Algebra I (Math 520A)
Topics and Assignments

Spring Semester, 2007

End of Semester Schedule

Tue., May. 15:

    Final Examination: 3:30 – 5:30 p.m.

Mon., May. 14:

    Office Hours: 2:30 – 3:30 p.m.

Fri., May. 11:

    Office Hours: 2:30 – 3:30 p.m.

PDF and DVI (requires TeX^1 software) versions of this page are available for printing.

For each date there is a list of topics covered (or to be covered). For each meeting your assignment is to be ready for a quiz on recently covered definitions and statements of theorems.

Each written assignment will be announced one week before it is due.

Mon., May. 7:

    Last meeting prior to the final exam.

    Written Assignment No. 5 (also available as PDF) is due.

Fri., May. 4:

    The notion of normal extension. A finite extension is Galois if and only if separable and normal. In a Galois extension there is a bijective correspondence between intermediate fields and subgroups of the Galois group. A finite extension L of degree n over K is Galois if and only if there is an irreducible polynomial f of degree n with no multiple root in "the" algebraic closure of K such that L is "the" splitting field of f. In any finite separable extension there are only finitely many intermediate fields.

Wed., May. 2:

    Completed the proof that every finite separable extension is simple. If L/K is a Galois extension with group G, then for every subgroup H of G with E the subfield of L fixed by H, the extension L/E is Galois with group H. Two consequences of that: (1) A finite extension L/K is Galois if and only if, with $G = \mathrm{Aut}(L/K)$, one has $K = L^G$ (the case $H = G$). (2) Every (finite) Galois extension is separable.

Mon., Apr. 30:

    The notion of element separably algebraic over a field, and separably algebraic extensions. Examples. A finite extension L/K is separable if and only if the number of K-algebra morphisms of L in "the" algebraic closure of K is equal to the extension degree of L over K. Every finite separable extension is simple.

Fri., Apr. 27:

    Example: The splitting field E over $\mathbf{Q}$ of the polynomial $t^3 - 2$ is $\mathbf{Q}(\sqrt[3]{2}, \rho)$ where ρ is a (complex) root of $t^2 - t + 1$. $E/\mathbf{Q}$ is a Galois extension with $\mathrm{Aut}_{\mathbf{Q}}(E) \cong S_3$. Theorem: Every finite extension of a finite field with q elements is a Galois extension with cyclic Galois group generated by $\alpha \mapsto \alpha^q$.

---

[1]URI: http://www.tug.org/

Wed., Apr. 25:

A finite sequence of distinct homomorphisms from a group G to the multiplicative group F^* of a field F is linearly independent when regarded as a finite sequence of elements of the vector space over F of arbitrary maps from G to F (with vector space operations defined pointwise). If G is a subgroup of the group $\text{Aut}_K(L)$ for a finite field extension L/K, then
$$|G| \leq [L : K] \quad .$$
A finite extension L/K is called a *Galois extension* if
$$|\text{Aut}_K(L)| = [L : K] \quad .$$

Mon., Apr. 23:

Every finite subgroup of the multiplicative group of a field is cyclic. The number of elements in a finite field must be a prime power. For every prime power q there is one and (up to non-unique isomorphism) only one finite field having q elements. The unique field with $q = p^r$ elements (p prime, $r \geq 1$) may be characterized as "the" splitting field of the polynomial $t^q - t \in \mathbf{F}_p[t]$.

Written Assignment No. 4 (also available as PDF) is due.

Fri., Apr. 20:

Notion of splitting field of a polynomial with coefficients in a field. Any field in which a polynomial splits is (in a non-unique way) an extension of any splitting field. Existence and uniqueness (up to non-unique isomorphism) of a splitting field for a given polynomial. Definition of "the" algebraic closure of a field. Every field has an algebraic closure that is unique up to non-unique isomorphism.

Wed., Apr. 18:

Notion of algebraic field extension. The long extension in a finite tower of algebraic extensions is an algebraic extension. An extension L of K is finite if and only if there exist finitely many elements $\alpha_1, \ldots \alpha_m$ algebraic over K such that $L = K(\alpha_1, \ldots, \alpha_m)$. In any extension L of K the set of all elements in L that are algebraic over K is a subfield of L that is called the *algebraic closure of K in L*. Definition and equivalent criteria for an algebraically closed field. Existence of an algebraically closed extension of any field.

Mon., Apr. 16:

Prime and maximal ideals in a commutative ring. An ideal I in a commutative ring A is prime if and only if A/I is a domain; I is maximal if and only if A/I is a field. For a field extension L/K and an element $\alpha \in L$ let $\varphi : K[t] \to L$ denote the ring morphism given by the substitution of α for t. Then
$$K[\alpha] = \text{Im}\varphi \cong K[t]/\text{Ker}\varphi \quad .$$

Because $K[\alpha]$ is finite-dimensional over K if and only if $\text{Ker}\varphi \neq (0)$, α is transcendental over K if and only if $K[\alpha] \cong K[t]$, and α is algebraic over K if and only if $K[\alpha] = K(\alpha)$, i.e., if $K[\alpha]$ is a field. When α is algebraic over K there is a unique irreducible monic polynomial $f \in K[t]$ such that $f(\alpha) = 0$.

Fri., Apr. 13:

Extension degrees multiply in a tower. Elements of a field algebraic or transcendental over a subfield. For a field extension L/K an element $\alpha \in L$ is algebraic over K if and only if $K(\alpha)$ is a finite extension of K. Examples.

