n \geq 5$. □

Kết quả này cũng kéo theo Định lý A.9. Thật vậy, nếu S_n giải được thì A_n giải được. Hơn nữa, từ định lý trên, ta có A_n là nhóm đơn. Từ Mệnh đề A.6, suy ra A_n có cấp nguyên tố. Vô lý vì cấp của A_n là $\frac{n!}{2}$, không nguyên tố khi $n \geq 5$.

3. Các p -nhóm

Trong mục này, ta xét lớp các nhóm giải được đặc biệt gọi là p -nhóm. Bên cạnh đó, ta chứng minh một số kết quả sâu sắc của lý thuyết nhóm, đặc biệt là tính chất của p -nhóm thông qua chuỗi chuẩn tắc của nó (A.17).

Định nghĩa.

Cho G là một nhóm nhân. Phần tử $a \in G$ gọi là liên hợp với $b \in G$ nếu tồn tại $g \in G$ sao cho $a = g^{-1}bg$. Quan hệ liên hợp là một quan hệ tương đương trên G . Các lớp tương đương theo quan hệ liên hợp gọi là các lớp liên hợp.

Nếu G hữu hạn, gọi các lớp liên hợp là C_1, C_2, \dots, C_r với $C_1 = \{1\}$. Kí hiệu $|S|$ là số phần tử của một tập hữu hạn S . Ta có đẳng thức :

$$|G| = 1 + |C_2| + \dots + |C_r|, \quad (13)$$

gọi là **phương trình lớp** của G .

Ta có một quan hệ tương đương tương tự trên tập các nhóm con của G .

Định nghĩa.

Hai nhóm con H, K của nhóm nhân G gọi là **liên hợp** với nhau nếu tồn tại $g \in G$ sao cho $K = g^{-1}Hg$. Dễ dàng kiểm tra đây là một quan hệ tương đương.

Định nghĩa.

Cho G là nhóm nhân và $x \in G$. Kí hiệu

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

Khi đó $C_G(x)$ là một nhóm con của G gọi là **nhóm con trung tâm của x trong G** .

Bổ đề A.11. Cho G là nhóm hữu hạn. Số phần tử trong lớp liên hợp của $x \in G$ bằng với chỉ số của $C_G(x)$ trong G .

Chứng minh. Lấy 2 phần tử $g^{-1}xg$ và $h^{-1}xh$ bất kì trong lớp tương đương của x . Ta có

$$g^{-1}xg = h^{-1}xh \iff hg^{-1}x = xhg^{-1} \iff hg^{-1} \in C_G(x).$$

Như thế h và g nằm trong cùng lớp ghép của $C_G(x)$. Suy ra số phần tử trong lớp liên hợp của x bằng với chỉ số của $C_G(x)$ trong G . \square

Bổ đề kéo theo :

Hệ quả A.12. Số phần tử trong một lớp liên hợp tùy ý chia hết cấp của nhóm G .

Định nghĩa. Một nhóm hữu hạn G gọi là một p -nhóm nếu cấp của G là lũy thừa của một số nguyên tố p .

Ví dụ A.13. Nhóm dihedral D_8 (xem tr. 30) là 2-nhóm. Nhóm S_n với $n \geq 3$ không phải là p -nhóm với mọi p nguyên tố.

Định nghĩa. Tâm của nhóm G là tập

$$Z(G) = \{x \in G \mid gx = xg, \forall g \in G\}.$$

Dễ dàng kiểm tra $Z(G)$ là một nhóm con chuẩn tắc của G .

Ví dụ A.14. a) Tâm của nhóm aben là chính nó.

b) Tâm của nhóm S_3 là nhóm tầm thường.

c) $Z(D_8) = \{1, \sigma^2\}$ với $\sigma \in D_8$ là phần tử có cấp 4 trong D_8 .

Ta có kết quả tổng quát sau đây :

Định lí A.15. Mọi p -nhóm khác 1 đều có tâm không tầm thường.

Chứng minh. Từ phương trình lớp, ta có

$$p^n = |G| = 1 + |C_2| + \cdots + |C_r|.$$

Vì số phần tử của mọi lớp liên hợp chia hết p^n , ta gọi $|C_i| = p^{n_i}$ với $n_i \geq 0$. Vì $|C_i|$ phải chia hết cho p , số lớp có 1 phần tử phải là một bội số của p . Mặt khác, nếu x thuộc vào lớp có 1 phần tử thì ta có $g^{-1}xg = x$ với mọi $g \in G$. Nghĩa là $x \in Z(G)$. Như thế $Z(G)$ có nhiều hơn 1 phần tử. \square

Bổ đề A.16. Nếu A là một nhóm aben hữu hạn có cấp chia hết cho một số nguyên tố p thì chứa một phần tử cấp p .

Chứng minh. Ta chứng minh bằng quy nạp trên $|A|$. Nếu $|A| = p$, thì kết quả là hiển nhiên.

Gọi M là một nhóm con thực sự có cấp tối đại trong A . Nếu p chia hết $|M|$ thì bổ đề được chứng minh theo nguyên lí quy nạp. Xét trường hợp p không chia hết

$|M|$. Gọi $b \in A \setminus M$, xét $B = \langle b \rangle$ là nhóm cyclic sinh ra bởi b . Khi đó MB là một nhóm con (chú ý G aben) chứa M thực sự nên $MB = A$. Ta có đẳng cấu nhóm (A.3)

$$M/(M \cap B) \cong MB/B.$$

Suy ra

$$|MB| = \frac{|M||B|}{|M \cap B|}.$$

Do đó p chia hết cấp r của $B = \langle b \rangle$. Khi đó phần tử $b^{r/p}$ có cấp p . □

Ta có một tính chất đặc biệt của p -nhóm.

Mệnh đề A.17. Cho G là một p -nhóm có cấp p^n . Khi đó G có chuỗi các nhóm con chuẩn tắc

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

sao cho $(G_i : 1) = p^i$ với mọi $i = 0, \dots, n$.

Chứng minh. Ta chứng minh bằng quy nạp trên n . Nếu $n = 0$ thì kết quả là hiển nhiên. Xét $n > 0$. Do $Z(G)$ là một nhóm aben khác 1 có cấp chia hết cho p

nên theo (A.16), tồn tại một phần tử $x \in Z(G)$ có cấp p . Nhóm cyclic $K = \langle x \rangle$ là nhóm con chuẩn tắc của G vì $x \in Z(G)$. Nhóm thương G/K có cấp p^{n-1} , theo giả thuyết quy nạp, tồn tại chuỗi các nhóm con chuẩn tắc của G/K thỏa

$$K/K = G_1/K \triangleleft G_2/K \triangleleft \cdots \triangleleft G_n/K = G/K$$

với $|G_i/K| = p^{i-1}$ và $G_i \triangleleft G$ với mọi $i = 1, \dots, n$. Như thế $|G_i| = p^i$. Đặt $G_0 = 1$, ta có điều phải chứng minh. \square

Hệ quả A.18. Mọi p -nhóm đều giải được.

Chứng minh. Từ chuỗi các nhóm con chuẩn tắc của G cho trong mệnh đề trên, ta có các thành phần G_i/G_{i-1} có cấp là p nên là nhóm cyclic. Suy ra G giải được. \square

B ĐỊNH LÝ SYLOW VÀ ĐỊNH LÝ CAUCHY

Ta giới thiệu khái niệm nhóm con Sylow và chứng minh một phần kết quả của Định lý Sylow, kết quả đó đủ để chứng minh Định lý Cauchy.

Định lý B.1 (Sylow). Cho G là một nhóm nhân hữu hạn có $p^\alpha m$ phần tử, trong đó p nguyên tố không chia hết m . Khi đó

- (i) G chứa một nhóm con có cấp p^α ;
- (ii) mọi nhóm con cấp p^α đều liên hợp với nhau ;
- (iii) mọi p -nhóm con của G đều chứa trong một nhóm con cấp p^α ;
- (iv) số các nhóm con cấp p^α bằng $1 + kp$ với $k \in \mathbb{N}$.

Một nhóm con có cấp p^α gọi là p -nhóm Sylow của G .

Chứng minh. Ta chỉ chứng minh phần i) của định lí trên. Bạn đọc có thể tham khảo chứng minh đầy đủ của định lí trong các sách về Đại số, ví dụ [1], tr. 141.

Ta chứng minh bằng quy nạp trên $|G|$. Kết quả hiển nhiên nếu $|G| = 1, 2$. Gọi C_1, \dots, C_r là các lớp liên hợp của G và gọi $c_i = |C_i|$. Khi đó, phương trình lớp cho ta

$$p^\alpha m = c_1 + \dots + c_r. \quad (14)$$

Gọi Z_i là nhóm con trung tâm của một phần tử $x_i \in C_i$ và $n_i = |Z_i|$ với $i = 1, \dots, r$. Từ (A.11), ta có

$$n_i = \frac{p^\alpha m}{c_i}. \quad (15)$$

Giả sử tồn tại c_i lớn hơn 1 và không chia hết cho p . Khi đó, từ (15), ta có $n_i < p^\alpha m$ và n_i chia hết cho p^α . Theo giả thuyết quy nạp, tồn tại một nhóm con cấp p^α trong Z_i . Ta có điều cần chứng minh.

Xét trường hợp với mọi $i = 1, \dots, r$, ta có $c_i = 1$ hay c_i không chia hết cho p . Gọi $z = |Z(G)|$. Như trong chứng minh của (A.15), số các $c_i = 1$ bằng với z . Như thế ta có

$$p^\alpha m = z + kp$$

với $k \in \mathbb{N}$. Suy ra p chia hết $z = |Z(G)|$. Theo (A.16), tồn tại một phần tử $x \in Z(G)$ có cấp p . Gọi $P = \langle x \rangle$ là nhóm cyclic sinh ra bởi x . Do $P \subset Z(G)$, ta có $P \triangleleft G$. Nhóm thương G/P có $p^{\alpha-1}m$ phần tử nên theo giả thuyết quy nạp chứa một nhóm con S/P cấp $p^{\alpha-1}$, với S là một nhóm con của G . Khi đó S có cấp p^α . Ta có điều phải chứng minh. \square

Từ định lí trên, ta có kết quả của Cauchy.

Định lí B.2 (Cauchy). Nếu một nhóm hữu hạn G có cấp chia hết cho số nguyên tố p thì G có một phần tử cấp p .

Chứng minh. Gọi S là p –nhóm con Sylow của G , khi đó $S \neq 1$. Theo (A.17), tồn tại một nhóm con chuẩn tắc cấp p trong S . Ta có điều phải chứng minh. \square

C BAO ĐÓNG ĐẠI SỐ CỦA MỘT TRƯỜNG

Mục này trình bày hai chứng minh về việc tồn tại của bao đóng đại số của một trường tùy ý.

Định lí C.1. Mọi trường F đều tồn tại một bao đóng đại số.

Chứng minh. Trước tiên ta chú ý rằng, tương tự như vành đa thức hữu hạn biến độc lập đại số, ta có thể xây dựng vành đa thức $F[\{x_j\}]$ với tập tùy ý các biến $\{x_j\}$, trong đó mỗi đa thức là tổng hữu hạn các đơn thức $ax_{i_1} \cdots x_{i_m}$, với $x_{i_t} \in \{x_j\}$. Gọi $F[\dots, y_f, \dots]$ là vành đa thức mà mỗi biến y_f ứng với một đa thức chuẩn tắc $f \in F[x]$. Gọi I là ideal của $F[\dots, y_f, \dots]$ sinh bởi tất cả đa thức $f(y_f)$. Nếu $I = (1)$ thì tồn tại $g_1, \dots, g_n \in F[\dots, y_f, \dots]$, sao cho

$$g_1 f(y_{f_1}) + \cdots + g_n f(y_{f_n}) = 1. \quad (16)$$

Gọi F' là một mở rộng của F chứa một nghiệm α_i của f_i với mọi $i = 1, \dots, n$.

Xét đồng cấu vành từ $F[\dots, y_f, \dots]$ vào F' biến y_{f_i} thành α_i , $\forall i = 1, \dots, n$ và biến $y_f = 0$ với $f \notin \{f_1, \dots, f_n\}$. Khi đó biểu diễn (16) cho $0 = 1$. Vô lí ! Cho nên $I \neq (1)$.

Do đó, theo Bổ đề Zorn, tồn tại một idêan tối đại M của $F[\dots, y_f, \dots]$ chứa I . Đặt $E_1 = F[\dots, y_f, \dots]/M$, khi đó E_1 là một trường chứa F . Mọi đa thức trong $F[x]$ đều có ít nhất một nghiệm trong E_1 . Lặp lại quá trình trên khi thay F bởi E_1 , ta có mở rộng E_2 của E_1 . Tiếp tục như thế, ta có chuỗi các mở rộng trường $F = E_0 \subset E_1 \subset \dots$, và đặt $E = \cup E_i$. Khi đó E là một trường đóng đại số vì với mọi đa thức $f \in E[x]$, tồn tại i sao cho $f \in E_i[x]$. Như thế f có ít nhất một nghiệm trong $E_{i+1} \subset E$. Lấy trường con \overline{F} các phần tử đại số trên F trong E . Khi đó \overline{F} là bao đóng đại số của F . \square

Một chứng minh khác sử dụng những tính chất về lực lượng. Ta cần bổ đề sau :

Bổ đề C.2. Cho F là một trường vô hạn và K là một mở rộng đại số của F . Khi đó K có cùng lực lượng với F .

