Archive for

MATH 524, Algebra 2, Spring 2023

Bilkent University, Laurence Barker, 20 June 2023.

Source file: arch524spr23.tex

MATH 524, Algebra 2, Spring 2023

Course specification

Laurence Barker, Bilkent University. Version: 1 June 2023

Classes: Tuesdays 09:30 - 10:20, Thursdays 13:30 - 15:20, room SAZ 02.

Office Hours: Tuesdays 08:30 - 09:20, room SA 129.

Instructor: Laurence Barker
e-mail: barker at fen nokta bilkent nokta edu nokta tr.

Course Texts: Required:

• David S. Dummit, Richard M. Foote, “Abstract Algebra”, 3rd edition, (Wiley, New York, 2003). PDF internet downloads available.

• Tsit Yuen Lam, “A First Course in Noncommutative Rings”, (Springer, New York, 1991).

Recommended:

• Joseph Rotman, “Galois Theory”, 2nd edition (Springer, New York, 1998).

• I. Martin Isaacs, “Algebra, a Graduate Course”, (Brooks/Cole, Pacfic Grove, 1993).

Syllabus: The format of the following details is *Week number: Monday date: Subtopics.*

1: Ring theory.

2: Ring theory.

3: Commutative rings.

4: Commutative rings.

5: Fields and field extensions.

6: Fields and field extensions

7: Fields and field extensions.

8: Galois extensions.

9: Galois extensions.

10: Galois theory.

11: Galois theory

12: Galois theory.

13: Applications of Galois theory.

14: Applications of Galois theory.

15: Review.

Assessment:

- Homework, 0%
- Project and Presentation, 25%
- Midterm, 35%, 12 April
- Final, 40%, 12 June

A score of least 20% in the Midterm is needed to qualify to take the Final Exam, otherwise an FZ grade will be awarded.

Projects and presentations

Cazibe Kavalcı, “Discrete valuation rings”.

Mehmat Kırtışoğlu, “Homological algebra and the Künneth theorem”.

Enes Koç, “Semisimplicity and the Hopkins–Levitzki theorem”.

MATH 524: Algebra 2 Midterm 12 April 2023, LJB

1: (20 marks.) Let $\mathbb{F}_5$ denote the field with order 5.

(a) Find an irreducible polynomial $f(X)$ of degree 3 over $\mathbb{F}_5$. Prove that your polynomial $f(X)$ is irreducible.

(b) For your polynomial $f(X)$, write $\alpha = X + (f(X))$. Thus, $\mathbb{F}_5[\alpha] = \mathbb{F}_5[X]/(f(X))$. Express α^{-1} as a linear combination of the basis elements 1, α, α^2 of $\mathbb{F}_5[\alpha]$.

2: (20 marks.) Let E/F be field extension, and let K and L be subfields of E containing F. We define the **join** KL to be the smallest subfield of E containing K and L.

(a) Show that if the extensions K/F and L/F are finite then the extension KL/F is finite and $|KL : F| \leq |K : F|.|L : F|$.

(b) Show that if, furthermore, $|K : F|$ and $|L : F|$ are coprime, then $|KL : F| = |K : F|.|L : F|$.

3: (20 marks.) We define the **field of constructible numbers** $\mathbb{E}$ to be the smallest subfield of $\mathbb{C}$ such that, given $x \in \mathbb{C}$ satisfying $x^2 \in \mathbb{E}$, then $x \in \mathbb{E}$. Thus, $\mathbb{E}$ is the set of complex numbers x such that there exists a sequence $x_0, ..., x_n = x$ with $x_0^2 \in \mathbb{Q}$ and each $x_m^2 \in \mathbb{Q}[x_0, ..., x_{m-1}]$. Show that there exists an automorphism θ of $\mathbb{E}$ such that $\theta(\sqrt{2}) = -\sqrt{2}$.

4: (20 marks.) Show that $\mathbb{Z}[e^{2\pi i/3}]$ is a principal ideal domain.

5: (20 marks.) Let $p_1, ..., p_n$ be distinct primes. Show that $|\mathbb{Q}[\sqrt{p_1}, ..., \sqrt{p_n}\,] : \mathbb{Q}| = 2^n$.

