Archive for

MATH 324, Algebra 2, Spring 2023

Bilkent University, Laurence Barker, 20 June 2023.

Source file: arch324spr23.tex

MATH 324, Algebra 2, Spring 2023

Course specification

Laurence Barker, Bilkent University. Version: 1 June 2023.

Classes: Wednesdays 09:30 - 10:20, Fridays 13:30 - 15:20, room SAZ 04.

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

For all students, those doing well and aiming for an A, those doing badly and aiming for a C, Office Hours is an opportunity to come and ask questions.

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

Assistant: Anıl Tokmak.

Course Texts: Required:

- David S. Dummit, Richard M. Foote, "Abstract Algebra", 3rd edition, (Wiley, New York, 2003). PDF internet download available.

Recommended:

- For gentle introduction to early parts: Thomas W. Judson, "Abstract Algebra", 2002, free download from http://abstract.ups.edu.
- More advanced: Joseph Rotman, "Galois Theory", 2nd edition (Springer, New York, 1998).

Syllabus: The format of the following details is *Week number: Monday date: Subtopics, Dummit–Foote section number.*

1: Euclidian domains and principal ideal domains, 8.1, 8.2.

2: Unique factorization domains, 8.3.

3: Polynomial rings over UFDs, 9.1 - 9.5.

4: Field extensions, 13.1, 13.2.

5: Ruler-and-compass constructions, 13.3

6: Splitting fields, 13.4.

7: Separable extensions, 13.5.

8: Cyclotomic extensions, 13.6.

9: Galois extensions 14.1.

10: The Fundamental Theorem of Galois Theory, 14.2.

11: Composite extensions. The Primitive Element Theorem, 14.4

12: The Galois group of a cyclotomic extension, 14.5.

13: Calculating Galois groups, 14.6.

14: The unsolvability of the quintic.

15: Review.

Assessment:

- Homework, 0% (but practice with the homework is the best way of training for the exams!)
- Presentation, 0% (giving a presentation is optional)
- Quizzes, 10%
- Midterm 40%, 12 April
- Final, 50%, 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.

75% attendance is compulsory.

Asking questions in class is very helpful. It makes the classes come alive, and it tends to improve my presentation. The rule for talking in class is: if you speak, then you must speak to everyone in the room.

Quizzes, with solutions

MATH 324, *Algebra 2*, Spring 2023, Laurence Barker

version: 2 June 2023

Quiz 1: *28 April.* Let $\omega \in \mathbb{F}_4 - \mathbb{F}_2$.

(a) What is the degree of the minimal polynomial of ω over $\mathbb{F}_2$?

(b) What is the minimal polynomial of ω over $\mathbb{F}_2$?

Solution: Part (a). Since $\mathbb{F}_4 = \mathbb{F}_2[\omega]$, the degree is $|\mathbb{F}_4 : \mathbb{F}_2| = 2$.

Part (b). The minimal polnomial must be the only polynomial of degree 2 over $\mathbb{F}_2$ that has no root in $\mathbb{F}_2$. So the minimal polynomial is $X^2 + X + 1$..

Comment: Alternatively, for part (b), ω is a root to the polynomial

$$X^3 - 1 = (X - 1)(X^2 + X + 1)$$

and the factor $X^2 + X + 1$, having no root in $\mathbb{F}_2$, must be the minimal polynomial of ω.

Quiz 2: *3 May.* Let p and q be distinct primes. Let g be the automorphism of the field $E = \mathbb{Q}[\sqrt{p}, \sqrt{q}]$ such that $g(\sqrt{p}) = \sqrt{p}$ and $g(\sqrt{q}) = -\sqrt{q}$. Let $G = \langle g \rangle$. You may assume that

$$E = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{p} \oplus \mathbb{Q}\sqrt{q} \oplus \mathbb{Q}\sqrt{pq}$$

as a direct sum of 1-dimensional subspaces. What is the fixed field E^G?

Solution: The fixed field is $E^G = \mathbb{Q}[\sqrt{p}]$.

Comment: The fixed field can also be expressed as $E^G = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{p}$.