Chứng minh. K bằng hợp rời rạc của các tập hữu hạn, mỗi tập chứa tất cả các

nghiệm trong K của một đa thức chuẩn tắc bất khả quy trong $F[x]$. Do đó lực lượng của K bằng với lực lượng các đa thức chuẩn tắc, bất khả quy trong $F[x]$. Ta biết rằng tập các đa thức chuẩn tắc có bậc bằng n cho trước trong $F[x]$ có cùng lực lượng với F , do đó lực lượng của tập tất cả các đa thức chuẩn tắc cũng bằng lực lượng của F , suy ra K và F có cùng lực lượng. \square

Chứng minh. (Định lý C.1) Ta chỉ cần chứng minh cho trường hợp F là trường vô hạn. Nhúng F vào trong một tập S có lực lượng lớn hơn lực lượng của F . Gọi Λ là tập các bộ $(E, +, \cdot)$, trong đó $E \subset S$ là một mở rộng đại số của F và $+, \cdot$ là các phép toán trên trường E . Trên Λ xét quan hệ thứ tự, định bởi $(E, +, \cdot) > (E', +, \cdot)$ nếu E là mở rộng trường của E' . Bổ đề Zorn chỉ ra rằng tồn tại một phần tử tối đại $(K, +, \cdot)$ trong Λ . Khi đó K là một mở rộng đại số của F . Ta chứng minh K đóng đại số. Giả sử ngược lại K không đóng đại số. Khi đó tồn tại một mở rộng đại số thực sự $L = K(\alpha)$ của K . Vì $|L| < |S|$, nhúng L vào S bằng một đơn ánh sao cho đồng nhất trên K . Khi đó tồn tại một phần tử của Λ lớn hơn $(K, +, \cdot)$, vô lí do tính tối đại của $(K, +, \cdot)$. \square

D SƠ LƯỢC VỀ MAPLE

Maple là một hệ thống tính toán trên các biểu thức đại số và minh họa toán học mạnh mẽ của công ty **Warterloo Maple Inc.**, ra đời năm 1991, đến nay (2006) đã phát triển đến phiên bản 10. Maple có cách cài đặt đơn giản, chạy trên tất cả các hệ điều hành, có cấu trúc linh hoạt để sử dụng tối ưu cấu hình máy và đặc biệt có trình trợ giúp (Help) rất dễ sử dụng. Từ phiên bản 7 trở đi, Maple cung cấp ngày càng nhiều các công cụ trực quan, các gói lệnh tự học gắn liền với toán phổ thông và đại học. Ưu điểm đó làm cho nhiều nước trên thế giới lựa chọn sử dụng Maple cùng các phần mềm toán học khác trong dạy học toán. Việc sử dụng Maple cũng như công nghệ thông tin trong dạy và học toán là một xu hướng ngày càng phổ biến trên thế giới và tỏ ra là một phương tiện hỗ trợ đắc lực nhằm làm cho việc dạy-học toán trở nên thực tiễn hơn, đáp ứng nhu cầu phát triển của giáo dục hiện đại. Phần này cung cấp những kiến thức cơ bản về Maple để người đọc có thể khai thác sử dụng nó trong việc học tập và giảng dạy toán học, trong đó có Lí thuyết Trường và Galois. Độc giả có thể tìm hiểu thêm về Maple trong các tài liệu tham khảo [8] và [10].

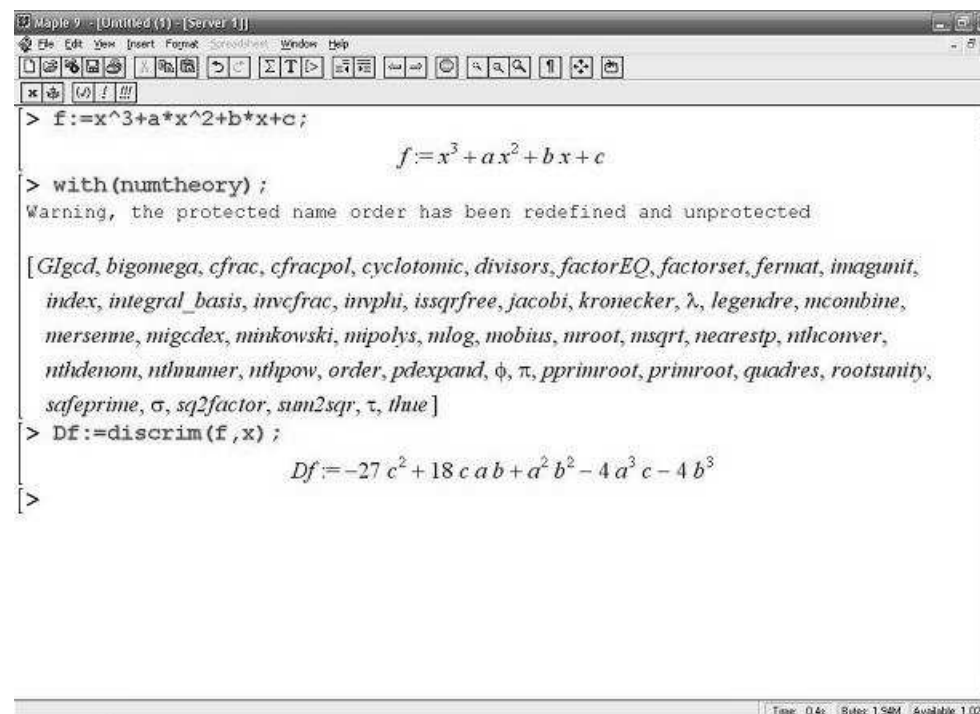
Các tính năng cơ bản của Maple.

Có thể nêu vắn tắt các chức năng cơ bản của Maple như sau.

- là một hệ thống tính toán trên các biểu thức số học và đại số ;
- có thể thực hiện được hầu hết các phép toán cơ bản trong chương trình toán đại học và phổ thông ;
- cung cấp các công cụ minh họa hình học thuận tiện gồm: vẽ đồ thị tĩnh và động của các đường và mặt được cho bởi các hàm tùy ý trong nhiều hệ tọa độ khác nhau ;
- một ngôn ngữ lập trình đơn giản và mạnh mẽ, có khả năng tương tác với các ngôn ngữ lập trình khác ;
- cho phép trích xuất dữ liệu ra các định dạng khác nhau như LaTeX, Word, HTML,...
- Một công cụ biên soạn giáo án và bài giảng điện tử ;
- cung cấp một môi trường dạy-học tương tác trực tiếp.

Giao diện và lệnh trong Maple.

Giao diện của Maple được thể hiện như trong Hình 12.



Hình 12: Giao diện của Maple

Lệnh của Maple được gõ vào trang làm việc (worksheet) tại dấu nhắc lệnh ">" và theo ngầm định được hiển thị bằng font Courier màu đỏ. Một lệnh được kết thúc

bởi dấu ":" hoặc dấu ";" và được ra lệnh thực hiện bằng việc nhấn Enter khi con trỏ đang ở trên dòng lệnh. Kết quả của lệnh được hiển thị ngay bên dưới dòng lệnh nếu dùng dấu ";".

Maple có dịch vụ trợ giúp khá đầy đủ và thuận lợi bao gồm cú pháp, giải thích cách dùng và các ví dụ đi kèm. Để nhận được trợ giúp, có thể dùng một trong các cách sau. Nếu đã biết tên lệnh thì từ dấu nhắc gõ vào, ví dụ:

```
> ?factor
```

Nếu dùng một gói lệnh thì khi nạp gói lệnh bằng lệnh “with”, Maple sẽ hiển thị toàn bộ lệnh trong gói đó. Một cách thông dụng nữa là dùng trình Help | Topic Search rồi gõ vào từ khóa cần tìm.

Các môi trường làm việc.

Maple có 2 môi trường làm việc là toán và văn bản. Người dùng có thể chuyển đổi một cách dễ dàng giữa 2 môi trường này để tạo ra một môi trường tương tác khi dạy-học qua hệ thống e-learning hoặc trích xuất ra bài giảng hoàn chỉnh sau này. Khi kích hoạt Maple, trang làm việc mở ra với môi trường toán. Con trỏ nằm ở dấu nhắc “>” màu đỏ. Muốn chuyển sang môi trường văn bản, chỉ cần kích chuột

vào biểu tượng T trên thanh công cụ hoặc vào Insert | Text, hay dùng tổ hợp phím Ctrl+T. Trong môi trường văn bản, Maple cho phép biên soạn tài liệu theo cấu trúc, cho phép hiển thị theo nhiều tầng lớp, rất phù hợp với việc giới thiệu tổng quan hoặc tổng kết ôn tập. Giống như một hệ soạn thảo văn bản, Maple cho phép thay đổi các font chữ, màu sắc và đặc biệt có thể tạo ra các bookmark để truy xuất nhanh chóng đến các vị trí tùy ý trong trang làm việc hiện hành hay các trang làm việc khác ; tạo ra các siêu liên kết để nối với trang web hay phần trợ giúp của Maple.

Lưu giữ và trích xuất dữ liệu.

Trang làm việc của Maple sẽ được lưu giữ bằng file có đuôi ".mws". File được lưu giữ bằng trình **File | Save**. Một file đã có được mở bằng **File | Open**. Ngoài việc lưu giữ bằng định dạng của Maple như trên, dữ liệu có thể được trích xuất thành các định dạng khác như Word, LaTeX hay HTML. Trích xuất bằng **File | Export**.

$$\phi(a) = \tau(a), \forall a \in D \text{ thì}$$

$$\phi(m/n) = \phi(m)\phi(n)^{-1} = \tau(m)\tau(n)^{-1} = \varphi(m/n).$$

Vậy φ xác định duy nhất.

0.4. Gọi $\varphi : \mathbb{Q} \longrightarrow \mathbb{Q}$ là một đồng cấu trường. Ta có $\varphi(1) = 1$. Với mọi $n \in \mathbb{N}$, dễ thấy rằng $\varphi(n) = \varphi(n \cdot 1) = n\varphi(1) = n$. Mặt khác $\varphi(-n) = -\varphi(n) = -n$. Vậy $\varphi(m) = m, \forall m \in \mathbb{Z}$. Hơn nữa

$$\varphi(1) = \varphi\left(n \cdot \frac{1}{n}\right) = n\varphi\left(\frac{1}{n}\right) = 1.$$

Do đó $\varphi\left(\frac{1}{n}\right) = \frac{1}{n}$. Cuối cùng

$$\varphi\left(\frac{m}{n}\right) = \varphi\left(m \cdot \frac{1}{n}\right) = \varphi(m)\varphi\left(\frac{1}{n}\right) = m \cdot \frac{1}{n} = \frac{m}{n},$$

với mọi $\frac{m}{n} \in \mathbb{Q}$. Như thế ánh xạ đồng nhất là tự đồng cấu trường duy nhất của \mathbb{Q} . Tương tự với tập các tự đồng cấu của trường \mathbb{Z}_p . Cuối cùng theo **0.2**, ánh xạ Frobenius là phép đồng nhất, suy ra điều phải chứng minh.

0.5. Nếu có đồng cấu $\psi : \mathbb{Q} \longrightarrow F$ thì F chứa một trường con đẳng cấu với \mathbb{Q} . Do đó 0 là đặc số của F . Tương tự cho trường hợp \mathbb{Z}_p . Ngược lại nếu F là trường có đặc số 0 thì tồn tại đồng cấu trường $\varphi : \mathbb{Q} \longrightarrow F$ sao cho $\varphi(\frac{m}{n}) = (m1_F)(n1_F)^{-1}$ (xem trang 23). Hơn nữa, nếu có $\psi : \mathbb{Q} \longrightarrow F$ là một đồng cấu trường thì chỉ ra rằng $\varphi(\frac{m}{n}) = (m1_F)(n1_F)^{-1}$. Do đó φ là duy nhất. Chứng minh tương tự cho \mathbb{Z}_p .

0.6. Nếu $\exists a \in \mathbb{Z}_p$ sao cho $2 = a^2$ thì

$$f = x^4 - 10x^2 + 1 = (x^2 - 1)^2 - a^6x^2 = (x^2 + a^3x - 1)(x^2 - a^3x - 1).$$

Nếu $\exists b \in \mathbb{Z}_p$ sao cho $b^2 = 3$ thì $f = (x^2 + 1)^2 - (2bx)^2$. Cuối cùng nếu 2 và 3 đều không chính phương trong \mathbb{Z}_p thì 6 chính phương trong \mathbb{Z}_p . Điều này suy ra từ tính chất đơn giản rằng trong một nhóm cyclic, tích của 2 phần tử không chính phương là chính phương. Theo 0.18, nhóm \mathbb{Z}_p^\times cyclic. Trong trường hợp này $f = (x^2 - 5)^2 - 24$ khả quy.

0.7. Do $F[x]$ là miền nguyên Euclide nên là miền nguyên chính. Thực ra, ta có thể chứng minh trực tiếp rằng, với mọi ideal thực sự $I \subset F[x]$, gọi $f \in I$ là đa

thức có bậc nhỏ nhất trong các đa thức thuộc I . Dễ dàng chỉ ra $I = (f)$.

Nếu f không bất khả quy, gọi h là một ước thực sự của f . Khi đó $(f) \subset (h) \neq F[x]$. Nghĩa là f không tối đại. Ngược lại nếu (f) không tối đại thì $(f) \subset m \neq F[x]$ với m là một idêan thực sự của $F[x]$. Gọi $m = (h)$ thì h là một ước thực sự của f . Vậy f không bất khả quy.

0.8. Giả sử $f = gh$ với g là một ước bất khả quy thực sự của f . Khi đó $\bar{f} = \bar{g}\bar{h}$. Vì hệ số cao nhất của f không chia hết cho p nên \bar{g} là một ước bất khả quy thực sự của \bar{f} . Vô lí !

0.9. $d = x + 2, s = 2$ và $t = 2x^2 + 8x + 6$.

0.10. Chứng minh tương tự như đối với trường hợp \mathbb{Z} và \mathbb{Q} .

0.11. a) $f = x^4 + 1$ bất khả quy trên \mathbb{Q} , dùng tiêu chuẩn Eisentein với $f(x - 1)$.

b) $x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$ là dạng nhân tử hóa trong $\mathbb{R}[x]$.

c) $x^7 + 11x^3 - 33x + 22$ bất khả quy theo Eisentein cho $p = 11$.

d) $g = x^4 + x^3 + x^2 + x + 1$ bất khả quy, dùng tiêu chuẩn Eisenstein với $g(x+5)$.