Solutions to Midterm

1: Part (a). We shall show that the polynomial $f(X) = X^3 + X + 1$ is irreducible over $\mathbb{F}_5$. The values at 0, 1, 2, 3, 4 are 1, 3, 1, 1, 4, respectively, so $f(X)$ has no linear factor. Therefore, $f(X)$ is irreducible.

Part (b). We have $\alpha^3 + \alpha + 1 = 0$. Therefore, $\alpha^{-1} = -1 - \alpha^2$.

2: Part (a). We argue by induction on $|L : F|$. The case $L = F$ is trivial. Suppose $L > F$ and let $\alpha \in L - F$.

First consider the case where $L = F[\alpha]$. Then $KL = K[\alpha]$. The minimal polynomial of α over K divides the minimal polynomial of α over F, so

$$|KL : K| = |K[\alpha] : K| \leq |F[\alpha] : F| = |L : F| \, .$$

Hence $|KL : F| = |KL : K|.|K : F| \leq |L : F|.|K : F|$.

Now suppose $L > F[\alpha]$. Applying the inductive hypothesis twice,

$$|KL : F| = |KL : F[\alpha|.|F[\alpha] : F| \leq |KF[\alpha] : F|.|L : F[\alpha]|.|F[\alpha] : F|$$

$$= |KF[\alpha] : F|.|L : F[\alpha]| \leq |K : F|.|F[\alpha] : F|.|L : F[\alpha]| = |K : F|.|L : F| \, .$$

Part (b). By an equality above, $|K : F|$ divides $|KL : F|$. Similarly, $|L : F|$ divides $|KL : F|$. So if $|K : F|$ and $|L : F|$ are coprime, $|K : F|.|L : F|$ divides $|KL : F|$ and the required equality follows.

3: Let $\mathcal{P}$ be the set of pairs (E, ϕ) such that $E \leq \mathbb{E}$ and $\phi : E \to \mathbb{E}$ is a map extending θ. We partially order $\mathcal{P}$ by inclusion and restriction. We have $(\mathbb{Q}, \theta) \in \mathcal{P}$, so $\mathcal{P} \neq \emptyset$. The unionset of a chain $\mathcal{C}$ in $\mathcal{P}$ is an upper bound for $\mathcal{C}$. So we can apply Zorn's Lemma, which tells us that $\mathcal{P}$ has a maximal element (M, ψ). We must show that $M = \mathbb{E}$ and ψ is an automorphism.

Suppose, for a contradiction, that $M < \mathbb{E}$. Then there exists $\alpha \in \mathbb{E}$ such that $\alpha^2 \in M$. Let $f(X) = X^2 - \alpha^2$ as a polynomial over M. Let β be a root in $\mathbb{E}$ to the polynomial $\psi(f(X)) = X^2 - \psi(\alpha^2)$ over $\psi(M)$. Then ψ extends to a map $M[\alpha] \to \psi(M)[\beta]$ such that $\alpha \mapsto \beta$. This contradicts the maximality of M. We have shown that $M = \mathbb{E}$.

Suppose, for another contradiction, that the endomorphism $\psi : \mathbb{E} \to \mathbb{E}$ is not an automorphism. Since ψ is injective, ψ cannot be surjective. Let $\gamma \in \mathbb{E} - \psi(\mathbb{E})$ such that $\gamma^2 \in \psi(\mathbb{E})$. Let $a \in \mathbb{E}$ such that $\psi(a) = \gamma^2$. The polynomial $g(X) = X^2 - a$ splits completely over $\mathbb{E}$, so the polynomial $\psi(g(X)) = X^2 - \gamma^2$ splits completely over $\psi(E)$. We deduce that $\gamma \in \psi(\mathbb{E})$, which is a contradiction, as required.

4: Write $\omega = e^{2\pi i/3}$. Given $a \in \mathbb{Z}[\omega]$, we define $N(r) = aa^*$ where a^* denotes the complex conjugate of a. Writing $a = m + n\omega$ with $m, n \in \mathbb{Z}$, then $N(a) = m^2 + n^2 - mn \in \mathbb{N}$. We shall show that N is a Euclidian norm. That will suffice, since every Eudlidian domain is a principal ideal domain.