Quiz 3: *5 May.* Consider the group $V_4 = \{1, x, y, z\}$. Find the subgroups of V_4. How many subgroups are there?

Solution: The subgroups are 1 and $\langle x \rangle$ and $\langle y \rangle$ and $\langle z \rangle$ and V_4. There are 5 of them.

Quiz 4: *10 May.* What are the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$? (Express them all in the form $\mathbb{Q}[\alpha_1, \alpha_2, ...]$.)

Solution: They are $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Quiz 5: *12 May.* Find all the subgroups of the group $Q_8 = \{1, -1, i, j, k, -i, -j, -k\}$. How many of those subgroups are normal?

Solution: The subgroups are 1, $\langle -1 \rangle$, $\langle i \rangle$, $\langle j \rangle$, $\langle k \rangle$, Q_8. All 6 of them are normal.

Quiz 6: *17 May.* Let E be the splitting field for $X^4 - X^2 - 1$ over $\mathbb{Q}$. We have seen that $\mathrm{Gal}(E/\mathbb{Q}) \cong D_8$. Let L be the intermediate field $\mathbb{Q} < L < E$ such that $|L : \mathbb{Q}| = 4$ and $L/\mathbb{Q}$ is Galois. Find, up to isomorphism, the group $\mathrm{Gal}(L/\mathbb{Q})$.

Solution: Identifying $\mathrm{Gal}(E/\mathbb{Q}) = D_8$, the subgroup $\mathrm{Gal}(E/L)$ fixing L is a normal subgroup of D_8 with order 2. There is only one such subgroup, namely $\mathrm{Gal}(E/L) = Z(D_8)$. We have $\mathrm{Gal}(L/\mathbb{Q}) = D_8/Z(D_8) \cong V_4$.

The next quiz will be similar. Beforehand, try to ensure that:

- You understand the Fundamental Theorem of Galois Theory. (There will be no need to memorize it. As soon you have understood the theorem, it will become fixed in your memory forever.)
- You know how to find the subgroups of a small given group.
- You know how to determine, up to isomorphism, the quotient of a given normal subgroup of a given small group. For instance, $A_4/V_4 \cong C_3$ and $S_4/A_4 \cong C_2$.
- You can put those three items together and do exercises such as Quiz 6.

Quiz 7: *24 May.* Let E/F be a Galois extension with $\mathrm{Gal}(E/F) \cong A_4$. Let $F \leq L \leq E$ with $\mathrm{Gal}(E/L) \cong V_4$. Find $\mathrm{Gal}(L/F)$ up to isomorphism.

Solution: We have $\mathrm{Gal}(L/F) \cong A_4/V_4 \cong C_3$.

Quiz 8: *31 May.* Express $\mathrm{Gal}(\mathbb{Q}_{30}/\mathbb{Q})$ as a direct product of cyclic groups and evaluate $|\mathrm{Gal}(\mathbb{Q}_{30}/\mathbb{Q})|$.

Solution: Using the Chinese Remainder Theorem,

$$\mathrm{Gal}(\mathbb{Q}_{30}/\mathbb{Q}) \cong (\mathbb{Z}/30)^\times \cong (\mathbb{Z}/2)^\times \times (\mathbb{Z}/3)^\times \times (\mathbb{Z}/5)^\times \cong C_2 \times C_4$$

which has order $\phi(30) = 8$.

Quiz 9: *2 June.* Find the smallest positive integer n such that there exists an intermediate field $\mathbb{Q} \leq E \leq \mathbb{Q}_n$ with $\mathrm{Gal}(E/\mathbb{Q}) \cong C_{11}$.

Solution: Since $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$, we are to find the smallest n such that C_{11} is isomorphic to a quotient group of $(\mathbb{Z}/n)^\times$. In view of the Chinese Remainder Theorem, $n = 23$.

MATH 324: Algebra 2 Midterm 12 April 2023, LJB

The duration of the exam is 120 minutes. It is a closed book exam.

1: (20 marks.) Evaluate $\gcd(X^4+5X^3+6X^2+10X+8, X^3+6X^2+11X+12)$ in $\mathbb{Q}[X]$.