- e) Chú ý $x^3 - 7x^2 + 3x + 3$ có nghiệm 1.
 f) Bất khả quy, có thể chứng minh bằng cách hạn chế $x^4 + 15x^3 + 7$ trên \mathbb{Z}_2 .
 g) Bất khả quy trên \mathbb{Z}_{17} .
 h) $x^3 - 5 = (x + 8)(x^2 + 3x + 9)$ trong $\mathbb{Z}_{11}[x]$.

0.12. Chú ý rằng

- c) $x^5 + x + 1 = (x^2 + x + 1)(x^3 - x^2 + 1)$.
 d) $x^4 - 6x^2 + 11$ bất khả quy trên \mathbb{Q} .

0.13. $x^2 + bx + c \in \mathbb{Z}_5$ bất khả quy khi và chỉ khi $\Delta = b^2 - 4c$ không chính phương trong \mathbb{Z}_5 . Các đa thức chuẩn tắc, bất khả quy bậc 2 là

$$\begin{aligned} &x^2 + x + 2, \quad x^2 + 4x + 2, \quad x^2 + 3x + 4, \quad x^2 + 2x + 4, \\ &x^2 + 2x + 3, \quad x^2 + 4x + 1, \quad x^2 + x + 1, \quad x^2 + 2 \\ &x^2 + 3, \quad x^2 + 3x + 3. \end{aligned}$$

0.14. Gọi $f = gh$ với $h \in \mathbb{Q}[x]$ chuẩn tắc. Gọi $m, n \in \mathbb{N}$ có số thừa số nguyên tố ít nhất sao cho $mg, nh \in \mathbb{Z}[x]$. Khi đó ta có $mnf = (mg)(nh)$. Giải sử $mn \neq 1$.

Gọi $p \mid mn$. Khi đó $p \mid (mg)$ hay $p \mid nh$. Suy ra p chia hết tất cả các hệ số của g hay của h . Khi đó $\frac{m}{p}g \in \mathbb{Z}[x]$ hay $\frac{n}{p}h \in \mathbb{Z}[x]$. Vô lí với cách chọn m, n .

0.15. Trong $\mathbb{Z}_p[x]$ có đúng p^2 đa thức chuẩn tắc bậc 2. Trong đó có p đa thức dạng $(x - a)^2$ và $(p^2 - p)/2$ đa thức dạng $(x - a)(x - b)$ với $a \neq b$. Suy ra số đa thức bất khả quy.

0.17. Với mọi $x \in \mathbb{N}$, $x \leq qn$, ta có $x = nt + y$ với $0 \leq t \leq q - 1$ và $0 \leq y \leq n - 1$. Do $(x, n) = (y, n)$, mỗi giá trị $y \leq n$ thỏa $(y, n) = 1$ có đúng q giá trị $x \leq qn$ sao cho $(x, n) = 1$. Như thế số các giá trị $x \leq qn$ sao cho $(x, n) = 1$ bằng $q\varphi(n)$.

a) Nếu $q \mid n$ thì $(x, n) = (x, qn)$. Do đó $\varphi(qn) = q\varphi(n)$.

b) Nếu p nguyên tố và $(n, p) = 1$ thì $(x, pn) = 1$ khi và chỉ khi $(x, n) = (x, p) = 1$. Như thế $\varphi(pn)$ bằng với số giá trị $x \leq pn$ thỏa $(x, n) = 1$ trừ đi cho các giá trị của x thỏa $(x, p) \neq 1$. Do $(p, n) = 1$, các giá trị x như thế có dạng $x = pt$ với $t \leq n$ và $(t, n) = 1$. Suy ra $\varphi(pn) = p\varphi(n) - \varphi(n)$.

c) Sử dụng 2 kết quả trên và chứng minh bằng quy nạp theo m .

d) Từ câu c), ta có $\varphi(p^m) = (p-1)p^{m-1}$ với mọi số nguyên tố p . Cho $a = p_1^{m_1} \cdots p_r^{m_r}$. Dùng quy nạp theo r .

e) Từ d), suy ra

$$\varphi(p_1^{m_1} \cdots p_r^{m_r}) = (p_1 - 1)p_1^{m_1-1} \cdots (p_r - 1)p_r^{m_r-1}.$$

Biến đổi về công thức chỉ ra. Chứng minh $\sum_{i=0}^m \varphi(p^i) = p^m$, bằng cách khai triển về trái. Phân tích $n = p_1^{m_1} \cdots p_r^{m_r}$ rồi chứng minh đúng cho n .

0.18. Nhắc lại công thức Euler : $\sum_{d|n} \varphi(d) = n$ với $\varphi(d)$ là số các số nguyên dương không vượt quá d và nguyên tố cùng nhau với d . Gọi $n = (G : 1)$ với G là nhóm con của F^* . Với $d|n$, gọi $\psi(d)$ là số các phần tử của G có bậc d . Như thế $\sum_{d|n} \psi(d) = n$.

Chú ý rằng các phần tử có cấp d đều là nghiệm của đa thức $x^d - 1$, do đó nếu có $a \in G$ là một phần tử cấp d thì mọi phần tử cấp d đều thuộc vào nhóm cyclic $(a) = \{1, a, \dots, a^{d-1}\}$. Do đó số các phần tử cấp d đúng bằng $\varphi(d)$. Nói cách khác, nếu tồn tại một phần tử cấp d thì $\psi(d) = \varphi(d)$. Suy ra $\psi(d) \leq \varphi(d)$, $\forall d|n$. Mặt khác, do $\sum_{d|n} \psi(d) = \sum_{d|n} \varphi(d) = n$, ta có

$\psi(d) = \varphi(d), \forall d|n$. Nói cách khác $\psi(n) \neq \emptyset$ nên tồn tại một phần tử cấp n trong G .

0.19. Cho φ là một tự đồng cấu của \mathbb{R} . Chỉ ra $\varphi(a) = a, \forall a \in \mathbb{Q}$. Mặt khác, chỉ ra $\varphi(r) > 0$ nếu $r > 0, r \in \mathbb{R}$. Suy ra $\varphi(a) < \varphi(b)$ nếu $a < b$.

Nếu có $r \in \mathbb{R}$ sao cho $\varphi(r) \neq r$. Giả sử $\varphi(r) < r$. Lấy $a \in \mathbb{Q}$ sao cho $\varphi(r) < a < r$. Suy ra $a < \varphi(r)$. Vô lý. Vô lý cũng xảy ra khi $\varphi(r) > r$. Vậy $\varphi(r) = r, \forall r \in \mathbb{R}$.

§ 1

1.1. Các trường hợp a), b) và d) là các mở rộng trường.

1.2. Đều là các mở rộng bậc 2.

1.3. Gọi $\varphi : \mathbb{Q}[\sqrt{3}] \longrightarrow \mathbb{Q}[\sqrt{5}]$ là một đẳng cấu trường. Gọi $\varphi(\sqrt{3}) = a + b\sqrt{5}$. Ta có $3 = (a + b\sqrt{5})^2 = (a^2 + 5b^2) + 2ab\sqrt{5}$. Suy ra $2ab\sqrt{5} = 0$ và $a^2 + 5b^2 = 3$. Chỉ ra rằng không tồn tại $a, b \in \mathbb{Q}$ như thế.

- 1.4.** Nếu $[\mathbb{R} : \mathbb{Q}]$ hữu hạn thì \mathbb{R} đếm được do \mathbb{Q} đếm được. Vô lý. Hoặc chỉ ra trong \mathbb{R} có một tập vô hạn độc lập tuyến tính.
- 1.5.** Xét trường hợp $P \cong \mathbb{Q}$. Khi đó mọi phần tử của $a \in P$ đều viết được dưới dạng $(m1_K)(n1_K)^{-1}$ với $m, n \in \mathbb{Q}$. Do đó $\varphi(a) = a, \forall a \in K$. Làm tương tự cho trường hợp $P \cong \mathbb{Z}_p$.
- 1.7.** Gọi E là một trường trung gian của $F \subset K$. Xét $[K : F] = [K : E][E : F]$.
- 1.8.** a) Dễ dàng chỉ ra τ_* là đồng cấu vành. Hơn nữa τ_* là đơn cấu do τ là đơn cấu. Cuối cùng, nếu τ toàn cấu thì chỉ ra τ_* cũng là toàn cấu.
- b) Chứng minh tương tự như trong Mệnh đề 1.3.

§ 2

- 2.1.a)** Đ b) Đ c) S d) S e) S
 f) Đ g) Đ h) Đ i) S j) Đ

2.2. Trước hết chỉ ra đa thức $f = x^3 - x^2 + x + 2$ bất khả quy. Đặt

$$g = (x^2 + x + 1)(x^2 - x).$$

Tìm dư của phép chia g cho f (có thể dùng Maple). Ta có $g = fq + (-4x - 2)$.

Suy ra $u = (\alpha^2 + \alpha + 1)(\alpha^2 - \alpha) = g(\alpha) = -4\alpha - 2$.

Tương tự, đặt $h = x - 1$. Do $(h, f) = 1$ (chứng minh), tồn tại $s, t \in \mathbb{Q}[x]$ sao cho $hs + ft = 1$. Khi đó $s(\alpha) = h(\alpha)^{-1} = (\alpha - 1)^{-1}$. Tìm được (có thể dùng Maple), $-1/3 - \alpha^2/3 = (\alpha - 1)^{-1}$.

2.3. Sử dụng Hệ quả 2.6.

2.4. Nếu $u \in K$ là một nghiệm của f . Xét

$$[K : F] = [K : F(u)][F(u) : F].$$

Suy ra điều vô lý.

2.5. Gọi u là một nghiệm của f . Ta có

$$[K(u) : F] = [K(u) : K][K : F] = [K(u) : F(u)][F(u) : F].$$

Chỉ ra $[K(u) : K] = m$. Suy ra f bất khả quy trên K .

2.6. a) bậc 4.

b) bậc 6, c) bậc 6 và f) bậc 12, sử dụng bài tập 2.5.

d) bậc 3 với chú ý $\mathbb{Q}(\sqrt{27}, 3 + \sqrt{12}) = \mathbb{Q}(\sqrt{3})$.

e) bậc 4 với chú ý $\mathbb{Q}(\sqrt{18}, \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2})$.

2.7. Sử dụng Hệ quả 2.7.

2.8. Chú ý rằng $\sqrt{a} - \sqrt{b} = \frac{a - b}{\sqrt{a} + \sqrt{b}} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Suy ra \sqrt{a} và \sqrt{b} đều thuộc $\mathbb{Q}(\sqrt{a} + \sqrt{b})$.

2.9. a) gồm các đa thức chỉ chứa các đơn thức với số mũ chẵn.

2.10. Các đa thức tối tiểu lần lượt là :

a) $x^2 - x - 1 \in \mathbb{Q}[x]$.

b) $x^2 + x + 1 \in \mathbb{Q}[x]$.

c) $x^2 - (t + 1) \in \mathbb{Z}_3(t)[x]$.

d) $u = \sqrt[4]{5} + \sqrt{5}$. Suy ra $\sqrt[4]{5} = u - \sqrt{5}$. Do đó $\sqrt{5} = u^2 - 2u\sqrt{5} + 5$. Hay $\sqrt{5}(1 + 2u) = u^2 + 5$. Suy ra $u^4 - 10u^2 - 20u + 20 = 0$.

e) $u = \sqrt[3]{2} + \sqrt[3]{4}$. Suy ra $u^3 = 6 + 6(\sqrt[3]{2} + \sqrt[3]{4}) = 6 + 6u$.

f) $v = u^2 + u$. Do $u^3 + 3u^2 - 3 = 0$, ta có $v^2 = 4u^2 + 3u - 3 = 4v - u - 3$. Mặt khác $v^3 = 15u^2 + 9u - 15 = 15v - 6u - 15$. Khử u , ta có $v^3 - 6v^2 + 9v - 3 = 0$.

g) $u = \xi + \xi^6$. Ta có $u^2 = 1 - u - (\xi^3 + \xi^4)$. Do đó $u^3 = 3u + (\xi^3 + \xi^4)$. Suy ra $u^2 + u^3 = 1 + 2u$. Chỉ ra $x^3 + x^2 - 2x - 1$ chính là đa thức tối thiểu của u .

h) $\xi + \xi^2 + \xi^4$ có đa thức tối thiểu là $x^2 + x + 2$.

i) $\xi^2 + \xi^5$ có đa thức tối thiểu là $x^3 + x^2 - 2x - 1$.

2.11. Xét đồng cấu vành $\varphi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[x]/(x^2 - 4x + 2) = \mathbb{Q}(\beta)$ xác định bởi $x \mapsto \beta$ và $a \mapsto a, \forall a \in \mathbb{Q}$. Chỉ ra $\text{Ker}(\varphi) = (x^2 - 2)$. Suy ra điều phải chứng minh.

2.12. Cho $f = ax^2 + bx + c \in F[x]$. Hai nghiệm của f thuộc vào $F(u)$ với $u^2 = b^2 - 4ac$. Kết quả không đúng với trường có đặc số 2, ví dụ trong \mathbb{Z}_2 do

mọi phần tử đều chính phương.

2.13. a) Cho $K : \mathbb{Q}$ là một mở rộng bậc 2. Khi đó $K = \mathbb{Q}(u)$ với u có bậc 2 trên \mathbb{Q} .

Gọi $f = ax^2 + bx + c \in \mathbb{Z}[x]$ là đa thức bất khả quy nhận u làm nghiệm.

