Archive of documentation for

MATH 524, Algebra 2

Bilkent University, Spring 2015, Laurence Barker

version: 4 June 2015

Source file: arch524spr15.tex

MATH 524, Algebra 2, Spring 2015

Course specification

Laurence Barker, Mathematics Department, Bilkent University.

Course Aims: To master two areas of core algebra appropriate for all professional pure and applicable mathematicians: Galois theory and ring theory.

Course Description: The first half of the course, based on Dummit and Foote, will be concerned with Galois theory of polynomials. Much of the rest of the course, based on Lam, will be devoted to ring theory, especially the theory of Artinian rings

Course Requirements: MATH 523 Algebra 1 or equivalent.

Instructor: Laurence Barker, Office SAZ 129,
e-mail: barker at fen dot bilkent dot edu dot tr.

Course Texts:

- D. S. Dummit, R. M. Foote, "Abstract Algebra", 3th Edition. (Wiley, 2004).
- T.-Y. Lam, "A First Course in Noncommutative Rings", Graduate Texts in Math. 131, (Springer, 2001).

Classes: Mondays 15:40 - 16:30 SA Z04, Thursdays, 13:40 - 15:30 SA Z04.

Office Hours: Mondays, 16:30 - 17:30, SA-129.

Syllabus:

Week number: Monday date: subtopics, section number.

1: 2 Feb: Symmetries of cubics. Field extensions, 13.1.

2: 9 Feb: Algebraic extensions and Ruler-and-compass constructions, 13.2, 13.3.

3: 16 Feb: Euler–Lagrange proof of Fundamental Theorem of Algebra. Uniqueness of splitting fields and algebraic closures, 13.4.

4: 23 Feb: Separability, 13.5

5: 2 Mar: Galois groups of normal separable extensions, 14.1, 14.2. 14.6.

6: 9 Mar: Fundamental Theorem of Galois Theory, 14.2.

7: 16 Mar: Applications of the Fundamental Theorem of Galois Theory, 14.7, 14.8.

8: 23 Mar: Midterm preparation. Midterm on Thursday 26 March.

9: 30 Mar: Rings, modules, ideals, 10.1, 10.2, Lam Chapter 1.

10: 6 Apr: Semisimplicity of modules and rings, Lam Chapter 2.

11: 13 Apr: Artin–Wedderburn Theorem, Lam Chapter 3.

12: 20 Apr: Jacobson radical, Lam Chapter 4.

13: 27 Apr: Presentations.

14: 4 May: Presentations.

15: 11 May: Review for Final.

Assessment:

- Homework 15%.
- Midterm, 30%, Thursday 26 March.
- Presentations, 20%.
- Final, 35%.

75% attendance is compulsory.

Class Announcements: All students, including any absentees from a class, will be deemed responsible for awareness of class announcements.

Presentations

Büsra Buyraz, "On the simple modules of a group algebra over $\mathbb{C}$".

Gökçen Buyukbaş Çakar, "On solvable field extensions".

Adnan Cıhan Çakar, "Idempotents of the Burnside algebra".

Bekir Daniş, "Rings that are left but not right Artinian or left but not right Noetherian".

Fikri Kaplan, "Frobenius' Theorem on division algebras".

Çisil Karagüzel, "On the number of simple modules of a group algebra over a field".

Abdullah Öner, "The Krull-Schmidt Theorem".

MATH 524, Algebra 2

Homeworks and Quizzes, Spring 2015

Laurence Barker, Mathematics Department, Bilkent University,
version: 2 April 2015.

Office Hours: Mondays, 16:40 - 17:30, SAZ 129.

Office Hours would be a good time to ask me for help with the homeworks.

Homework 1 due Thursday 26th February

Review the proofs of the four results below, which concern the polynomial ring $F[X]$, where F is a field.

Proposition 1: Show that $F[X]$ is a Euclidian domain with respect to degree. In other words, given nonzero polynomials f and g then there exist polynomials q and r such that $f = qg + r$ and either $r = 0$ or else $\deg(r) \leq \deg(g)$.

Proposition 2: Show that, for any nonzero polynomials $f, g \in F[X]$, there exist polynomials $x, y \in F[X]$ such that $xf + yg$ divides f and g. Also show that $xf + yg$ is unique up to a non-zero factor in F. (We call $xf + yg$ the greatest common divisor of f and g.)