2: (20 marks.) Let $\mathbb{F}_3$ denote the field with order 3. Thus, $\mathbb{F}_3 = \{0, 1, 2\}$. Let

$$R = \mathbb{F}_3[X]/(X^3+2X+1) .$$

(a) Is R a field?

(b) Evaluate $|R|$, the cardinality of the set R.

3: (20 marks.) Let $f(X) = X^3+3X^2+3X+3$ and $g(X) = X^4+3X^3+3X^2+3X+3$. Let α and β be roots to $f(X)$ and $g(X)$, respectively. Evaluate:

(a) the degree $|\mathbb{Q}[\alpha] : \mathbb{Q}|$,

(b) the degree $|\mathbb{Q}[\beta] : \mathbb{Q}|$,

(c) the degree $|\mathbb{Q}[\alpha, \beta] : \mathbb{Q}|$.

4: (20 marks.) Let F be a field. Consider the polynomial ring with two variables

$$F[X, Y] = F[X][Y] .$$

Show that $F[X, Y]$ is not a Euclidian domain.

5: (20 marks.) Let $n \geq 3$ and let E be the splitting field for $X^{2^n} - 1$ over $\mathbb{Q}$.

(a) Show that $\sqrt{2} \in E$.

(b) Show that there exists an automorphism θ of E such that $\theta(\sqrt{2}) = -\sqrt{2}$.

(c) Show that, for exactly half of the automorphisms ϕ of E, we have $\phi(\sqrt{2}) = -\sqrt{2}$.

Solutions to Midterm

1: By considering coeffients of X^4 and X^3, we have

$$X^4+5X^3+6X^2+11X+12 = (X-1)(X^3+6X^2+11X+12)+aX^2+bX+c$$

for some $a, b \in \mathbb{Z}$. Now

$$(X-1)(X^3+6X^2+11X+12) = X^4+5X^3+5X^2+X-12 .$$

So $a = 1$ and $b = 9$ and $c = 20$. Therefore,

$$\gcd = \gcd(X^3+6X^2+11X+12, X^2+9X+20) .$$

By considering coefficients of X^3 and X^2, we have

$$X^3+6X^2+11X+12 = (X-3)(X^2+9X+20)+dX+e$$

for some $d, e \in \mathbb{Z}$. Since

$$(X-3)(X^2+9X+20) = X^3+6X^2-7X-60$$

we have $d = 18$ and $e = 72$. So

$$\mathrm{gcd} = \mathrm{gcd}(X^2+9X+20, X+4) \; .$$

Finally, $X^2+9X+20 = (X+5)(X+4)$. So gcd $= X+4$.

2: Part (a). Let $f(X) = X^3+2X+1$. We have $f(1) = f(2) = 1$, so $f(X)$ has no roots in $\mathbb{F}_3$. It follows that $f(X)$ is irreducible. Therefore, R is a field.

Part (b). Let α be the image of X in R. Then $R = \mathbb{F}_3[\alpha]$ and R has $\mathbb{F}_3$-basis $\{1, \alpha, \alpha^2\}$. So $|R| = |\mathbb{F}_3|^3 = 3^3 = 27$.

3: Part (a). By Eisenstein's Criterion, $f(X)$ is irreducible, so $|\mathbb{Q}[\alpha] : \mathbb{Q}| = \deg(f(X)) = 3$.

Part (b). By Eisenstein's Criterion, $g(X)$ is irreducible, so $|\mathbb{Q}[\beta] : \mathbb{Q}| = \deg(g(X)) = 4$.

Part (c). Since $|\mathbb{Q}[\alpha] : \mathbb{Q}|$ and $|\mathbb{Q}[\beta] : \mathbb{Q}|$ are coprime,

$$|\mathbb{Q}[\alpha, \beta] : \mathbb{Q}| = |\mathbb{Q}[\alpha] : \mathbb{Q}|.|\mathbb{Q}[\beta] : \mathbb{Q}| = 12 \; .$$

4: The ideal (X, Y) is not principal. So $F[X][Y]$ is not a PID. Perforce, $F[X][Y]$ is not an ED.