Rõ ràng $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{d})$ với $d = b^2 - 4ac \in \mathbb{Z}$ không chính phương.

b) Gọi $K : \mathbb{R}$ là mở rộng bậc 2. Khi đó $K = \mathbb{R}(u)$ với u có bậc 2 trên \mathbb{R} . Gọi

$f = x^2 + bx + c \in \mathbb{R}[x]$ là đa thức tối tiểu của u . Tương tự $\mathbb{R}(u) \cong \mathbb{R}(\sqrt{d})$

với $d = b^2 - 4c < 0$. Do $\mathbb{R}(\sqrt{d}) \subset \mathbb{C}$ và $[\mathbb{C} : \mathbb{R}] = 2$ nên $\mathbb{C} = \mathbb{R}(\sqrt{d})$.

2.14. Xét $F \subset F(u) \subset K$.

2.15. Trong \mathbb{Z}_3 chỉ có 3 đa thức bất khả quy bậc 2 là $x^2 + 1$, $x^2 + x + 2$ và $x^2 + 2x + 2$.

Sử dụng phương pháp như trong Bài tập 2.11.

2.16. Vì $x^4 + x^2 + 1 = x(x^3 - 1) + (x^2 + x + 1)$ nên α là nghiệm của $x^2 + x + 1$.

Suy ra $x^2 + x + 1$ chính là đa thức tối tiểu của α .

2.17. Tương tự như trong chứng minh Hệ quả 2.7.

2.18. a) Rõ ràng.

b) Nếu $\beta \in K$ là một nghiệm của f thì tồn tại F -đẳng cấu từ $F(\alpha)$ vào $F(\beta)$ biến α thành β . Do đó ánh $\alpha \mapsto \varphi(\alpha)$ là toàn cầu.

Mặt khác, nếu $\varphi(\alpha) = \psi(\alpha)$ thì $\varphi = \psi$ vì $\{1, \alpha, \dots, \alpha^{n-1}\}$, với n là bậc của α , là một cơ sở của $F(\alpha)$.

2.19. a) Rõ ràng.

b) Cho $\beta \in K$ là một nghiệm của $\tau_*(f)$. Chú ý rằng $\tau_* : F[x] \longrightarrow \tau(F)[x]$ là một đẳng cấu vành và $\tau_*(f)$ bất khả quy trong $\tau(F)[x]$. Do đó $\tau_*(f)$ là đa thức tối tiểu của β . Hơn nữa, đẳng cấu vành τ_* cảm sinh một đẳng cấu trường

$$\varphi : F(\alpha) \cong F[x]/(f) \longrightarrow \tau(F)[x]/(\tau_*(f)) \cong \tau(F)(\beta)$$

thỏa $\varphi(\alpha) = \beta$ và $\varphi(a) = \tau(a)$, $\forall a \in F$. Xem φ như một đồng cấu từ F vào K . Suy ra ánh xạ $\varphi \mapsto \varphi(\alpha)$ là một toàn ánh. Tính đơn ánh được chứng minh như trong bài tập trên.

2.20. Dùng tính chất mọi mở rộng đơn của một trường đếm được là đếm được.

2.21. a) Rõ ràng.

b) “khi” là hiển nhiên. Nếu có $S(E) = S(E')$. Khi đó $E = F(\alpha)$ với $\alpha^2 = d \in S(E) = S(E')$ và $d \in F$ không chính phương. Do đó tồn tại $\beta \in E'$ sao cho $\alpha^2 = \beta^2$. Rõ ràng $\beta \notin F$ và do đó $E' = F(\beta)$. Các trường E và E' đều đẳng cấu với $F[x]/(x^2 - d)$.

c) Lấy các mở rộng $E_p := \mathbb{Q}(\sqrt{p})$ của \mathbb{Q} với p nguyên tố. Khi đó $S(E_p)$ chỉ chứa một số nguyên tố là p . Thực vậy xét $(a + b\sqrt{p})^2$.

d) Một trường có p^2 phần tử có trường con nguyên tố đẳng cấu với \mathbb{Z}_p . Xét các mở rộng bậc 2 của \mathbb{Z}_p . Xét đồng cấu nhóm $\phi : \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times$ cho bởi $\phi(a) = a^2$. Rõ ràng $\text{Ker}(\phi) = \{\pm 1\}$. Chỉ ra ảnh của ϕ là nhóm con có chỉ số 2 của \mathbb{Z}_p^\times . Như thế $S(E)$ bằng \mathbb{Z}_p^\times . Cho nên chỉ có 1 mở rộng bậc 2 của \mathbb{Z}_p , đẳng cấu với $\mathbb{Z}_p[x]/(x^2 - d)$ với $d \notin \mathbb{Z}_p^2$.

§ 3

3.1.a) S

b) Đ

c) S

d) Đ

e) Đ f) S g) S h) Đ

3.2. Gọi $K : \mathbb{R}$ là mở rộng đại số. Xét $[K : \mathbb{R}] > 1$. Lấy $u \in K \setminus \mathbb{R}$. Chỉ ra u có bậc 2 trên \mathbb{R} . Như thế $\mathbb{C} \cong \mathbb{R}(u) \subset K$. Mọi phần tử thuộc K đại số trên $\mathbb{R}(u) \cong \mathbb{C}$. Suy ra $K = \mathbb{R}(u) \cong \mathbb{C}$.

3.3. Vì $F \subsetneq M$ nên tồn tại $\frac{f(x)}{g(x)} \in M$ với $\deg(f) > 0$ hay $\deg(g) > 0$. Khi đó x là nghiệm của đa thức

$$f(t) - \frac{f(x)}{g(x)}g(t) \in M[t].$$

Do đó x đại số trên M .

3.4. Tất cả đều bất khả quy, sử dụng Bài tập 2.5.

3.5. Câu trả lời khẳng định cho a), b) và c) là rõ ràng. Với d) chú ý rằng $u^2 = -2v^2 - 3v + 11$. Kết hợp với $2u = 2v^2 + 2v + 2$, ta có $v = 13 - u^2 - 2u$. Do đó $\mathbb{Q}(u) = \mathbb{Q}(v)$.

- 3.6.** Gọi $f = a_n x^n + \dots + a_0 \in K[x]$. Gọi u là một nghiệm của f . Xét $F(a_0, \dots, a_n, u)$ là một mở rộng đại số của F . Do đó u đại số trên F . Khi đó f chia hết đa thức tối tiểu $g \in F[x]$ của u .
- 3.7.** Cho $g = a_0 + \dots + a_n x^n \in E[x]$ có bậc lớn hơn 0. Gọi u là một nghiệm của g . Xét $F(a_0, \dots, a_n, u)$ là một mở rộng đại số của F . Do đó u đại số trên F . Gọi $m \in F[x]$ là đa thức tối tiểu của u . Vì m phân rã trong E nên $u \in E$. Suy ra điều phải chứng minh.
- 3.8.** Sau này, ta thấy rằng kết quả này cũng đúng khi F là trường hữu hạn. Khi F vô hạn, chứng minh theo các gợi ý sau :

- Nếu $K = F(u_1, u_2)$ thì xét các trường con

$$J_c = F(u_1 + cu_2)$$

với $c \in F$. Do K chỉ có hữu hạn các trường con chứa F , tồn tại $c \neq c'$ sao cho $J_c = J_{c'}$. Từ $u_1 + cu_2, u_1 + c'u_2 \in J_c$, ta có $u_2 \in J_c$. Suy ra $u_1 \in J_c$. Hay

$$K = F(u_1, u_2) \subset J_c = F(u_1 + cu_2).$$

Dùng quy nạp, chứng minh cho trường hợp tổng quát.

- Ngược lại cho $F \subset M \subset F(u) = K$. Gọi f và f_1 lần lượt là đa thức tối tiểu của u trên F và M . Rõ ràng $f_1 \mid f$. Ta có $F(a_1, \dots, a_m) \subset M$ với a_i là hệ tử của f_1 . Mặt khác,

$$[F(u) : F(a_1, \dots, a_m)] = [F(u) : M] = \deg(f_1).$$

Do đó $M = F(a_1, \dots, a_m)$. Như thế chỉ có hữu hạn các trường trung gian M .

§ 4

- 4.1. a) Đ b) S c) Đ d) S e) Đ
 f) Đ g) S h) Đ i) Đ

- 4.2. Dễ dàng thấy rằng nếu (α_j, β_j) là giao điểm của 2 đường thẳng mà phương trình của chúng có hệ tử trong K_{j-1} thì $[K_j : K_{j-1}] = 1$. Nếu (α_j, β_j) là giao điểm của một đường thẳng d và một đường tròn C mà phương trình của chúng

lần lượt là :

$$d : ax + by + c = 0$$

$$C : (x - a_1)^2 + (y - b_1)^2 - r^2 = 0$$

với các hệ số trong K_{j-1} . Rút x hoặc y từ phương trình của d rồi thay vào phương trình của C , ta suy ra

$$[K_{j-1}(\alpha_j, \beta_j) : K_{j-1}] \leq 2.$$

Cuối cùng xét nếu (α_j, β_j) là giao điểm của hai đường tròn C_1, C_2 mà phương trình của chúng lần lượt là:

$$C_1 : (x - a_1)^2 + (y - b_1)^2 - r_1^2 = 0$$

$$C_2 : (x - a_2)^2 + (y - b_2)^2 - r_2^2 = 0$$

với các hệ số trong K_{j-1} . Suy ra

$$2(a_2 - a_1)(x - a_2) + (a_2 - a_1)^2 + 2(b_2 - b_1)(y - b_2) + (b_2 - b_1)^2 + (r_1^2 - r_2^2) = 0.$$

Tương tự như trường hợp trên, ta có $[K_j : K_{j-1}] \leq 2$.

Như thế $K_j = K_{j-1}(\sqrt{\gamma_j})$ với $a_j \in K_{j-1}$. Vậy sau hữu hạn bước, ta có điều phải chứng minh.

4.3. Từ chứng minh của Định lý 4.8, ta thấy rằng các phần tử của $\mathbb{Q}(\sqrt{\gamma_1}, \dots, \sqrt{\gamma_{n-1}})$ dựng được, nên α, β dựng được. Suy ra (α, β) dựng được.

4.4. Do $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ nên điểm $(\sqrt[3]{2}, 0)$ không dựng được.

4.5. Chú ý rằng $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$ do $\sqrt{\pi}$ siêu việt trên \mathbb{Q} .

4.6. a) Cho đoạn thẳng AB có 2 điểm mút A, B dựng được. Dựng đường tròn tâm A qua B và đường tròn tâm B qua A . Đường thẳng qua 2 giao điểm của 2 đường tròn này cắt AB tại trung điểm của AB .

b) Cho hình bình hành $ABCD$ có 3 đỉnh A, B, C dựng được. Dựng trung điểm O của đoạn thẳng AC . Đường thẳng BO cắt đường tròn tâm O qua B tại đỉnh thứ tư D .

4.7. Gọi L là trường các số dựng được. Cho $\alpha \in L$. Vì $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ nên α đại số trên \mathbb{Q} . Vậy $L : \mathbb{Q}$ đại số. Nếu $[L : \mathbb{Q}] = n$ thì dễ dàng chỉ ra số $\sqrt[n]{2}$ dựng

được nhưng bậc của nó bằng $2^n > n$. Vô lý !

4.8. Chỉ ra rằng $\cos(\frac{\pi}{5}) - \cos(\frac{2\pi}{5}) = \frac{1}{2}$. Thật vậy

$$\begin{aligned}\cos(\frac{\pi}{5}) - \cos(\frac{2\pi}{5}) &= 2 \sin(\frac{\pi}{10}) \sin(\frac{3\pi}{10}) \\ &= \frac{\sin(\frac{2\pi}{10}) \sin(\frac{6\pi}{10})}{2 \cos(\frac{\pi}{10}) \cos(\frac{3\pi}{10})} = \frac{1}{2}.\end{aligned}$$

Từ đó suy ra $\cos(\frac{\pi}{5}) = \frac{\sqrt{5}}{4} + \frac{1}{4}$ và $\cos(\frac{2\pi}{5}) = \frac{\sqrt{5}}{4} - \frac{1}{4}$.

4.9. Chú ý rằng $\cos(\frac{2\pi}{15}) = \cos(\frac{\pi}{3} - \frac{\pi}{5})$.

4.12. Nếu $\cos(\beta)$ chia 3 được, tức là $\cos(\frac{\beta}{3})$ dựng được. Mà $\cos(\frac{\beta}{3})$ là nghiệm của $4x^3 - 3x - \cos \beta \in \mathbb{Q}(\cos \beta)$. Rõ ràng

$$[\mathbb{Q}(\cos \beta, \cos(\beta/3)) : \mathbb{Q}(\cos \beta)] = 2^r \leq 3.$$

Suy ra $[\mathbb{Q}(\cos \beta, \cos(\frac{\beta}{3})) : \mathbb{Q}(\cos(\beta))]$ bằng 1 hay 2. Do đó $4x^3 - 3x - \cos(\beta)$ khả quy trên $\mathbb{Q}(\cos(\beta))$.

Ngược lại, nếu $4x^3 - 2x - \cos(\beta)$ khả quy trên $\mathbb{Q}(\cos \beta)$ thì $\cos(\frac{\beta}{3})$ có bậc 1 hoặc 2 trên $\mathbb{Q}(\cos \beta)$. Do $\cos \beta$ dựng được, góc $\frac{\beta}{3}$ dựng được.

4.13. Chú ý rằng $\widehat{NOD} = \widehat{NDO}$

§ 5

5.1. a) Đ b) Đ c) S d) S e) S k) Đ
f) S g) Đ h) Đ i) S j) Đ l) Đ

5.2. Chứng minh bằng qui nạp theo r . Nếu $r = 1$, đây chính là kết quả của Bài tập 2.18. Ta viết

$$F(\alpha_1, \dots, \alpha_r) = F(\alpha_1, \dots, \alpha_{r-1})(\alpha_r).$$

Khi đó, tồn tại F -đồng cấu từ $E_{r-1} = F(\alpha_1, \dots, \alpha_{r-1})$ vào K ; số đồng cấu không quá $[E_{r-1} : F]$ và đạt tối đa khi K chứa n nghiệm phân biệt của f . Với mỗi đồng cấu từ E_{r-1} vào K , tồn tại mở rộng F -đồng cấu từ $E_{r-1}(\alpha_r)$ vào K vì K chứa nghiệm của f . Số các mở rộng như thế không vượt quá $[E_{r-1}(\alpha_r) : E_{r-1}]$ và bằng $[E_{r-1}(\alpha_r) : E_{r-1}]$ khi K chứa n nghiệm phân biệt

của f (xem Bài tập 2.19). Như thế số F -đồng cấu từ E vào K không vượt quá

$$[E_{r-1}(\alpha_r) : E_{r-1}] \cdot [E_{r-1} : F] = [E : F].$$

Số đồng cấu đạt tối đa khi K chứa n nghiệm phân biệt của f .