The elements of $\mathbb{Z}[\omega]$ form a lattice of equilateral triangles in the complex plane. The sides of the triangles have length 1. By straightforward trigonometry, the circumcircle of any one of the triangles has radius $1/\sqrt{3}$. Let $a, b \in \mathbb{Z}[\omega]$ with $b \neq 0$. Let q be a lattice point at minimal distance from the complex number a/b. Then $|a/b - q|^2 \leq 1/3$. Letting $r \in \mathbb{Z}[\omega]$ such that $a = bq + r$, then $|r| < |b|$. Squaring, $N(r) < N(b)$. So N is a Euclidian norm, as required.

5: For $I \subseteq \{1, ..., , n\}$, we define

$$r_I = \prod_{i \in I} \sqrt{p_i} \, .$$

We shall show that the set consisting of the r_I is a $\mathbb{Q}$-basis for the field $K_n = \mathbb{Q}[\sqrt{p_1}, ..., \sqrt{p_n}]$ and, moreover, for every subset $I \subseteq \{1, ..., n\}$, there is an automorphism σ_I of K_n such that $\sigma(\sqrt{p_i}) = -\sqrt{p_i}$ if and only if $i \in I$. For a contradiction, consider a counter-example with n minimal. Plainly, $n \geq 2$.

We claim that $K_{n-1} < K_n$. Supposing otherwise, then $\sqrt{p_n} \in K_{n-1}$ and we can write

$$\sqrt{p_n} = \sum_{J \subseteq \{1,...,n-1\}} a_J r_J$$

with each $a_J \in \mathbb{Q}$. If $1 \notin J$ for all J satisfying $a_J \neq 0$, then we obtain a contradiction by considering $\mathbb{Q}[\sqrt{p_2}, ..., \sqrt{p_n}]$. If $1 \in J$ for all J satisfying $a_J \neq 0$, then

$$p_n = p_1 (\prod_J a_J r_J / \sqrt{p_1})^2$$

and the squared term is both rational and an algebraic integer, hence a rational integer, which contradicts the Fundamental Theorem of Arithmetic. So there exist indices J and J' such that $a_J \neq 0 \neq a_{J'}$ and $J \ni 1 \notin J'$. Part of the inductive hypothesis is that for each $K \subseteq \{1, ..., n-1\}$, there is an automorphism σ_K such that $\sigma_K(\sqrt{p_k}) = -\sqrt{p_k}$ if and only if $k \in K$. We have

$$\pm\sqrt{p_n} = \sigma_{\{1\}}1(\sqrt{p_n}) = \sum_J s_J a_J r_J$$

where s_J is 1 or -1 depending on whether $1 \in J$ or $1 \notin J$, respectively. For some of the nonzero terms of the summation, we have $s_J = 1$, while for some of the nonzero terms, we have $s_J = -1$. By comparing with the above equality for $\sqrt{p_n}$, we obtain a nonzero $\mathbb{Q}$-linear relation between the r_J. This contradicts the condition that the r_J comprise a $\mathbb{Q}$-basis for K_{n-1}. We have established the claim.

Since an automorphism of K_n is determined by its actions on the elements $\sqrt{p_i}$ for $1 \leq i \leq n$, we have $|\mathrm{Aut}(K_n)| \leq 2^n$ and it remains only to show that $|\mathrm{Aut}(K_n)| = 2^n$. Now K_n is a splitting field for $X^2 - p_n$ over K_n, so each σ_K extends to an automorphism τ_K of K_n. On the other hand, K_n is a splitting field for $\prod_{j=1}^{n-1}(X^2 - p_j)$ over $\mathbb{Q}[\sqrt{p_n}]$, so the nontrivial automorphim $\sqrt{p_n} \mapsto -\sqrt{p_n}$ of $\mathbb{Q}[\sqrt{p_n}]$ extends to an automorphism τ of K_n. The 2^n automorphisms τ_J and $\tau\tau_J$ of K_n are mutually distinct. We have confirmed that $|\mathrm{Aut}(K_n)| = 2^n$, as required.

MATH 524: Algebra 2 Final 12 June 2023, LJB

1: (25 marks.) Let $f(X)$ be the minimal polynomial of $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$. Let E be the splitting field for $f(X)$ over $\mathbb{Q}$.

(a) Show that $|E : \mathbb{Q}| = 8$.

