Math 122 Course Outline (Fall 2005)

Meeting 1 - September 19 (first day of class)

- Briefly review linear algebra. Matrix multiplication, associativity, inverses.
- Define a group using GL_n as an example.
- Laws of composition. Associativity. Commutativity. Composition of maps. Inverses and their uniqueness. Power notation.
- Characterization of determinant as unique normalized multilinear alternating homomorphism [not proven]. Basic properties (1.3.15, 1.3.16, 1.3.18).

Meeting 2 - September 21

- Groups.
- Abelian groups. Examples. $\mathbb{Z}$. Cyclic groups.
- Non-abelian groups. Cancellation law (1.1.12). Examples (GL_n, permutations). Cycle notation for S_n.
- Subgroups. Examples. The subgroups of $\mathbb{Z}$.

Meeting 3 - September 23 (study card day)

- Re-introduce the language of groups, subgroups.
- Order of an element. Order of a group. Cyclic groups again.
- More examples of groups (Klein 4-group, quaternion group).
- The Rubik's cube and related groups.

Meeting 4 - September 26

- Isomorphisms. Equivalent characterizations. Automorphisms.
- Conjugation. Inner automorphisms. Interpretations in GL_n.
- Homomorphisms. Examples. Structure preserved (1.4.3).
- Image. Kernel. Examples (in case of det).
- Normal subgroups. Show kernels are normal.
- Center of a group.

Meeting 5 - September 28

- Partitions. Equivalence relations. Equivalence classes. Correspondence between partitions and equivalence relations.
- Examples of partitions. Fibers of a homomorphism.
- Left cosets. Index of a subgroup.
- "Counting formula" and Lagrange's theorem. Consequences (groups of prime order, $|G| = |\ker| \times |\mathrm{im}|$).
- Right cosets. Characterization of normal subgroups (2.6.18).

Meeting 6 - September 30

- Continue explanation of cosets, normal subgroups.
- Remarks on restrictions of a homomorphism to a subgroup (2.7.1, 2.7.2).
- Quick explanation of products of groups.

Meeting 7 - October 3

- Congruence modulo n. $[\mathbb{Z} : n\mathbb{Z}] = n$. Congruence classes well defined under $+$ and $\times$.
- Thought experiment concerning structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ (to be treated fully later).

Meeting 8 - October 5

- Multiplication of subsets of a group. Multiplication of cosets. Quotient groups and the canonical projection map.
- Characterization of normal subgroups (2.10.6).
- First isomorphism theorem (2.10.9). Examples.

Meeting 9 - October 7

- Basic operations in $\mathbb{R}^n$. Homogeneous linear equations revisited.
- Abstract definition of real vector spaces. Basic properties (3.1.7). Examples.
- Fields. Examples (including finite fields).
- Vector spaces. Subspaces. Linear maps. Examples.

Meeting 10 - October 12 (October 10 is Columbus Day)

- Spans. Linear independence. Bases. Properties (3.3.2, 3.3.4, 3.3.7, 3.3.8, 3.3.10, 3.3.11).
- Dimension and properties (3.3.13, 3.3.14, 3.3.15, 3.3.16, 3.3.17, 3.3.19, 3.3.20).

- TAKE HOME QUIZ: Group theory through Meeting 8. Given Tuesday, October 11 and due Today.

Meeting 11 - October 14

- Finish material from meeting 9.
- The matrix associated to a linear operator and bases. Basic properties. Algorithms for studying linear operators in terms of matrices.
- Dimension formula and relation to counting formula.
- Rank and nullity of matrices.

Meeting 12 - October 17 (Add/drop deadline)

- Similarity and change of basis.
- Invariant subspaces. Eigenvalues and eigenvectors.
- Obvious facts (4.3.10, 4.3. 11, 4.3.12, 4.3.13).
- An observation (4.4.5). Singularity. Characteristic polynomials and properties (4.4.13, 4.4.14, 4.4.17, 4.4.18, 4.4.19).
- Mid-term evaluations.

Meeting 13 - October 19

- Orthogonal group. Special orthogonal group. Fundamental results (4.5.16, 4.5.20, 4.5.21).

Meeting 14 - October 21

- Examples of isometries of plane figures.
- Explicit classification of orientation-preserving and orientation-reversing motions.

Meeting 15 - October 24

- Cyclic and dihedral groups. The finite subgroups of O_2.
- Discrete gropus of motions. Discrete subgroups of $\mathbb{R}^2$ $(0, \mathbb{Z}, L)$.