5.3. Nếu $K = \cup F_j$ với F_j là các trường hoàn chỉnh. Gọi $p > 0$ là đặc số của K . Với mọi $a \in K$, tồn tại j sao cho $a \in F_j$. Do F_j hoàn chỉnh, phần tử a có căn bậc p trong F_j . Nếu K là mở rộng đại số của \mathbb{Z}_p , ta có $K = \cup_{\alpha} \mathbb{Z}_p(\alpha)$, với $\mathbb{Z}_p(\alpha)$ là các trường hoàn chỉnh.

5.5. Kiểm tra các đa thức đó đều bất khả quy. Gọi α là nghiệm của $f = x^3 + 2x + 1$. Khi đó các nghiệm còn lại của f là $\alpha + 1$ và $\alpha + 2$. Do đó trường phân rã của f trên \mathbb{Z}_3 là $\mathbb{Z}_3(\alpha)$. Tương tự, gọi β là nghiệm của $g = x^3 + x^2 + x + 2$. Khi đó các nghiệm còn lại của g là $\beta^2 + 1$ và $\beta^2 + \beta + 1$. Do đó trường phân rã của g là $\mathbb{Z}_3(\beta)$.

Chú ý rằng α^2 là một nghiệm của g nên tồn tại một \mathbb{Z}_3 -đồng cấu từ $\mathbb{Z}_3(\beta)$ vào $\mathbb{Z}_3(\alpha)$ biến β thành α^2 .

5.7. a) Gọi α là một nghiệm của $f = x^p - x - a$ trong một trường phân rã của f trên F . Khi đó $\alpha + 1, \dots, \alpha + (p - 1)$ là các nghiệm còn lại của f . Giả sử

$$f = (x^m + a_1x^{m-1} + \dots + a_m)(x^n + \dots + b_n)$$

với $m > 0, n > 0$ là một phân tích của f trong $F[x]$. Khi đó $-a_1$ là tổng của m nghiệm của f . Do đó $-a_1 = m\alpha + d$ với $m, d \in \mathbb{Z}_p \subset F$. Suy ra $\alpha \in F$. Vậy f phân rã trong F .

b) Xét $\bar{f} = x^p - x - 1$ trong $\mathbb{Z}_p[x]$. Dễ thấy rằng \bar{f} không có nghiệm trong \mathbb{Z}_p nên bất khả quy trên \mathbb{Z}_p .

5.8. Viết $f = a \prod_{i=1}^r (x - \alpha_i)^{m_i}$. Khi đó

$$f' = \sum \frac{m_i f}{x - \alpha_i}.$$

Do đó $d = \prod_{i=1}^r (x - \alpha_i)^{m_i-1}$. Suy ra $h = \prod_{i=1}^r (x - \alpha_i)$.

5.9. Nếu f tách được thì kết luận là hiển nhiên. Nếu f không tách được thì $f = f_1(x^p)$ với $f_1 \in F[x]$ bất khả quy. Nếu f_1 không tách được, ta có

$f_1 = f_2(x^p)$. Khi đó $f = f_2(x^{p^2})$. Tiếp tục như thế. Do $\deg(f_i) > \deg(f_{i+1})$, quá trình trên sẽ dừng sau e bước, ta có điều cần chứng minh.

Cuối cùng, đặt $g = a \prod (x - \alpha_i)$, với $\alpha_i \neq \alpha_j$. Ta có

$$f = a \prod (x^{p^e} - \alpha_i) = a \prod (x - \alpha_i)^{p^e}.$$

5.10. Giả sử f khả quy. Khi đó $f = gh$ với

$$g = x^m + a_1 x^{m-1} + \cdots + a_0$$

sao cho $0 < m < p$. Trong trường phân rã E_f của f trên F , do tính duy nhất của dạng nhân tử hóa, ta có

$$g = (x - b)^m = x^m + (-1)^m m b x^{m-1} + \cdots + (-1)^m b^m,$$

xem Ví dụ 20. Suy ra $a_1 = (-1)^m m b$. Do $m \neq 0$ trong F , ta có $b \in F$. Vô lý !

5.11. Ta chứng minh bằng quy nạp trên r . Nếu $r = 1$, ta có

$$\sharp\{\varphi : F(\alpha) \longrightarrow K \mid \varphi|_F = \tau\} = \sharp\{\beta \in K \mid \tau_* g(\beta) = 0\}$$

với $g \in F[x]$ là đa thức tối thiểu của α (xem Bài tập 2.19). Rõ ràng

$$\sharp\{\varphi : F(\alpha) \longrightarrow K \mid \varphi \text{ là } F\text{-đồng cấu, } \varphi|_F = \tau\}$$

không vượt quá $[F(\alpha) : F] = \deg(g)$. Nếu τ_*f có n nghiệm phân biệt trong K thì τ_*g có $\deg(g)$ nghiệm phân biệt trong K nên

$$\sharp\{\varphi : F(\alpha) \longrightarrow K \mid \varphi|_F = \tau\} = [F(\alpha) : F].$$

Kết quả đúng với $r = 1$.

Ta có $E = F(\alpha_1, \dots, \alpha_r) = F(\alpha_1, \dots, \alpha_{r-1})(\alpha_r)$. Đặt $F' = F(\alpha_1, \dots, \alpha_{r-1})$. Theo giả thuyết quy nạp

$$\sharp\{\psi : F' \longrightarrow K \mid \psi|_F = \tau\} \leq [F' : F]$$

và đẳng thức xảy ra nếu τ_*f có n nghiệm phân biệt trong K . Với $\psi : F' \longrightarrow K$ là đồng cấu thỏa $\psi|_F = \tau$ có α_r là nghiệm của f thỏa $\psi_*f = \tau_*f$, do đó

$$\sharp\{\psi : F'(\alpha_r) \longrightarrow K \mid \psi|_{F'} = \psi\} \leq [F'(\alpha_r) : F']$$

và đẳng thức xảy ra khi τ_*f có n nghiệm phân biệt trong K . Chú ý rằng $\varphi|_F = \psi|_F = \tau$. Suy ra

$$\#\{\psi : E \longrightarrow K \mid \varphi|_F = \tau\} \leq [E : F'] [F' : F] = [E : F]$$

và đẳng thức xảy ra khi K chứa n nghiệm phân biệt của τ_*f .

§6

- 6.1.** a) Đ b) S c) Đ d) S e) Đ f) S g) S
h) S i) Đ j) S k) Đ l) Đ m) S n) Đ

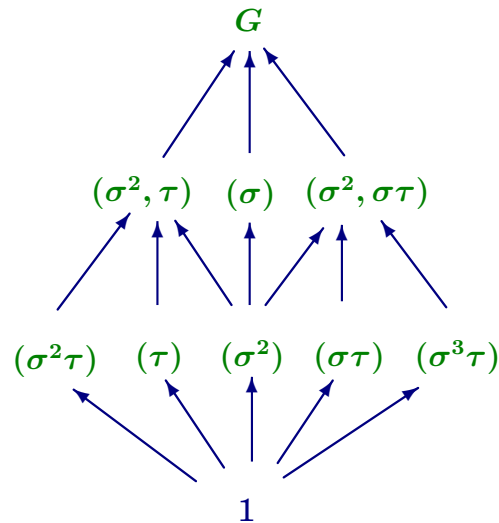
- 6.2.** a) $\text{Aut}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}_2$.

b) $\mathbb{Q}(\omega)$ là trường phân rã của $f = x^4 + x^3 + x^2 + x + 1$ trên \mathbb{Q} . Do đó $(\text{Aut}(\mathbb{Q}(\omega)/A) : 1) = [\mathbb{Q}(\omega)/A : \mathbb{Q}] = 4$. Gọi $\sigma : \omega \mapsto \omega^2$, khi đó $\text{Aut}(\mathbb{Q}(\omega)/A) = \langle \sigma \rangle$ là nhóm cyclic cấp 4. Do đó nó chỉ có một nhóm con cấp 2 là $\langle \sigma^2 \rangle$ ứng với trường trung gian là $\mathbb{Q}(\omega^2 + \omega^3)$. Nó cũng chính là trường trung gian duy nhất.

c) Dễ dàng tìm được trường phân rã của $f = x^4 - 2$ là $E_f = \mathbb{Q}(\sqrt[4]{2}, i)$. Nhóm $G = \text{Aut}(E_f)$ (đẳng cấu với nhóm đối xứng của hình vuông), sinh bởi:

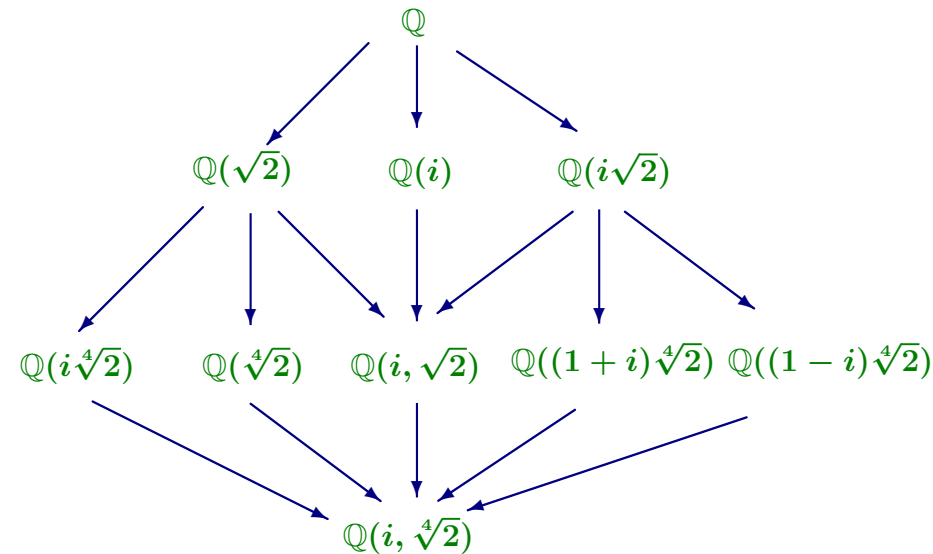
$$\sigma : \begin{cases} i \mapsto i \\ \sqrt[4]{2} \mapsto i\sqrt[4]{2} \end{cases}; \quad \tau : \begin{cases} i \mapsto -i \\ \sqrt[4]{2} \mapsto \sqrt[4]{2} \end{cases}.$$

Từ đó suy ra sơ đồ bao hàm các nhóm con của G như trong Hình 1.



Hình 1: Sơ đồ các nhóm con của $\text{Aut}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$.

Tính lần lượt các trường trung gian tương ứng, ta có sơ đồ các trường trung gian như trong Hình 2.



Hình 2: Sơ đồ các trường trung gian tương ứng.

d) $E_f = \mathbb{Q}(\theta, \sqrt[3]{2})$. Nhóm $\text{Aut}(E_f)/\mathbb{Q}(\theta) \cong \mathbb{Z}_3$ sinh bởi $\sigma : \sqrt[3]{2} \mapsto i\sqrt[3]{2}$. Do đó nó không có trường trung gian nào.

e) Nhóm $G = \text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ là trường phân rã của đa thức $f = (x^2 - 2)(x^2 - 3)(x^2 - 5)$ trên \mathbb{Q} . Vì thế nhóm G đẳng cấu với $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

sinh ra bởi các phần tử cấp 2:

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases} ; \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases} ;$$

$$\theta : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases} .$$

f) Trường phân rã E_f của $f = (x^3 - 5)(x^3 - 7)$ trên \mathbb{Q} là $\mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{7}, \xi)$ với $\xi = e^{i2\pi/3}$. Do đó nhóm $\text{Aut}(\mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{7}, \xi)/\mathbb{Q})$ có cấp 18, sinh bởi các phần tử

$$\sigma : \begin{cases} \xi \mapsto \xi \\ \sqrt[3]{5} \mapsto \xi \sqrt[3]{5} \\ \sqrt[3]{7} \mapsto \sqrt[3]{7} \end{cases} ; \tau : \begin{cases} \xi \mapsto \xi \\ \sqrt[3]{5} \mapsto \sqrt[3]{5} \\ \sqrt[3]{7} \mapsto \xi \sqrt[3]{7} \end{cases} ;$$

và

$$\theta \begin{cases} \xi \mapsto \xi^2 \\ \sqrt[3]{5} \mapsto \sqrt[3]{5} \\ \sqrt[3]{7} \mapsto \sqrt[3]{7} \end{cases}$$

g) Trường phân rã E_f của $f = x^6 - 5$ trên \mathbb{Q} là $\mathbb{Q}(\sqrt[6]{5}, \sqrt{-3})$. Do đó nhóm $\text{Aut}(\mathbb{Q}(\sqrt[6]{5}, i\sqrt{3})/\mathbb{Q})$ có cấp 12 (đẳng cấu với nhóm đối xứng của lục giác đều) sinh bởi

$$\sigma : \begin{cases} i\sqrt{3} \mapsto -i\sqrt{3} \\ \sqrt[6]{5} \mapsto \sqrt[6]{5} \end{cases} ; \quad \tau : \begin{cases} i\sqrt{3} \mapsto i\sqrt{3} \\ \sqrt[6]{5} \mapsto \xi \sqrt[6]{5} \end{cases} ;$$

với $\xi = e^{\pi i/3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$.