5: Part (a). The complex numbers $\zeta = (1+i)/\sqrt{2}$ and $\overline{\zeta} = (1-i)/\sqrt{2}$ are 8-th roots of unity, so we may assume that $\zeta, \overline{\zeta} \in E$. Hence $\sqrt{2} = \zeta + \overline{\zeta} \in E$.

Part (b). Plainly, there is a $\mathbb{Q}$-automorphism ψ of $\mathbb{Q}[\sqrt{2}]$ given by $\psi(\sqrt{2}) = -\sqrt{2}$. Since E is a splitting field for $X^{2^n} - 1$ over $\mathbb{Q}[\sqrt{2}]$, the automorphism ψ extends to an automorphism of E.

Part (c). For every automorphism η of E, we have $\eta(\sqrt{2}) = \pm\sqrt{2}$. So there is a function $\sigma : \mathrm{Aut}(E) \to \{\pm 1\}$ such that $\eta(\sqrt{2}) = \sigma(\eta)\sqrt{2}$. Plainly, σ is a group homomorphism. By the First Isomorphism Theorem for groups,

$$|\mathrm{Ker}(\sigma)| = |\mathrm{Aut}(E) - \mathrm{Ker}(\sigma)| = |\mathrm{Aut}(E)|/2 \; .$$

We have $\mathrm{Aut}(E) - \mathrm{Ker}(\sigma) = \{\phi \in \mathrm{Aut}(E) : \phi(\sqrt{2}) = -\sqrt{2}\}$.

Comment: Part (c) can also be done without any group theory. We are to show that the sets $\Psi = \{\psi \in \mathrm{Aut}(E) : \psi(\sqrt{2}) = \sqrt{2}\}$ and $\Phi = \{\phi \in \mathrm{Aut}(E) : \psi(\sqrt{2}) = -\sqrt{2}\}$ have the same size. That follows because there is a bijective correspondence $\Psi \leftrightarrow \Phi$ such that $\psi \leftrightarrow \phi$ when $\theta_\circ \psi = \phi$.

MATH 324: Algebra 2 Final 12 June 2023, LJB

The duration of the exam is 120 minutes. It is a closed book exam.

1: (10 marks.) Let $f(X)$ be a polynomial over $\mathbb{R}$ such that not all of the roots of $f(X)$ are real. Let E be the splitting field for $f(X)$ over $\mathbb{R}$. Determine the Galois group $\mathrm{Gal}(E/\mathbb{R})$ up to isomorphism.

2: (20 marks.) Let $f(X) = X^2 - X - 1$ as a polynomial over $\mathbb{Q}$. Let E be the splitting field for $f(X)$ over $\mathbb{Q}$.

(a) Evaluate the degree $|E : \mathbb{Q}|$.

(b) How many fields L are there such that $\mathbb{Q} \leq L \leq E$?

(c) How many $\mathbb{Q}$-automorphisms of E are there?

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

3: (30 marks.) Let $g(X) = X^3 - 3X + 101$ as a polynomial over $\mathbb{Q}$. Let K be the splitting field for $g(X)$ over $\mathbb{Q}$.

(a) Explain why $g(X)$ is irreducible.

(b) Show that $g(X)$ has exactly one real root.

(c) Show that the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ has an element with order 2.

(d) Determine $\mathrm{Gal}(K/\mathbb{Q})$ up to isomorphism.

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

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

4: (20 marks.) For a positive integer n, let $\Phi_n(X)$ denote the cyclotomic polynomial with index n (the minimal polynomial of the primitive n-th roots of unity). Show that $\Phi_n(0) = \pm 1$.

5: (20 marks.) Show that the extension $\mathbb{Q}[\sqrt{1+\sqrt{2}}\,]/\mathbb{Q}$ is not Galois. Using that observation, give a counter-example to the assertion: "Given fields $D \geq E \geq F$ such that the extensions D/E and E/F are Galois, then the extension D/F is Galois."

Solutions to Final

1: We have $E = \mathbb{C}$ and $\mathrm{Gal}(E/\mathbb{R}) \cong C_2$.