Proposition 3: Show that $F[X]$ is a unique factorization domain. In other words, any polynomial $f \in F[X]$ can be expressed in the form $af_1 ... f_r$ where $a \in F$ and f_1, ..., f_r are irreducible monic polynomials, and moreover, the factorization is unique in that, if $f = bg_1 ... g_s$ similarly, then $a = b$ and $r = s$ and, after renumbering, each $f_j = g_j$.

Proposition 4: Show that $F[X]$ is a principal ideal domain. In other words, every ideal of $F[X]$ can be expressed in the form $(f) = \{gf : g \in F[X]$ for some $f \in F[X]$.

Homework 2 due Thursday 16th April

2.1: Let Δ be a division ring and ley n be a positive integer. Show that $Z(\mathrm{Mat}_n(D)) \cong Z(D)$.

2.2: Is every subring of a semisimple ring semisimple?

2.3: Describe the semisimple $\mathbb{Z}$-modules.

2.4: Let R be the ring of continuous functions $[0, 1] \to \mathbb{R}$. Show that R is not semisimple.

2.5: Give a example of a finite-dimensional algebra A over $\mathbb{C}$ such that A is not semisimple.

2.6: Let R be a semisimple ring. Describe the two-sided ideals of R. Hence show that any quotient ring of R is semisimple.

2.7: Let M be a finitely-generated semsimple module of a ring R. Show that the ring $\mathrm{End}_R(M)$ is semisimple.

2.8: Up to isomorphism, how many 10-dimensional semisimple algebras over $\mathbb{C}$ are there?

MATH 524: Algebra II.

Midterm Practise Exercises.

LJB, 10 March 2015, Bilkent University.

1: Let α_1, ..., α_n be algebraic numbers. Let $E = \mathbb{Q}[\alpha_1, ..., \alpha_n]$.
(a) State and prove an inequality relating $[E : \mathbb{Q}]$ to the degrees $[\mathbb{Q}[\alpha_j] : \mathbb{Q}]$.
(b) Suppose that $n = 4$, and that the minimal polynomials of α_1, ..., α_4 are $X^2 - 2$, $X^3 - 3$, $X^5 - 5$, $X^7 - 7$. Evaluate $[E : \mathbb{Q}]$.

2: Let p be a prime and let $1 \leq m \leq n$ be integers. State and prove a necessary and sufficient condition on m and n for $\mathbb{F}_{p^n}$ to be an extension of the field $\mathbb{F}_{p^m}$.

3: Let $f_1(X)$, ..., $f_n(X)$ be polynomials over $\mathbb{Q}$ with degree 2. Let L be the splitting field for $f_1(X)...f_n(X)$ over $\mathbb{Q}$.
(a) Show that the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is abelian. (Hint: consider the squares of the group elements.)
(b) Now suppose that the degree of L over $\mathbb{Q}$ is $|L : \mathbb{Q}| = 8$. How many fields K are there such that $\mathbb{Q} \leq K \leq L$?

4: Let F be a field with characteristic zero, let $f(X)$ be an irreducible quartic (degree 4) polynomial over F, let E be the splitting field for $f(X)$ over F, and let G be the Galois group of the extension E/F.
(a) State the Fundamental Theorem of Galois Theory, including clauses concerning the order of the Galois group and the normal subgroups of the Galois group.
(b) Let α_1, α_2, α_3, α_4 be the roots to $f(X)$, and let

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4)\,.$$

Suppose that $\delta \in F$. Show that $G \cong V_4$ or $G \cong A_4$.
(c) In each of the two cases in part (b), find the number of intermediate fields $F \leq L \leq E$. In each of those two cases, how many of those L are normal extensions of F?

5: Let E be the splitting field for $X^6 - 2$ over $\mathbb{Q}$.
(a) Show that the Galois group for E over $\mathbb{Q}$ is the dihedral group with order 12.
(c) How many intermediate fields $\mathbb{Q} \leq K \leq E$ are there?

MATH 524: Algebra 2. Midterm. LJB, 26 March 2015, Bilkent.

Time allowed: 110 minutes. Please put your name on EVERY sheet of your manuscript.

1: 10% Let J be the splitting field for $(X^2 - 2)(X^3 - 3)$ over $\mathbb{Q}$. Find the degree $[J : \mathbb{Q}]$.