6.3. Trường phân rã của $x^5 - 2$ là $\mathbb{Q}(\sqrt[5]{2}, \xi)$ với $\xi = e^{2\pi i/5}$. Nhóm G có cấp bằng $[\mathbb{Q}(\sqrt[5]{2}, \xi) : \mathbb{Q}] = 20$. Nhóm G không giao hoán. Gọi

$$\sigma : \begin{cases} \xi \mapsto \xi \\ \sqrt[5]{2} \mapsto \xi \sqrt[5]{2} \end{cases} ; \quad \tau : \begin{cases} \xi \mapsto \xi^2 \\ \sqrt[5]{2} \mapsto \sqrt[5]{2} \end{cases}.$$

Rõ ràng $\sigma\tau \neq \tau\sigma$.

- 6.4.** Trường phân rã của $f = (x^3 - 2)(x^3 - 5)$ trên \mathbb{Q} là $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{5}, \xi)$ với $\xi = e^{2\pi i/3}$. Nhóm Galois G có cấp 18. Nhóm Galois của f trên \mathbb{R} có cấp 2.
- 6.5.** Chú ý rằng $\mathbb{Q}(\xi)$ là trường phân rã của đa thức $x^n - 1$ trên \mathbb{Q} . Mỗi phần tử φ thuộc $\text{Aut}(\mathbb{Q}(\xi)/\mathbb{Q})$ xác định bởi $\varphi(\xi) = \xi^r$. Dễ dàng kiểm tra tính giao hoán của nhóm $\text{Aut}(\mathbb{Q}(\xi)/\mathbb{Q})$.
- 6.6.** Gọi α là một nghiệm của $x^p - a$. Khi đó trường phân rã của f trên \mathbb{Q} là $\mathbb{Q}(\alpha, \xi)$ với $\xi = e^{2\pi i/p}$; trên \mathbb{Z}_p là $\mathbb{Z}_p(\alpha)$ vì $x^p - a = (x - \alpha)^p$.
- 6.7.** a) Không đúng, chẳng hạn xét $F = \mathbb{Z}_2(t^2) \subset \mathbb{Z}_2(t)$. Khi đó $[E : F] = 2$ và $\text{Aut}(E/F) = 1$.
- b) Mệnh đề đúng vì trường hữu hạn là trường hoàn chỉnh nên $\text{Aut}(E/F) \cong \mathbb{Z}_2$.
- 6.8.** Các nghiệm của $x^5 - 1$ là ξ^i với $i = 0, \dots, 4$. Suy ra $K = \mathbb{Q}(\xi)$. Do đó nhóm $G = \text{Aut}(K/\mathbb{Q})$ có cấp bằng 4 và là nhóm cyclic sinh ra bởi $\sigma : \xi \mapsto \xi^2$. Vì thế, G chỉ có một nhóm con thực sự duy nhất là $\langle \sigma^2 \rangle$. Trường trung gian ứng

với nhóm con này là $\mathbb{Q}(\xi + \xi^4)$. Dễ dàng tìm được đa thức tối tiểu của $\xi + \xi^4$ là $x^2 + x - 1$.

a) Chú ý rằng

$$\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5} - 1}{4} = \frac{1}{2}(\xi + \xi^4).$$

Suy ra trường phân rã của $(x^2 - 5)(x^5 - 1)$ chính là K .

b) Trường phân rã của $(x^2 + 3)(x^5 - 1)$ là $\mathbb{Q}(\xi, i\sqrt{3})$.

6.9. Chú ý rằng $x^3 - 5$ bất khả quy trên $\mathbb{Q}(\sqrt{7})$. Ta có $K = \mathbb{Q}(\sqrt[3]{5}, \xi)$ với $\xi = e^{2\pi i/3}$. Rõ ràng $[K : \mathbb{Q}(\sqrt{7})] = 6$ và do đó $G = \text{Aut}(K/\mathbb{Q})$ có cấp 6. Nhóm G sinh bởi các phần tử

$$\sigma : \begin{cases} \xi \mapsto \xi \\ \sqrt[3]{5} \mapsto \xi \sqrt[3]{5} \end{cases} \text{ cấp } 3; \quad \tau : \begin{cases} \xi \mapsto \xi^2 \\ \sqrt[3]{5} \mapsto \sqrt[3]{5} \end{cases} \text{ cấp } 2.$$

Nhóm này không giao hoán nên $G \cong S_3$.

§ 7

7.1. a) S b) S c) S d) Đ e) S f) S g) S
h) Đ i) Đ j) Đ k) S l) Đ m) S n) S

7.2. Không đúng, chẳng hạn $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

7.3. Mọi đa thức bất khả quy bậc 2 trên trường có đặc số khác 2 đều tách được. Trên trường có đặc số 2 khẳng định không đúng, ví dụ mở rộng bậc hai $\mathbb{Z}_2(x^2) \subset \mathbb{Z}_2(x)$ không Galois vì đa thức $t^2 - x^2 \in \mathbb{Z}_2(x^2)[t]$ không tách được.

7.4. Nếu f bất khả quy trên F , gọi α là một nghiệm của f . Khi đó trường phân rã là $F(\alpha)$ (xem Bài tập 5.7), và nhóm Galois của f đẳng cấu với nhóm cyclic có p phần tử.

7.5. Gọi K là trường phân rã của $f = x^{p^n} - x$. Do f là đa thức tách được, f có đúng p^n nghiệm trong K . Mặt khác nếu $\alpha, \beta \in K$ là 2 nghiệm của f thì ta có $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$. Tương tự $(\alpha\beta)^{p^n} = \alpha\beta$. Cuối cùng nếu $\alpha \neq 0$

thì $(\alpha^{-1})^{p^n} = \alpha^{-1}$. Như thế tập tất cả các nghiệm của f chính là trường phân rã của f (sau này ta sẽ kí hiệu trường có p^n phần tử là \mathbb{F}_{p^n}).

Nhóm Galois của f có n phần tử. Gọi $\varphi : K \longrightarrow K$ là ánh xạ Frobenius. Rõ ràng $\varphi \in \text{Gal}(K/F)$. Chứng tỏ rằng $\text{Gal}(E/F)$ là nhóm cyclic sinh bởi φ .

7.6. Ví dụ $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$. Giải thích $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ và $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}, i)$ là các mở rộng Galois nhưng $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ không phải là mở rộng Galois.

7.7. Chứng tỏ rằng $\alpha = \sqrt{2 + \sqrt{2}}$ là nghiệm của đa thức bất khả quy $f = x^4 - 4x^2 + 2$. Chứng tỏ rằng $\mathbb{Q}(\alpha)$ chứa 4 nghiệm của f và do đó nó là trường phân rã của f trên \mathbb{Q} . Nhóm Galois của mở rộng đẳng cấu với nhóm cyclic có 4 phần tử.

7.9. a) Nhóm Galois đẳng cấu với $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

b) Nhóm Galois $G = \langle \sigma, \tau \rangle$ với σ có cấp p và τ có cấp $p - 1$. Mọi phần tử của G có dạng $\sigma^m \tau^n$ với $1 \leq m \leq p, 1 \leq n \leq p - 1$.

c) Nhóm Galois đẳng cấu với $\mathbb{Z}_2 \times \mathbb{Z}_2$.

7.10. Xét ánh xạ φ định bởi $\sigma \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ và $\tau \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Chứng minh ánh xạ đó là đẳng cấu.

7.11. Nếu f có 2 nghiệm phức liên hợp thì nhóm Galois sẽ có 1 phép chuyển trí, hoán vị 2 nghiệm phức. Vô lí !

§ 8

8.1. a) S b) Đ c) S d) Đ e) S
f) Đ g) Đ h) S i) Đ j) Đ

8.2. $\mathbb{Q}(\xi)$ là trường phân rã của $x^7 - 1$ nên là mở rộng Galois trên \mathbb{Q} . Phần tử ξ có đa thức tối tiểu là

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Nhóm Galois $G = \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ là nhóm cyclic cấp 6 sinh bởi $\sigma : \xi \mapsto \xi^3$. Do đó các nhóm con thực sự của G là $\langle \sigma^2 \rangle$ và $\langle \sigma^3 \rangle$. Do G cyclic, các trường

trung gian của $\mathbb{Q}(\xi) : \mathbb{Q}$ đều là các mở rộng Galois của \mathbb{Q} .

Trường trung gian ứng với $\langle \sigma^2 \rangle$ (cấp 3) là $M_1 := \mathbb{Q}(\xi + \xi^2 + \xi^4)$. Nhóm Galois của M_1/M có cấp bằng 2. Dễ dàng chỉ ra đa thức tối thiểu của $\xi + \xi^2 + \xi^4$ là $x^2 + x + 2$.

Trường trung gian ứng với $\langle \sigma^3 \rangle$ là $\mathbb{Q}(\xi + \xi^5)$ có bậc mở rộng bằng 3 và đa thức tối thiểu của $\xi + \xi^5$ là $x^3 + x^2 - 2x - 1$.

8.3. (i) rõ ràng do các tương ứng Galois là song ánh, đồng thời do định nghĩa $M_1 \cdots M_r$ là trường con nhỏ nhất chứa M_1, \dots, M_r .

(ii) Ta chỉ cần kiểm tra $\cap_{\sigma \in G} (\sigma^{-1} H \sigma)$ là nhóm con chuẩn tắc lớn nhất chứa trong H là đủ. Thật vậy, do H là một thành phần của $\cap_{\sigma \in G} (\sigma^{-1} H \sigma)$ nên chứa $\cap_{\sigma \in G} (\sigma^{-1} H \sigma)$. Hơn nữa $\forall \sigma \in G$, dễ dàng kiểm tra tập $\sigma^{-1} H \sigma$ là một nhóm con chuẩn tắc, nên giao của chúng cũng là một nhóm con chuẩn tắc. Cuối cùng, giả sử $N \triangleleft G$ và $N \subset H$. Với mọi $\sigma \in G$, với mọi $n \in N$, ta có $\sigma n \sigma^{-1} \in N \subset H$. Suy ra $\sigma n \sigma^{-1} = h$, với $h \in H$. Khi đó $n = \sigma^{-1} h \sigma \in \sigma^{-1} H \sigma$. Như thế $N \subset \sigma^{-1} H \sigma$ với mọi $\sigma \in G$. Suy ra điều

phải chứng minh.

8.4. Trường phân rã của $x^3 - 2$ là $\mathbb{Q}(\sqrt[3]{2}, \xi)$ với $\xi = e^{2\pi i/3}$. Nhóm Galois của $x^3 - 2$ là G có 6 phần tử sinh bởi

$$\sigma : \begin{cases} \xi \mapsto \xi \\ \sqrt[3]{2} \mapsto \xi \sqrt[3]{2} \end{cases} \text{ cấp } 3 ; \tau : \begin{cases} \xi \mapsto \xi^2 \\ \sqrt[3]{2} \mapsto \sqrt[3]{2} \end{cases} \text{ cấp } 2 .$$

Nhóm $G \cong S_3$ và có các nhóm con thực sự như sau :

- Nhóm con cấp 3 duy nhất là $A = \langle \sigma \rangle$. Trường trung gian ứng với A là $\mathbb{Q}(\xi)$. Trường trung gian này là mở rộng Galois.
- Nhóm con cấp hai $B_1 = \langle \tau \rangle$ ứng với trường trung gian là $\mathbb{Q}(\sqrt[3]{2})$.
- Nhóm con cấp hai $B_2 = \langle \sigma\tau \rangle$ ứng với trường trung gian là $\mathbb{Q}(\sqrt[3]{4}\xi^2)$.
- Nhóm con cấp hai $B_3 = \langle \sigma^2\tau \rangle$ ứng với trường trung gian là $\mathbb{Q}(\sqrt[3]{2}\xi^2)$.

Chú ý rằng các trường trung gian ứng với các nhóm con cấp 2 đều không phải là mở rộng Galois trên \mathbb{Q} .

8.5. Ta phân tích tương ứng Galois của Bài tập 7.7. Khi đó nhóm Galois $G \cong \mathbb{Z}_4$ nên chỉ có 1 nhóm con thực sự là nhóm cấp 2. Gọi $\sigma : \sqrt{2 + \sqrt{2}} \mapsto \sqrt{2 - \sqrt{2}}$ là phần tử sinh của nhóm Galois. Khi đó $\sigma^2 : \sqrt{2 + \sqrt{2}} \mapsto -\sqrt{2 + \sqrt{2}}$. Nhóm con cấp 2 $\langle \sigma^2 \rangle$ ứng với trường trung gian $\mathbb{Q}(\sqrt{2})$.

8.6. Nhóm $G = \text{Gal}(K/\mathbb{Q}(\sqrt{7})) \cong S_3$. Gọi M là trường trung gian ứng với nhóm thay phiên A_3 . Khi đó $[K : M] = 3$.

8.7. a) Khi $F = \mathbb{Q}$, chứng minh f có đúng 3 nghiệm thực nên nhóm Galois đẳng cấu với S_5 . Có đúng 1 trường trung gian ứng với nhóm thay phiên A_5 .

b) Khi $F = \mathbb{Z}_2$, ta có

$$x^5 - 6x^4 + 3 = (x + 1)(x^4 + x^3 + x^2 + x + 1).$$

Do đó trường phân rã của f là mở rộng bậc 4 của \mathbb{Z}_2 , có nhóm Galois đẳng cấu với \mathbb{Z}_4 . Vì vậy có duy nhất 1 trường trung gian như yêu cầu đề bài.

8.8. a) $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ và $\text{Gal}(L/\mathbb{Q}) \cong S_3$.

b) K không chứa nghiệm nào của f .

c) Chú ý nếu $K \cap L \neq \mathbb{Q}$ thì $[K \cap L : \mathbb{Q}] = 2$. Chứng minh điều đó không thể xảy ra. Suy ra $[K \cap L : \mathbb{Q}] = 1$.