Meeting 16 - October 26

- Group actions. Orbits. Stabilizers.
- Examples.
- Transitive G-sets as coset spaces (5.6.4).
- Stabilizers of translates.

Meeting 17 - October 28

- Finish material from Meeting 17.
- $|G| = |\text{stab}| \times |\text{orbit}|$. The symmetries of the regular dodecahedron.
- $[H : H \cap K] \leq [G : K]$.

Meeting 18 - October 31 (Withdrawal deadline)

- Group acting on itself by left multiplication. Cayley's Theorem.
- Centralizers. Conjugacy classes. Class equation.
- Center of a p-group. Groups of order p^2 are abelian.
- The group of symmetries of an icosahedron is simple.
- Stabilizer of a subset. Examples.
- Normalizers.

Meeting 19 - November 2

- Sylow theorems.
- Applications to groups of order 6, 15, 21.

Meeting 20 - November 4

- Finish Sylow theorems.
- Classification of groups of order 12.

Meeting 21 - November 7

- Permutations. Support. Transpositions.
- Review of cyclic notation and disjoint cycle decomposition.
- Structure of conjugacy classes in S_n.
- Commutators and Rubik's cube.

Meeting 22 - November 9

- Rubik's cube.

Meeting 23 - November 14 (November 11 is Veteran's Day)

- Wrap up of material on groups.

Meeting 24 - November 16

- HOUR EXAM.

Meeting 25 - November 18

- Gaussian integers. Rings. Subrings. Examples.
- Formal construction of $\mathbb{Z}$.
- Formal construction of $R[x]$.

Meeting 26 - November 21

- Homomorphisms or rings. Isomorphisms. "Substitution principle" (10.3.4). More examples.
- Ideals. Examples.
- Lattice of ideals in a ring. Fields revisited. Principalness in $\mathbb{Z}$ (division algorithm).

Meeting 27 - November 23

- Quotient rings. First isomorphism theorem. The lattice of ideals is a quotient ring.
- Examples. Relations to algebraic geometry.
- When $p = 1 \pmod 4$, $\mathbb{Z}[i]$ has an ideal I with $\mathbb{Z}[i]/I = \mathbb{Z}/p\mathbb{Z}$.

Meeting 28 - November 28 (November 24-27 is Thanksgiving break)

- Review of Meeting 27.
- Field with p^2 elements.
- Ring extensions. Algebraic extensions.
- Nilpotents. Zero divisors.

Meeting 29 - November 30

- Integral domains.
- Field of fractions. Universal property.

Meeting 30 - December 2

- Fundamental theorem of arithmetic.
- Euclidean algorithm in $F[x]$. Consequences.
- Divisors. Proper divisors. Associates.

Meeting 31 - December 5

- Existence of factorizations. UFDS. Structural results (11.2.8, 11.2.9, 11.2.10, 11.2.11).
- PIDs. PID $\Rightarrow$ UFD.
- Structural results in PIDs.
- Euclidean domains. Examples. Euclidean $\Rightarrow$ PID.
- Emphasis on Euclidean domain part.

Meeting 32 - December 7

- UFDs. Gauss' lemma. Irreducibility in $\mathbb{Q}[x]$.
- Irreducibility criteria. Eisenstein's criteria.

Meeting 33 - December 9

- Modules as generalizations of vector spaces.
- Free modules. Rank.
- $\mathbb{Z}$ modules and relation to abelian groups.
- Submodules. Homomorphisms. Submodules of R.

Meeting 34 - December 12

- Finitely generated. Span. Linear independence.
- Homomorphisms $R^n \to R^m$. Matrices. Conditions for invertibility.
- Reduction of integer matrices to diagonal form.

Meeting 35 - December 14

- Diagonalization of matrices over Euclidean rings.
- Applications (12.4.8, 12.4.11).
- Finitely generated submodules of free modules are free.
- Noetherian rings. Hilbert Basis Theorem [not proven]. Submodules of finitely generated modules (over Noetherian rings) are finitely generated.
- Take Home Quiz: Rings. Given Tuesday, December 13 and due Today.

Meeting 36 - December 16

- Finish Meeting 35.
- PIDs Noetherian. Submodules of R^n, R Euclidean, are free.

- Classification of finitely generated abelian groups.

Meeting 37 - December 19

- RSA and prime factorization.
- $\mathbb{Z}/n\mathbb{Z}$ and primality testing.
- Wrap up.