2: 20% For a prime power q, let $\mathbb{F}_q$ denote the field with order q.

(a) Show that $\mathbb{F}_{27}$ is not an extension field of $\mathbb{F}_9$.

(b) Show that $\mathbb{F}_{81}$ is an extension field of $\mathbb{F}_9$.

3: 40% Let L be the splitting field for $X^3 + 3X^2 + 3X - 6$ over $\mathbb{Q}$.

(a) Find the degree $[L : \mathbb{Q}]$. (Hint: consider the substitution $Y = X + 1$.)

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

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

(d) Find all the fields K such that $\mathbb{Q} \leq K \leq L$ and K is not Galois over $\mathbb{Q}$.

4: 15% Let F be a field of characteristic zero. Let f_1 and f_2 be polynomials over F. Let E be a splitting field for $f_1 f_2$ over F. Let $F \leq K_1 \leq E$ and $F \leq K_2 \leq E$ such that K_i is a splitting field for f_i over F. Suppose that $[E : F| = [K_1 : F][K_2 : F]$. Show that $K_1 \cap K_2 = F$. (You may not assume any results pertaining to the condition $[E : F| = [K_1 : F][K_2 : F]$.)

5: 15% In the scenario of Question 4, show that:

(a) $\mathrm{Gal}(E/K_1) \cap \mathrm{Gal}(E/K_2) = 1$.

(b) $\mathrm{Gal}(E/K_1) \trianglelefteq \mathrm{Gal}(E/F) \trianglerighteq \mathrm{Gal}(E/K_2)$.

(c) $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(E/K_1) \times \mathrm{Gal}(E/K_2)$.

Solutions to MATH 524 *Algebra 2* Midterm, Spring 2015.

1: Let $t = \sqrt[3]{3}$ and $\omega = e^{2\pi i/3}$. Then $J = \mathbb{Q}[\sqrt{2}, t, \omega]$. Now $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ and, by Eisenstein's Criterion, $[\mathbb{Q}[t] : \mathbb{Q}] = 3$. Hence $[\mathbb{Q}[\sqrt{2}, t] : \mathbb{Q}] = 6$. Since $\mathbb{Q}[\sqrt{2}, t] \leq \mathbb{R} \not\ni \omega$ and $1 + \omega + \omega^2 = 0$, we have $[J : \mathbb{Q}[\sqrt{2}, t] = 2$. Therefore,

$$[J : \mathbb{Q}] = [J : \mathbb{Q}[\sqrt{2}, t][\mathbb{Q}[\sqrt{2}, t] : \mathbb{Q}] = 2.6 = 12 \ .$$

2: Part (a). Since 27 is not a power of 9, the field $\mathbb{F}_{27}$ cannot be a vector space over $\mathbb{F}_9$.

Part (b). Recall, writing $q = p^n$ with p prime, then $\mathbb{F}_q$ is the splitting field for $X^{q-1} = 1$ over $\mathbb{F}_p$. The multiplicative group $F_{81}^{\times}$ is cyclic with order 80. Since 8 divides 80, there is a primitive 8-th root of unity α in $\mathbb{F}_{81}$. We have $\mathbb{F}_9 = \mathbb{F}_3[\alpha]$ as a subfield of $\mathbb{F}_{81}$.

3: Part (a). We have $X^3 + 3X^2 + 3X - 6 = Y^3 - 7$. By Eisenstein, the polynomial $Y^3 - 7 \in \mathbb{Q}[Y]$ is irreducible. Let $\alpha = \sqrt[3]{7}$. Much as in Question 1, we have $L = \mathbb{Q}[\alpha, \omega]$ and

$$[L : \mathbb{Q}] = [L : \mathbb{Q}[\alpha]][\mathbb{Q}[\alpha] : \mathbb{Q}] = 2.3 = 6 \ .$$

Part (b). The Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$ has order 6. Since $\omega\alpha$ is a conjugate of α and $\omega\alpha \notin \mathbb{R} \geq \mathbb{Q}[\alpha]$, the extension $\mathbb{Q}[\alpha]/\mathbb{Q}$ is not Galois. So G is non-abelian. Therefore $G \cong S_3$.

Part (c). The number of K is the number of subgroups of S_3, which is 6.

Part (d). The three non-Galois intermediate fields are $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[\omega\alpha]$ and $\mathbb{Q}[\omega^2\alpha]$. From the argument in part (b), it is clear that these three fields are mutually distinct. There are no other non-Galois intermediate fields because S_3 has exactly 3 non-normal subgroups.