8.9. a) Xét $F \subset F(\sqrt{a}) \subset F(\sqrt{a}, \sqrt{b}) = K$. Rõ ràng $[F(\sqrt{a}) : F] = 2$. Do giả thiết về a, b , ta có $\sqrt{b} \notin F(\sqrt{a})$ nên $[K : F(\sqrt{a})] = 2$. Suy ra $[K : F] = 4$. Trường $F(\sqrt{a}, \sqrt{b})$ là trường phân rã của $(x^2 - a)(x^2 - b)$ không tách được nên là mở rộng Galois. Nhóm Galois $\text{Gal}(K/F)$ gồm các phần tử $1, \sigma, \tau$ và $\sigma\tau$ với:

$$\sigma : \begin{cases} \sqrt{a} \mapsto -\sqrt{a} \\ \sqrt{b} \mapsto \sqrt{b} \end{cases}; \quad \tau : \begin{cases} \sqrt{a} \mapsto \sqrt{a} \\ \sqrt{b} \mapsto -\sqrt{b} \end{cases}.$$

Suy ra $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

b) Ngược lại, nếu $G = \text{Aut}(K/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Gọi $H_1 \subset G$ là một nhóm con cấp 2. Xét $\mathcal{T}(H_1)$. Chỉ ra $F \subset \mathcal{T}(H_1)$ và $F \neq \mathcal{T}(H_1)$. Do đó $[\mathcal{T}(H_1) : F] = 2$ nên $\mathcal{T}(H_1) = F(\sqrt{a})$ với $a \in F$. Tương tự, gọi H_2 là nhóm cấp 2 khác H_1 của G . Ta có $\mathcal{T}(H_2) = F(\sqrt{b})$ với $b \in F$. Chỉ ra $K = F(\sqrt{a}, \sqrt{b})$.

8.10. Nhúng $\mathbb{Q}(\sqrt[8]{2}, i)$ trong mở rộng Galois $\mathbb{Q}(\sqrt[8]{2}, \sqrt{i})$. Khi đó $[\mathbb{Q}(\sqrt[8]{2}, \sqrt{i}) : \mathbb{Q}(\sqrt[8]{2}, i)] = 2$ nên $[\mathbb{Q}(\sqrt[8]{2}, i) : \mathbb{Q}] = 16$. Chỉ ra

$$[\mathbb{Q}(\sqrt[8]{2}, i) : \mathbb{Q}(i)] \cong \mathbb{Z}_8, [\mathbb{Q}(\sqrt[8]{2}, i) : \mathbb{Q}(\sqrt{2})] \cong D_8$$

và $[\mathbb{Q}(\sqrt[8]{2}, i) : \mathbb{Q}(\sqrt{-2})] \cong Q_8$.

8.11. a) Rõ ràng.

b) Các nghiệm còn lại là $\gamma = -\sqrt{1 + \sqrt{3}}$ và $\delta = -\sqrt{1 - \sqrt{3}}$.

c) Vì $\mathbb{Q}(\sqrt{1 + \sqrt{3}}) \subset \mathbb{R}$ còn $\sqrt{1 - \sqrt{3}} \notin \mathbb{R}$ nên $K_1 \neq K_2$. Ta có $\sqrt{3} \in K_1 \cap K_2$. Mặt khác

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset K_1 \cap K_2 \subset K_1$$

kéo theo $[K_1 : \mathbb{Q}(\sqrt{3})] = [K_1 : K_1 \cap K_2] = 2$. Vậy $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3})$.

d) Do K_1 và K_2 đều là các mở rộng bậc 2 trên F nên Galois trên F . Suy ra $K_1 K_2$ Galois (xem Mệnh đề 8.5). Nhóm

$$\text{Gal}(K_1 K_2 / F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

e) Do K_1K_2 chứa tất cả các nghiệm của f nên K_1K_2 chính là trường phân rã của f trên \mathbb{Q} . Suy ra điều phải chứng minh.

§ 9

- 9.1.** a) Đ b) S c) Đ d) S e) Đ f) S g) Đ
h) Đ i) Đ j) S k) Đ l) Đ m) S n) Đ
o) Đ p) S q) Đ r) Đ s) Đ t) S u) S

9.2. Các đa thức bậc 5 chuẩn tắc, bất khả quy trên \mathbb{Z}_2 là

$$\begin{aligned} & x^5 + x^4 + x^3 + x + 1, x^5 + x^4 + x^2 + x + 1, \\ & x^5 + x^3 + 1, x^5 + x^2 + 1, x^5 + x^4 + x^3 + x^2 + 1, \\ & x^5 + x^3 + x^2 + x + 1. \end{aligned}$$

Sử dụng Maple, ta tìm được có 624 đa thức chuẩn tắc, bất khả quy bậc 5 trên \mathbb{Z}_5 . Còn trên \mathbb{Z}_3 , con số tương ứng là 48.

9.3. Ta có $E \cong \mathbb{F}_{p^n}$ với p nguyên tố. Gọi bậc của f và g là r . Khi đó

$$E(\alpha) \cong \mathbb{F}_{p^{rn}} \cong E(\beta).$$

9.4. Trường \mathbb{F}_{p^n} là một mở rộng đơn của \mathbb{F}_p . Tồn tại $\alpha \in \mathbb{F}_{p^n}$ sao cho $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. Gọi $f \in F[x]$ là đa thức tối tiểu của α . Khi đó f bất khả quy có bậc n .

9.5. Nếu $p = 2$, ta có $x^4 + 1 = (x + 1)^4 \in \mathbb{Z}_2[x]$. Nếu p là số nguyên tố lẻ thì $8 \mid (p^2 - 1)$. Suy ra

$$(x^4 + 1) \mid (x^8 - 1) \mid (x^{p^2-1} - 1) \mid (x^{p^2} - x).$$

Do đó $x^4 + 1$ phân rã trong trường phân rã \mathbb{F}_{p^2} của $x^{p^2} - x$ trên \mathbb{Z}_p . Vì $[\mathbb{F}_{p^2} : \mathbb{Z}_p] = 2$, suy ra $x^4 + 1$ khả quy trên \mathbb{Z}_p .

9.6. $\mathbb{Q}(\xi_{12})$ là trường phân rã của $x^{12} - 1$ trên \mathbb{Q} . Phần tử ξ_{12} có đa thức tối tiểu là $\Phi_{12} = x^4 - x^2 + 1$. Do đó nhóm $G = \text{Gal}(\mathbb{Q}(\xi_{12})/\mathbb{Q})$ có cấp 4 và đẳng cấu với \mathbb{Z}_{12}^\times . Nhóm G sinh bởi

$$\sigma : \xi \mapsto \xi^5 = \xi^3 - \xi; \quad \tau : \xi \mapsto \xi^7 = -\xi.$$

Khi đó các nhóm con thực sự của G là 3 nhóm con cấp 2 như sau :

- Nhóm $H_1 = \langle \sigma \rangle$ có trường trung gian tương ứng là $\mathbb{Q}(\xi_{12}^3)$.
- Nhóm $H_2 = \langle \tau \rangle$ có trường trung gian tương ứng là $\mathbb{Q}(\xi_{12}^2)$.
- Nhóm $H_2 = \langle \tau\sigma \rangle$ có trường trung gian tương ứng là $\mathbb{Q}(2\xi_{12} - \xi_{12}^3)$.

9.7. Nhóm Galois $G = \text{Gal}(\mathbb{Q}(\xi_{13})/\mathbb{Q})$ là nhóm cyclic đẳng cấu với \mathbb{Z}_{12} . Nhóm G sinh bởi $\sigma : \xi_{13} \mapsto \xi_{13}^2$.

9.8. Nếu F hữu hạn thì E hữu hạn. Khi đó kết quả là hiển nhiên. Nếu F vô hạn, xem Bài tập 3.8.

9.9. Dễ dàng tính được $[\mathbb{F}_p(x, y) : \mathbb{F}_p(x^p, y^p)] = p^2$. Gọi $F = \mathbb{F}_p(x^p, y^p)$. Như trong chứng minh của Bài tập 3.8, xét các trường con $F(x + cy)$ với $c \in \mathbb{F}_p$. Nếu có $F(x + cy) = F(x + c'y)$ với $c \neq c'$ thì $F(x + cy) = \mathbb{F}_p(x, y)$. Tuy nhiên, do

$$(x + cy)^p = x^p + c^p y^p \in F,$$

ta có $[F(x + cy) : F] \leq p$. Vô lí, vậy các trường con $F(x + cy)$ với $c \in \mathbb{F}_p$ là

phân biệt. Suy ra điều phải chứng minh.

- 9.10.** Trong nhóm cyclic F^* có cấp 15 có hai phần tử cấp 3. Suy ra $x^3 - 1$ có đúng 3 nghiệm trong F . Tương tự, đa thức $x^4 - 1$ có một nghiệm trong F ; đa thức $x^{15} - 1$ có 15 nghiệm trong F và đa thức $x^{17} - 1$ có 1 nghiệm trong F .
- 9.11.** Nghiệm ξ của $x^2 = -1$ là một căn nguyên thủy bậc 4 của đơn vị. Phần tử ξ thuộc F khi và chỉ khi F^* có một phần tử cấp 4. Tương đương với cấp của F^* chia hết cho 4.
- 9.12.** Vì $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ nên dễ dàng chỉ ra rằng $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta^3)] = 2$. Suy ra không có trường con thực sự nào.
- 9.13.** Nhóm cyclic F^* có 80 phần tử. Số nghiệm lần lượt là 80, 1, 8.
- 9.14.** Trên \mathbb{F}_5 , đa thức $f = (x + 2)(x + 3)$. Do $[\mathbb{F}_{25} : \mathbb{F}_5] = 2$ nên f phân rã trong \mathbb{F}_{25} . Trường phân rã của f trên \mathbb{F}_{125} đẳng cấu với \mathbb{F}_{5^6} .

§ 10

10.1. a) Đ b) Đ c) Đ d) Đ e) Đ f) S g) Đ h) Đ i) Đ
j) Đ k) Đ l) S m) S n) Đ o) S p) Đ q) S

10.2. Gọi α là một nghiệm của f , rồi phân tích $f = (x - \alpha)h$ trong $\mathbb{Q}(\alpha)$. Trong Maple, sử dụng lệnh `alias` và `factor` để xác định h . Tiếp tục, tìm dạng nhân tử hóa của h trong $\mathbb{Q}(\sqrt{37})$. Kết quả khó có thể viết ra trên giấy !

10.3. a) Đa thức $-x^3 - 3x^2 + 4x - 1$ bất khả quy có biệt thức bằng 49 nên nhóm Galois đẳng cấu với A_3 .

b) Đa thức $x^3 + 2x^2 - 2x - 2$ bất khả quy có biệt thức bằng 148, nên nhóm Galois đẳng cấu với S_3 .

c) Đa thức $7x^3 + 10x^2 + 5x + 1$ bất khả quy có biệt thức bằng -23, nên nhóm Galois đẳng cấu với S_3 .

d) Đa thức $x^3 + x - 1$ bất khả quy có biệt thức bằng -31, nên nhóm Galois đẳng cấu với S_3 .

- e) Đa thức $x^3 - 2x - 2$ bất khả quy có biệt thức bằng -76 , nên nhóm Galois đẳng cấu với S_3 .
- f) Đa thức $x^3 - x + 1/3$ bất khả quy có biệt thức bằng 1 , nên nhóm Galois đẳng cấu với A_3 .
- g) Đa thức $x^3 - 3x + 1$ bất khả quy có biệt thức bằng 81 , nên nhóm Galois đẳng cấu với A_3 .
- h) Đa thức $x^3 + 2x^2 - 2x - 2$ bất khả quy có biệt thức bằng 148 , nên nhóm Galois đẳng cấu với S_3 .

10.4. a) Đa thức $f = x^4 - x^2 + 4x + 5$ bất khả quy trên \mathbb{Q} (có thể dùng Maple để kiểm tra). Giải thức bậc 3 của f là

$$h = x^3 + 2x^2 - 19x + 16 = (x - 1)(x^2 + 3x - 16)$$

có biệt thức bằng $10512 = 2^4 \cdot 3^2 \cdot 73$. Vì f bất khả quy trên $\mathbb{Q}(\sqrt{73})$ nên nhóm Galois là D_8 .

- b) Đa thức $x^4 + x^2 + 3x + 5$ bất khả quy trên \mathbb{Q} , có giải thức là $h = x^3 - 2x^2 - 19x + 9$ bất khả quy trên \mathbb{Q} . Ngoài ra, biệt thức của

chúng là **33137** không chính phương. Nên nhóm Galois của đa thức là S_4 .

c) Đa thức $x^4 + 3x + 1$ bất khả quy trên \mathbb{Q} (có thể hạn chế trên $\mathbb{Z}_2[x]$), có giải thức là $x^3 + 9 - 4x$ bất khả quy và biệt thức là -1931 . Do đó nhóm Galois là S_4 .

d) Đa thức $x^4 - 4x^2 - 4x - 2$ có nhóm Galois là S_4 .

e) Đa thức $x^4 - 4x - 2$ có nhóm Galois là S_4 .

f) Đa thức $x^4 + 2x^2 - 4$ có giải thức là $h = x^3 - 4x^2 + 20x$. Nhóm Galois đẳng cấu với D_8 .

g) Đa thức $x^4 - x^3 - 3x + 4$ bất khả quy, có giải thức là $x^3 + \frac{3}{4}x^2 - \frac{205}{16}x + \frac{625}{64}$ bất khả quy, có biệt thức $4225 = 5^2 \cdot 13^2$ nên nhóm Galois đẳng cấu với A_4 .

h) Đa thức $x^4 + 2x^3 + 2x^2 - 4x + 2$ bất khả quy, có giải thức là $h = x^3 - x^2 - 17x + 25$ bất khả quy và biệt thức bằng $10816 = 2^6 \cdot 13^2$ nên có nhóm Galois đẳng cấu với A_4 .

i) Đa thức $f = x^4 - 4x^3 + 5x^2 - 2x + 1$ có giải thức là

$$h = x^3 + 2x^2 - 3x = x(x + 3)(x - 1)$$

nên nhóm Galois đẳng cấu với V . Chú ý rằng nếu đặt $x = u + 1$ thì có đa thức theo u là $g = u^4 - u^2 + 1$ nên dễ dàng suy ra g bất khả quy. Chú ý rằng trường phân rã của f là $\mathbb{Q}(\alpha)$ với α là một nghiệm của f . Dùng Maple để tìm các nghiệm còn lại của f theo α .

j) Giống như trường hợp trên, đa thức $x^4 + 2x^2 + 4$ có nhóm Galois đẳng cấu với V .