Comment: The non-trivial element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is complex conjugation.

2: Part (a). The roots to $f(X)$ are $(1 \pm \sqrt{5})/2$, so $E = \mathbb{Q}[\sqrt{5}]$. Evidently, $|E : \mathbb{Q}| = 2$.

Part (b). By part (a), the number of such L is 2.

Part (c). There is a unique non-trivial $\mathbb{Q}$-automorphism of E, namely the automorphism given by $\sqrt{5} \mapsto \sqrt{5}$. So the answer is 2.

Part (d). By part (c), $\mathrm{Gal}(E/\mathbb{Q}) \cong C_2$.

3: Part (a). Suppose $g(X)$ is not irreducible. Since $\deg(g(X)) = 3$, there must exist a rational root q of $g(X)$. Noting that 101 is prime, the rational root test implies that $q = \pm 101$. But, plainly, $g(-101) < 0 < g(101)$, which is a contradiction.

Part (b). The polynomial function $g : \mathbb{R} \to \mathbb{R}$ has derivative $x \mapsto 3(x^2 - 1)$, so the only local maxima and minima are at $x = -1$ and $x = 1$. Since $g(-1)$ and $g(1)$ are both positive, $g(X)$ has only one real root (for some value of x less than -1).

Part (c). Since $g(X)$ is an irreducible cubic polynomial, $g(X)$ has exactly 2 nonreal roots. Embedding K in $\mathbb{C}$, complex conjugation fixes the real root of $g(X)$ and interchanges the 2 non-real roots.

Part (d). Write $G = \mathrm{Gal}(K/\mathbb{Q})$. The action of G on the 3 roots to $g(X)$ gives rise to an embedding of G in S_3. That action is transitive, so G owns a 3-cycle. By part (c), G owns a transposition. Therefore, $G \cong S_3$.

Part (e). By the Fundamental Theorem of Galois theory, the number of m of intermediate L is the number of subgroups of S_3. The subgroups of S_3 are C_1, C_2, C_3, S_3 appearing 1, 3, 1, 1 times, respectively. So $m = 6$.

Part (f). Let n be the number of L such that $\mathrm{Gal}(L/\mathbb{Q})$ is Galois. By the Fundamental Theorem of galois Theory again, n is the number of normal subgroups of S_3. The normal subgroups of S_3 are precisely those subgroups that are isomorphic to C_1 or C_3 or S_3. So $n = 3$.

4: Let ζ be a primitive n-th root of unity. The roots to $\Phi_n(X)$ are the elements of $\mathbb{Q}_n$ having the form ζ^a where $a \in (\mathbb{Z}/n)^\times$. Except in the case where $\zeta = -1$, the roots to $\Phi_n(X)$ occur in pairs, where ζ^a is paired with ζ^{-a}. Therefore, $\Phi_n(0) = \prod_a \zeta^a = \pm 1$.

Alternative: Since $\Phi_1(X) = X - 1$, we have $\Phi_1(0) = -1$. Generally, $X^n - 1 = \prod_d \Phi_d(X)$, where d runs over the positive divisors of n. So $-1 = \prod_d \Phi_d(0)$. The required conclusion now follows by an inductive argument on n.

Comment: In fact, both of the above arguments can be refined to show that $\Phi_n(0) = 1$ for all integers n with $n \geq 2$.

5: Write $a = \sqrt{1 + \sqrt{2}}$ and $D = \mathbb{Q}[a]$. For a contradiction, suppose $D/\mathbb{Q}$ is Galois. Since D is the splitting field for a polynomial over $\mathbb{Q}$ the automorphism of $\mathbb{Q}[\sqrt{2}]$ given by $\sqrt{2} \mapsto -\sqrt{2}$ extends to an automorphism σ of D. Since $\sigma(a)^2 = 1 - \sqrt{2} < 0$, we have $\sigma(a) \notin \mathbb{R}$. That is impossible, since $D \leq \mathbb{R}$.

For the counter-example, we let D be as above, and we put $E = \mathbb{Q}[\sqrt{2}]$ and $F = \mathbb{Q}$.