4: Letting $\{a_1, ..., a_m\}$ and $\{b_1, ..., b_n\}$ be bases for K_1 and K_2 over F, with $a_1 = b_1 = 1$, then the elements $a_i b_j$ span E as a vector space over F. The constraint on the dimensions implies that the elements $a_i b_j$ are linearly independent. So if $\lambda_1 a_1 + ... + \lambda_m a_m = \mu_1 b_1 + ... + \mu_n b_n$ as an element of $K_1 \cap K_2$ with $\lambda_i, \mu_j \in F$, then $\lambda_2 = ... = \lambda_m = \mu_2 = ... = \mu_n$.

5: Part (a). We have $E = K_1 K_2$. Any element σ of $\mathrm{Gal}(E/K_1) \cap \mathrm{Gal}(E/K_2)$ must fix both K_1 and K_2, hence σ fixes E, in other words, $\sigma = 1$.

Part (b). This follows from the Fundamental Theorem of Galois Theory because K_1/F and K_2/F are Galois extensions.

Part (c). By parts (1) and (2), $\mathrm{Gal}(E/F) \geq \mathrm{Gal}(E/K_1) \times \mathrm{Gal}(E/K_2)$. We have equality because $[E : K_1] = [K_2 : F]$ and $[E : K_2] = [K_1 : F]$ and

$$|\mathrm{Gal}(E/F)| = [E : F] = [E : K_1][E : K_2] = |\mathrm{Gal}(E/K_1)| \, . \, |\mathrm{Gal}(E/K_2)| \ .$$

MATH 524: Algebra 2. Makeup. LJB, 15 May 2015, Bilkent.

Time allowed: 110 minutes. Please put your name on EVERY sheet of your manuscript.

1: 10% State the Fundamental Theorem of Galois Theory (including clauses about normal subgroups and normal extensions).

2: 10% Let n be a rational integer. Under what conditions is the polynomial $X^3 - n$ irreducible over $\mathbb{Q}$?

3: 30% Let E be the splitting field of $X^3 - 9$ over $\mathbb{Q}$.

(a) Find the Galois group $\mathrm{Gal}(E/\mathbb{Q})$.

(b) Find all the fields K such that $\mathbb{Q} < K < E$. Explain why your list is complete.

4: 30% For a positive integer n, let $\mathbb{Q}_n$ denote the splitting field of $X^n - 1$ over $\mathbb{Q}$.

(a) Determine the Galois group $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. When justifying your answer, you may assume that the n-th cyclotomic polynomial is irreducible.

(b) How many fields K are there such that $\mathbb{Q} < K < \mathbb{Q}_{16}$?

5: 20% Let $\mathbb{F}_{64}$ denote the field of order 64. Find the order of the automorphism group $\mathrm{Aut}(\mathbb{F}_{64})$.

MATH 524: Algebra 2. Final. LJB, 18 May 2015, Bilkent.

Please put your name on EVERY sheet of your manuscript. The use of very faint pencils is prohibited.

1: 25% Let A be an Artinian ring and suppose that $A = B \oplus N$ where B is a subring and N is a nilpotent ideal. Show that every idempotent of $Z(A)$ belongs to $Z(B)$.

2: 25% Let A be an Artinian ring, and let $\bar{i}$ be an idempotent of $A/J(A)$. Show that there exists an idempotent $i \in A$ such that $i + J(A) = \bar{i}$. Hint: Choose an element $i_1 \in A$ such that $i_1 + J(A) = \bar{i}$. Let $j_1 = i_1^2 - i_1$. Consider sequences i_1, i_2, ... and j_1, j_2, ... such that

$$i_{n+1} = i_n + j_n - 2i_n j_n \ , \qquad\qquad j_{n+1} = i_{n+1}^2 - i_{n+1} \ .$$

3: 25% Let X be a finite set and let F be a field. We define $\mathrm{Mat}_X(F)$ to be the algebra with an F-basis consisting of elements $e_{x,y}$ with $x, y \in X$ such that

$$e_{x,y} e_{y',z} = \begin{cases} e_{x,z} & \text{if } y = y', \\ 0 & \text{otherwise,} \end{cases}$$

for $x, y, y', z \in X$. Let $\sim$ be a reflexive and transitive relation on X. We define the **incidence algebra** $FI(\sim)$ of $\sim$ over F to be the subalgebra of $\mathrm{Mat}_F(X)$ spanned by those elements $e_{x,y}$ such that $x \sim y$. Give combinatorial descriptions of the number of isomorphism classes of simple $FI(\sim)$-modules in the cases:
(a) where $\sim$ is a partial ordering,
(b) where $\sim$ is an equivalence relation,
(c) generally.