10.5. Giải thức của đa thức $x^4 + ax^2 + b$ khả quy nên nhóm Galois của nó không thể có quá 8 phần tử. Nếu b chính phương thì nhóm Galois là nhóm $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

10.6. Suy ra trực tiếp từ tiêu chuẩn trong mục 10.3.

10.7. Gọi α là một nghiệm của f thì trường phân rã của f trên F là $F(\alpha)$. Do đó cấp của nhóm Galois G_f là 3. Như thế $G_f = A_3$, suy ra điều phải chứng minh.

§ 11

11.1. a) S b) S c) S d) Đ e) Đ f) S g) Đ

h) Đ i) S j) Đ k) Đ l) Đ m) Đ

11.2. a) Biệt thức của f là $D = -567 = -3^4 \cdot 7$. Một nghiệm của f cho bởi

$$\sqrt[3]{-\frac{5}{2} + \frac{1}{2}\sqrt{21}} + \sqrt[3]{-\frac{5}{2} - \frac{1}{2}\sqrt{21}}.$$

b) Ta có $t^3 - 7t + 6 = (t - 1)(t - 2)(t + 3)$.

c) Ta có $t^3 + t^2 - 2 = (t - 1)(t^2 + 2t + 2)$. Từ công thức nghiệm Cardano, suy ra

$$\sqrt[3]{26 + 15\sqrt{3}} = 2 + \sqrt{3}, \quad \sqrt[3]{26 - 15\sqrt{3}} = 2 - \sqrt{3}.$$

d) Thay $t = u + 5/3$, ta có đa thức $g = u^3 - \frac{13}{3}u + \frac{65}{27}$. Ta có biệt thức của g là $(13)^2$, nên có 3 nghiệm thực. Biểu diễn căn thức của 1 nghiệm của đa thức ban đầu là

$$\sqrt[3]{-\frac{65}{54} + \frac{13}{18}\sqrt{-3}} + \sqrt[3]{-\frac{65}{54} - \frac{13}{18}\sqrt{-3}} + 5/3.$$

e) Giải thức của f là $x^3 + 3/4x^2 + 99/16x + 289/64$. Thay $x = u - 1/4$, ta có đa thức theo u là $h = u^3 + 6u + 3$.

f) Đa thức $f = t^4 + 4t + 2$ bất khả quy, có giải thức là $x^3 - 8x + 16$. Biệt thức của chúng là $-4864 = -2^8 \cdot 19$

g) Đa thức f đã cho có dạng nhân tử hóa

$$f = (t^2 - t + 1)(t^4 + 3t^3 - 3t^2 + 3t + 1).$$

Đặt $g = t^4 + 3t^3 - 3t^2 + 3t + 1$. Khi đó g có giải thức là

$$\begin{aligned} h &= x^3 + \frac{51}{4}x^2 + \frac{899}{16}x + \frac{7569}{64} \\ &= \frac{1}{64}(4x + 29)(16x^2 + 88x + 261). \end{aligned}$$

11.3. Chỉ ra rằng nếu trường K là mở rộng hữu hạn sinh của một trường đếm được F thì K đếm được.

11.4. a) bằng 2 ; b) bằng 0.

11.5. Nếu F có đặc số 3 thì $f = (x + 1)^3$. Xét F có đặc số khác 3. Khi đó f tách được trên F . Biệt thức của f là 81, chính phương trong F nên có nhóm Galois

chứa trong A_3 . Nếu f không bất khả quy và f phân tích thành một đa thức bậc nhất và 1 đa thức bậc 2 bất khả quy thì nhóm Galois chứa một chuyển trí. Vô lí ! Do đó f phân rã trong F .

Ta có thể chỉ ra trực tiếp, nếu β là một nghiệm của f thì các nghiệm còn lại là $2 - \beta - \beta^2, \beta^2 - 2$.

11.6. Chứng minh các đa thức đó bất khả quy và có đúng 2 nghiệm không thực.

a) Có đúng 3 nghiệm thực trong các khoảng $(-2, -1)$; $(0, 1)$ và $(1, 2)$.

b) Tương tự.

c) Tương tự.

d) Chứng minh đa thức có đúng 5 nghiệm thực trong khoảng $(-4, 4)$.

BẢNG KÍ HIỆU VÀ QUY ƯỚC

Kí hiệu	Ý nghĩa
\mathbb{N}	Tập các số tự nhiên
\mathbb{N}^*	Tập các số tự nhiên khác 0
\mathbb{Z}	Vành các số nguyên
\mathbb{Z}_n	Vành các lớp modulo n
\mathbb{Z}_p	Trường các lớp modulo p nguyên tố
\mathbb{F}_{p^n}	Trường hữu hạn có p^n phần tử
\mathbb{Q}	Trường các số hữu tỉ
\mathbb{R}	Trường các số thực
\mathbb{C}	Trường các số phức
S_n	Nhóm đối xứng trên n phần tử
A_n	Nhóm thay phiên trên n phần tử

Kí hiệu	Ý nghĩa
sign	Hàm dấu của phép thế
D_{2n}	Nhóm dihedral
D^\times	Nhóm nhân các phần tử khả nghịch của vành có đơn vị
D^*	Tập các phần tử khác 0 của một vành D
$F[x]$	Vành đa thức 1 biến trên trường F
$F(x)$	Trường phân thức hữu tỉ trên trường F
$\deg(f)$	Bậc của đa thức f
D_f	Biệt thức của đa thức f
$F \subset E, E : F$	Mở rộng trường
$[E : F]$	Bậc của mở rộng trường
$ S $	Lực lượng của tập S
$(G : 1)$	Cấp của nhóm G

Kí hiệu	Ý nghĩa
$(G : H)$	Chỉ số của nhóm con H trong nhóm G
Φ_n	Đa thức chia đường tròn
$F(\alpha)$	Mở rộng đơn sinh ra bởi α trên trường F
$\text{Aut}(F)$	Nhóm các tự đẳng cấu của trường F
$\text{Aut}(E/F)$	Nhóm các F –tự đẳng cấu của $E : F$
$\text{Gal}(E/F)$	Nhóm Galois của mở rộng Galois $E : F$
$\mathcal{T}(H)$	Trường trung gian cố định bởi $H \subset \text{Aut}(E/F)$
$\mathcal{N}(M)$	Nhóm con cố định trường trung gian M của $E : F$

TÀI LIỆU THAM KHẢO

- [1] Dummit D., Foote R., **Abstract Algebra**, Prentice Hall (1991).
- [2] Hungerford T., **Abstract Algebra**, Saunders College Publishing (1990).
- [3] Jacobson N., **Basic Algebra I**, Freeman and Company (1974).
- [4] Milne J.S., **Fields and Galois Theory**, preprint (2002).
- [5] Stewart I., **Galois Theory**, Second edition, Chapman & Hall (1989).
- [6] Weisstein E., **Concise Encyclopedia of Mathematics**, Second edition, Wolfram Research, Inc. (2002).
- [7] The MacTutor History of Mathematics archive
- [8] Nguyễn Chánh Tú, **Sử dụng Maple trong học tập, giảng dạy và nghiên cứu toán học**, Bài giảng cho sinh viên năm thứ 3, Khoa Toán, ĐHSP Huế (2004).
- [9] Nguyễn Chánh Tú, **Mở rộng trường và Lí thuyết Galois**, NXB Giáo Dục (2006), 196 tr.

[10] Trần Vui (chủ biên), Lương Hà, Lê Văn Liêm, Hoàng Tròn, Nguyễn Chánh Tú, Một số xu hướng đổi mới trong dạy học toán ở trường trung học phổ thông, Giáo trình bồi dưỡng thường xuyên giáo viên THPT chu kì III, NXB Giáo Dục (2005), 224 tr.

Chỉ mục

Kí hiệu	
F -đồng cấu	
số lượng.....	66, 272
$F(S)$	53
$F(\alpha)$	Xem mở rộng đơn
$F(s_1, \dots, s_n)$	53
$F[S]$	53
$F[s_1, \dots, s_n]$	53
F^\times	44
K/F	Xem mở rộng trường
$K : F$	Xem mở rộng trường

$\text{Aut}(F)$	22
-----------------------	----

A

Ars Magna.....	5
Artin	115
ánh xạ Frobenius.....	40

B

bất khả quy.....	41
Tiêu chuẩn Eisenstein	29
bậc	
của mở rộng...Xem mở rộng trường	
siêu việt	192

bao đóng
 chuẩn tắc 146, 204
 bao đóng đại số 73, 242
 của trường hữu hạn 159
 tồn tại 73
 biệt thức 179
 biểu diễn vòng xích 32

C

cầu phương hình tròn. Xem dựng hình
 không thể 81
 căn
 chuỗi 202
 căn nguyên thủy 160
 căn thức
 biểu diễn được 202
 công thức

Cardano 215
 Cantor 56
 Cardano
 công thức 201, 215
 chia 3 một góc Xem dựng hình
 không thể 80
 chuẩn tắc
 bao đóng 204
 chuỗi
 chuẩn tắc 223
 hợp thành 224
 chuyển trí 33

D

dấu của phép thế 35
 dựng được 77
 đường thẳng 79

đường tròn.....	79	độc lập đại số.....	191
đa giác đều.....	81, 85, 169	đẳng cấu	
điểm.....	78	của các mở rộng.....	47
đoạn thẳng.....	79	tự.....	110
góc.....	79	đẳng cấu trường	
số thực.....	79	tự.....	22
tập các số.....	83	đại số	
dựng hình		độc lập.....	191
3 bài toán cổ điển.....	77	bao đóng.....	242
thước kẻ và compa.....	77, 86	mở rộng.....	Xem mở rộng
		phần tử.....	55
		đạo hàm hình thức.....	100
		định lí	
		đẳng cấu	
		thứ hai.....	225
		thứ nhất.....	225

D

đóng đại số.....	Xem trường
đồng cấu trường.....	22
<i>F</i> -.....	46
tự.....	22
đặc số.....	23

cơ bản của đại số	171
cơ bản của LT Galois	137
Cauchy	239, 241
phần tử nguyên thủy	125
Sylow	239
đa giác đều dựng được.....	169
đa thức	25
đối xứng	
sơ cấp	194
bất khả quy.....	Xem bất khả quy
nghiem bội của	101
chia đường tròn.....	162
bất khả quy	167
chuẩn tắc	28
nghiem bội của	Xem nghiem bội
tách được	98, 102

tối tiểu	58
tổng quát	191
vành	25

E

Euler	85
hàm	37

F

Fermat	
công thức	40
số nguyên tố	85
Frobenius	
ánh xạ	40

G

gấp đôi hình lập phương ...	Xem dựng hình
-----------------------------	---------------

không thể 80

Galois

tương ứng 115

Gauss 85

Gel'fond 56

giải được

bằng căn thức 202

nhóm không 230

giải thức 187

Lagrange 208

giải thức bậc 3 217

H

hàm

Euler 37

Hermite 56

Hilbert 56

hoàn chỉnh Xem trường

L

Lagrange 208

liên hợp 234

lớp 234

Lindemann 56

Liouville 56

M

Möbius 165

công thức đảo ngược 165

mở rộng

đơn 55

cấu trúc 57, 59

ph.t. nguyên thủy 55

số đồng cấu 66

đại số 56, 71

aben	203
của đồng cầu	47
căn	202
cyclic	203
Galois	127
tiêu chuẩn của	128
hữu hạn	48
là mở rộng đơn	156
tiêu chuẩn	70
hữu hạn sinh	191
tách được	124
trường	45
vô hạn	48
mở rộng trường	48
bậc của	48
cơ sở của	48

Maple	27, 216, 218
sử dụng	158, 165, 188

N

nghiệm đơn	99
nghiệm bội	99
có	99
nghiệm căn thức	213
nhóm	
đối xứng	31
đơn	228
con	
cô định trường trung gian	114
dihedral	30
Galois	127
của đa thức	179
của một đa thức	130

giải được.....	224
Klein	119
liên hợp.....	235
quaternion.....	36
tâm của.....	236
tự đẳng cấu.....	110
thay phiên.....	35
nhóm con	
Sylow.....	239, 240
trung tâm.....	235

P

p-nhóm.....	236
phép chia Euclid.....	26
phép chuyển trí.....	33
phép thế.....	31
chẵn	35

phần tử nguyên thủy	
định lí	125
phân rã.....	91
trường	92
phương trình lớp	235

S

số bội	99
số nguyên tố Fermat.....	Xem Fermat
Schneider.....	56
siêu việt	
phần tử.....	55
trên \mathbb{Q}	56

T

tách được	
đa thức.....	Xem đa thức
mở rộng.....	124

Tâm của nhóm 236
 tương ứng Galois Xem Galois
 trường 22
 đóng đại số 72
 chia đường tròn 160
 con 23
 các phần tử đại số 71
 sinh bởi một tập 53
 hợp thành 145
 hữu hạn 22, 40, 44, 156
 hoàn chỉnh 102
 phân rã 92
 bậc 93
 duy nhất 96
 số đẳng cấu 112
 tồn tại 93

trung gian 51, 114
 cổ định bởi nhóm con 114
 trường con nguyên tố 24

V

vành
 đa thức Xem đa thức
 con sinh bởi một tập 53
 vòng xích 31
 độ dài 31
 độc lập 31