(b) Find the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ up to isomorphism.

(c) Find the number of intermediate fields $\mathbb{Q} \leq L \leq E$.

(d) Find the number of L such that $\mathbb{Q} \leq L \leq E$ and $L/\mathbb{Q}$ is Galois.

2: (25 marks.) Let E be the splitting field for $X^{12}-1$ over $\mathbb{Q}$. Find all the strictly intermediate fields $\mathbb{Q} < L < E$, expressing them all in the form $L = \mathbb{Q}[a]$ with $a \in E$.

3: (25 marks.) Let K/F be a finite-degree field extension with characteristic 0. Show that there exists an extension field E of K such that

$$|E : F| \leq |K : F|!$$

and E/F is a Galois extension.

4: (25 marks.) Let A be a finite abelian group. Show that there exists a positive integer n and a field L such that $\mathbb{Q} \leq L \leq \mathbb{Q}_n$ and $\mathrm{Gal}(L/\mathbb{Q}) \cong A$. Here, $\mathbb{Q}_n$ denotes the cyclotomic field with index n. (You may find it helpful to use Dirichlet's Theorem, which asserts that, given coprime positive integers a and b, then there are infinitely many primes in the set $\{a + mb : m \in \mathbb{N}\}$.)

Solutions to Final

1: Part (a). Let $a = \sqrt{1+\sqrt{2}}$. We have $(a^2-1)^2 = 2$, in other words, $a^4 - 2a^2 - 1 = 0$. So $f(X)$ divides $X^4 - 2X^2 - 1$.

Plainly, $\mathbb{Q}[\sqrt{2}\,] \leq \mathbb{Q}[a] \leq E$. Since E is a splitting field over $\mathbb{Q}$, there exists $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(\sqrt{2}\,) = -\sqrt{2}$. We have $\sigma(a)^2 = 1 - \sqrt{2}$. It is now clear that the roots to $f(X)$ are $\pm\sqrt{1 \pm \sqrt{2}}$. In particular, $\deg(f(X)) = 4$ and $f(X) = X^4 - 2X^2 - 1$. Noting that $\mathbb{Q}[a] \leq \mathbb{R} \not\ni \sigma(a)$, we deduce that

$$|E : \mathbb{Q}| = |\mathbb{Q}[a, \sigma(a)] : \mathbb{Q}[a]|.|\mathbb{Q}[a] : \mathbb{Q}| = 2.4 = 8 \ .$$

Part (b). Writing $G = \mathrm{Gal}(E/\mathbb{Q})$, we claim that $G \cong D_8$. By part (a), $|G| = 8$. But G acts faithfully on the 4 roots to $f(X)$, so G embeds in S_4. The claim follows because the Sylow 2-subgroups of S_4 are isomorphic to D_8.

Part (c). The number of intermediate L is 10. Indeed, this is the number of subgroups of D_8, the subgroups being 1, 5, 1, 2, 1 copies of C_1, C_2, C_4, V_4, D_8, respectively.

Part (d). The number of L with $L/\mathbb{Q}$ Galois is 6, since this is the number of normal subgroups of D_8, the only non-normal subgroups of D_8 being 4 of those isomorphic of C_2.

2: Let $\zeta = e^{2\pi i/6} = (\sqrt{3} + i)/2$, which is a primitive 12-th root of unity. Since $(\mathbb{Z}/12)^\times = \{1, 5, 7, 11\}$, the other Galois conjugates of ζ are

$$\zeta^5 = (-\sqrt{3} + i)/2 \ , \qquad \zeta^7 = (-\sqrt{3} - i)/2 \ , \qquad \zeta^{11} = (\sqrt{3} - i)/2 \ .$$

We have $\zeta + \zeta^{11} = \sqrt{3}$ and $\zeta + \zeta^5 = i$. So 3 of the strictly intermediate fields L are $\mathbb{Q}[\sqrt{3}\,]$ and $\mathbb{Q}[i\sqrt{3}\,]$ and $\mathbb{Q}[i]$. To see that there are no other possibilities for L, we apply the Fundamental Theorem of Galois Theory and observe that

$$\mathrm{Gal}(\mathbb{Q}_{12}/\mathbb{Q}) \cong (\mathbb{Z}/12)^\times \cong (\mathbb{Z}/4)^\times \times (\mathbb{Z}/3)^\times \cong V_4$$

which has precisely 3 proper (non-trivial and strict) subgroups.