Wed., Apr. 11:

Comments on assignment no. 3. Ring and field adjunction inside a field. Finite extensions and extensions of finite type. $F[t]/f(t)F[t]$ is a finite extension of F when f is a polynomial in $F[t]$ irreducible over F.

Mon – Mon., Apr. 2 – 9:

University Recess: no meetings

Fri., Mar. 30:

The characteristic and characteristic subring of a ring. The pth-power endomorphism of a commutative ring in prime characteristic p; this endomorphism is an automorphism in the case of a finite field of characteristic p.

Written Assignment No. 3 (also available as PDF) is due.

Wed., Mar. 28:

Overview of field extensions. The group of relative automorphisms. Examples.

Mon., Mar. 26:

Normal series and composition series. The Jordan-Holder theorem. Examples.

Fri., Mar. 23:

The notion of *invariant* or *characteristic* subgroup. Examples: The *center* and the *commutator* (or *derived*) subgroup of a group. $G^{\text{ab}} \cong G/\text{Der}(G)$ is universal for morphisms from G to an abelian group.

Wed., Mar. 21:

Midterm Test.

Mon., Mar. 19:

Questions prior to the test.

The concept of simple group.

Fri., Mar. 16:

The quaternion group as an example of a group given by generators and relations. Complete classification of groups of orders up to 8.

Wed., Mar. 14:

A finite abelian group is the direct product of its Sylow subgroups. Thus the classification of finite abelian groups reduces to the classification of finite abelian p-groups. There is a course supplement (also available as PDF) following this approach that is accessible at this point.

The classification of finite abelian groups will be revisited in Math 520B as part of the study of finitely-generated modules over principal ideal domains.

Mon., Mar. 12:

Proof of the Sylow theorems.

Written Assignment No. 2 (also available as PDF) is due.

Fri., Mar. 9:

Application of the Sylow theorems to the classification of groups of order 105

Wed., Mar. 7:

The concept of a p-group. Application of Cauchy's theorem: a finite p-group is the same thing as a group of order p^r. Kernel of the action of a group by translation on a quotient set; normality of a subgroup having smallest prime index. Classification of groups of order pq where p and q are distinct primes. Announcement of the Sylow theorems.

Mon., Mar. 5:

Issue: the existence of subgroups in a finite group. The case of cyclic groups. If X is a finite G-set and $|G|$ a power of p, a prime, then the number of fixed points is congruent to $|X|$ modulo p. Cauchy's theorem on the existence of elements of prime order.

Fri., Mar. 2:

The second and third isomorphism theorems as applications of the universality of the quotient. Examples.

Wed., Feb. 28:

The class formula and its application to p-groups. The center of a group cannot have prime index. Every group of order p^2 is abelian. The subgroup of a group generated by a subset. In a group G if H is a subgroup and N a normal subgroup, then $\langle N \cup H \rangle = NH$, and NH is semi-direct if and only if $N \cap H = (0)$. Example: $\mathrm{SL}_2(\mathbf{Z})$ is generated by two elements with orders 3 and 4.

Mon., Feb. 26:

Splittings. Example: Split and non-split homomorphisms on the Heisenberg group of a vector space. Cyclic and dihedral groups.

Week Feb 19 − 23

University Recess: no classes.

Fri., Feb. 16:

Internal and external semi-direct products as equivalent notions.

Written Assignment No. 1 (also available as PDF) is due.

Wed., Feb. 14:

No Meeting. The University has announced that, due to severe snow conditions, all day and evening classes on February 14 are cancelled. As a result, the due date for Written Assignment No. 1 has been postponed to Friday, Feb. 16.

Mon., Feb. 12:

Transitive actions and factor sets. Actions by automorphisms.

Fri., Feb. 9:

The notion of group action. Examples. Actions lurking in the group of rotations of the cube.

Wed., Feb. 7:

Universality of the quotient for rings. Examples. The notion of algebra over a ring.

Mon., Feb. 5:

Kernels and images, of morphisms for rings and modules over a ring. Ideals in a ring, and the quotient of a ring by a two-sided ideal.

Fri., Feb. 2:

Universality of the quotient morphism and the first isomorphism theorem.

Wed., Jan. 31:

Kernels and images of morphisms for groups, normal subgroups, and the quotient construction.

Mon., Jan. 29:

Hamilton's quaternions as an example of a division ring that is not a field. Left, right and two-sided modules over a ring and morphisms of modules.

Fri., Jan. 26:

Rings, zero divisors, division rings, fields, and ring morphisms.

Wed., Jan. 24:

Left and right translations, invertibility in a monoid, groups.

Mon., Jan. 22:

Two different understandings of the notion of sub-object. A set with binary operation as a sub-object of another. Subsemigroups, submonoids, the monoid of endomorphisms of a semigroup as a submonoid of the monoid of self-maps of the underlying set.

Fri., Jan. 19:

Binary operations, associativity, commutativity, semigroups, monoids, and the corresponding morphisms. Examples: Addition and multiplication of $n \times n$ matrices, the Lie bracket, and the monoid of endomorphisms of a set under composition. For $n \times n$ real matrices x, y the function

$$t(x, y) \;=\; \mathrm{trace}(xy)$$

defines a symmetric bilinear form, not a commutative binary operation.

UP | TOP | Department