4: 25% Let R be a ring.
(a) Show that any finitely generated non-zero R-module M contains a maximal submodule N, we mean, a submodule $N < M$ such that there is no submodule I with $N < I < M$.
(b) Give a counter-example to show that we cannot drop the assumption that M is finitely generated.

Final Solutions, MATH 524 Spring 2015

1: Let e be an idempotent of $Z(A)$. Write $e = b + n$ where $b \in B$ and $n \in N$. We have

$$b^2 + bn = be = eb = b^2 + nb\ .$$

So $bn = nb$. By considering the epimorphism $A \to b$ with kernel N, we deduce that b is an idempotent. For a contradiction, suppose that $n \neq 0$ and let r be maximal such that $n \in N^r$. Modulo N^{2r}, we have

$$b + 2bn \equiv e^2 = e = e^3 \equiv b + 3bn\ .$$

Subtracting, we deduce that $bn \equiv 0$. But this implies that $e \equiv b$, in other words, $n \in N^{2r}$, which contradicts the definition of r.

2: Since A is Artinian, $J^n(A) = 0$ for sufficiently large n. It suffices to show that $j_n \in J^n(A)$ for all n. We argue by induction. Plainly, $j_1 \in J(A)$. Suppose that $j_n \in J^n(A)$. Note that i_n and j_n commute. Modulo $J^{n+1}(A)$, we have

$$j_{n+1} = (i_n + j_n - 2i_nj_n)^2 - (i_n + j_n - 2i_nj_n)$$

$$\equiv (i_n + 2i_nj_n - 4i_n^2j_n) - i_n - j_n + 2i_nj_n = 4(i_n - i_n^2)j_n = -4j_n^2 \equiv 0;.$$

3: Generally, let $\equiv$ be the equivalence relation such that, given $x, y \in X$, then $x \equiv y$ provided $x \sim y$ and $y \sim x$. The Jacobson radical $J(FI(\sim))$ is spanned by those $e_{x,y}$ such that $x \sim y$ and $y \not\sim x$. The semisimple quotient $FI(\sim)/J(FI(\sim))$ is spanned by the images of the elements $e_{x,y}$ such that $x \equiv y$. Thus, letting X_1, ..., X_k be the equivalence classes under $\equiv$, then

$$FI(\sim)/J(FI(\sim)) \cong \mathrm{Mat}_{n_1}(F) \oplus ... \oplus \mathrm{Mat}_{n_k}(F)$$

where the subalgebra $\mathrm{Mat}_{n_i}(F)$ is spanned by the images of the elements $e_{x,y}$ with $x, y \in X_i$. In particular, the number of isomorphism classes of simple $FI(\sim)$-modules is k, the number of equivalence classes.

In part (b), the relations $\sim$ and $\equiv$ coincide. In part (a), each equivalence class is singleton and the number of isomorphism classes of simple $FI(\sim)$-modules is $|X|$.

4: Part (a). Let X be a finite generating set for M. Consider the poset $\mathcal{P}$ of strict submodules of M. Since $\mathcal{P}$ owns the zero submodule, $\mathcal{P}$ is non-empty. Let $\mathcal{N}$ be a chain in $\mathcal{P}$. Since none of the elements of $\mathcal{N}$ contain X, the unionset $\bigcup \mathcal{N}$ cannot contain X. Therefore $\bigcup \mathcal{N}$ belongs to $\mathcal{P}$ and is an upper bound for $\mathcal{N}$ in $\mathcal{P}$. By Zorn's Lemma, $\mathcal{P}$ has a maximal element N. Plainly, N is a maximal submodule of M.

Part (b). Let p be a prime and let M be the Prüfer p-group (the multiplicative group of complex numbers having the form $e^{im/q}$ where m is an integer and q is a power of p.) Plainly, as a $\mathbb{Z}$-module, the infinitely-generated group M has no maximal submodule.