Comment: Let ρ, σ, τ be the elements of $\mathrm{Gal}(\mathbb{Q}_{12}/\mathbb{Q})$ sending ζ to ζ^5, ζ^7, ζ^{11}, respectively. Then ρ fixes i, while τ fixes $\sqrt{3}$. So the element $\sigma = \rho\tau$ fixes $i\sqrt{3}$. Therefore, the 3 proper subgroups $\langle\rho\rangle$, $\langle\sigma\rangle$, $\langle\tau\rangle$ of $\mathrm{Gal}(\mathbb{Q}_{12}/\mathbb{Q})$ have fixed fields

$$\mathbb{Q}_{12}^{\langle\rho\rangle} = \mathbb{Q}[i] \ , \qquad \mathbb{Q}_{12}^{\langle\sigma\rangle} = \mathbb{Q}[i\sqrt{3}\,] \ , \qquad \mathbb{Q}_{12}^{\langle\tau\rangle} = \mathbb{Q}[\sqrt{3}\,] \ .$$

3: Let us first note that, combining Artin's Theorem with the Fundamental Theorem of Galois Theory, we obtain following standard corollary: every finite-degree characteristic 0 field extension C/D is simple, that is, $C = D[a]$ for some $a \in C$. Indeed, writing $C = D[a_1, ..., a_r]$, letting $f_i X$ be the minimal polynomial of a_i over D and letting B be the splitting field over D for the product $f_1(X)...f_r(X)$, then $B \geq C \geq D$ and the Fundamental Theorem of Galois Theory implies that there are only finitely many intermediate fields between B and D. Perforce, there are only finitely many intermediate fields between C and D whence, by Artin's Theorem, C/D is simple.

In particular, $K = F[a]$ for some $a \in K$. Let $f(X)$ be the minimal polynomial for a over F. Let $n = \deg(f(X)) = |K : F|$. Let E be a splitting field for $f(X)$ over K. Then E is a splitting field for $f(X)$ over F. So E/F is Galois. It remains only to show that $|E : F| \leq n!$.

Let a_0, ..., a_{n-1} be the roots of $f(X)$ in E and let $L_m = F[a_0, ..., a_m]$, understanding that $L_{-1} = F$. Since a_0, ..., a_{m-1} belong to L_{m-1}, the degree of the minimal polynomial of a_m over L_{m-1} is at most $n - m$. In other words, $|L_m : L_{m-1}| \leq n - m$. By the Tower Law for Degrees of Field Extensions, $|E : F| \leq \prod_m (n - m) \leq n!$.

4: The Structure Theorem for Finite Abelian Groups tells us that $A \cong C_{a_1} \times ... \times C_{a_r}$ for some positive integers r and a_1, ..., a_r. By Dirichlet's Theorem, there exist mutually distinct primes p_1, ..., p_r such that each $p_i \equiv 1$ modulo a_i. Put $n = p_1 ... p_r$. Writing $p_i - 1 = a_i b_i$, we have canonical isomorphisms

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p_1)^\times \times ... \times (\mathbb{Z}/p_r)^\times \cong C_{a_1 b_1} \times ... \times C_{a_r b_r} \ .$$

Let B be the subgroup of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ corresponding, via those isomorphisms, to the subgroup $C_{b_1} \times ... \times C_{b_r}$ of $C_{a_1 b_1} \times ... \times C_{a_r b_r}$. Let L be the subfield of $\mathbb{Q}_n$ fixed by B. By the Fundamental Theorem of Galois Theory,

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})/B \cong C_{a_1 b_1}/C_{b_1} \times ... \times C_{a_r b_r}/C_{b_r} \cong A \ .$$

Comment: A deeper result, the Kronecker–Weber Theorem, is as follows: given a finite-degree Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, then K embeds in $\mathbb{Q}_n$ for some positive integer n. It is not hard to show that this is equivalent to the assertion that, given an algebraic number x, letting E be the splitting field of the minimal polynomial of x, then x is a $\mathbb{Q}$-linear combination of roots of unity if and only if $\mathrm{Gal}(E/\mathbb{Q})$ is abelian.