MATH 71 FALL 2015

DIARY

Textbook

[**DF**] *Abstract Algebra (3rd ed.)*, by S. Dummit and R. M. Foote.

Effective syllabus

O. Preliminaries - *2 lectures*

O.1 Binary relations
O.2 Basic arithmetic

I. Groups - *15 lectures*

I.1. Generalities
I.2. Examples of groups
I.3. Morphisms and subgroups
I.4. Cyclic groups
I.5. Groups presented by generators and relations
I.6. Quotient groups
I.7. The First Isomorphism Theorem
I.8. Lagrange's Theorem
I.9. The alternating group $\mathfrak{S}_n$
I.10. Group actions
I.11. Composition series and Hölder's Program
I.12. Sylow's Theorems
I.13. The Fundamental Theorem of finitely generated abelian groups
I.14. Direct and semi-direct products

II. Rings - *10 lectures*

II.1. Generalities
II.2. Properties of ideals
II.3. Euclidean domains
II.4. Principal ideal domains
II.5. Unique factorization domains
II.6. Rings of fractions
II.7. Polynomial rings
II.8. Field extensions

III. Introduction to representation theory - *1 lecture*

Updated: November 16, 2015.

Week 1

Lecture 1. [**DF**, §0.1-§0.3]
Equivalence relations: definition and examples. Equivalence classes, representatives. Correspondence between equivalence relations and partitions.
Basic arithmetic vocabulary, relatively prime numbers. Congruence modulo n.

Lecture 2. [**DF**, §0.1-§0.3]
Review of Euclidean division, the Euclidean Algorithm.
Addition and multiplication are well-defined operations in $\mathbb{Z}/n\mathbb{Z}$.
Characterization of invertible elements: $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a}\ ,\ a \wedge n = 1\}$.

Lecture 3. [**DF**, §1.1-§1.4]
Composition laws (binary operationa), associativity, commutativity.
Groups: definition, first examples. Abelian groups are denoted additively.
General properties: uniqueness of the identity and of the inverse, inverse of a composition.
Cancellation laws, conjugation.
Fields: definition, examples ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$, p prime). Matrix groups: $\mathrm{GL}(2, \mathrm{F})$, $\mathrm{SL}(2, F)$.

Week 2

Lecture 4. [**DF**, §1.2]
Dihedral groups: geometric definition, enumeration ($\#\mathrm{D}_{2n} = 2n$). Table of a group.
Generators and relations: examples of $\mathbb{Z}/n\mathbb{Z}$ and $\mathrm{D}_{2n} = \langle r, s \mid s^2 = 1\ ,\ r^n = 1\ ,\ rs = sr^{-1}\rangle$.

Lecture 5. [**DF**, §1.3-§1.6]
Symmetric groups $\mathfrak{S}_n$: permutations, cycles. Cycles with disjoint supports commute.
Canonical decomposition: every permutation can be uniquely written as a (commuting) product of cycles with disjoint supports. Cycle Decomposition Algorithm. Application to the determination of the order of a permutation.
Group homomorphisms: definition, examples. Morphisms map identity to identity and inverse to inverse. Isomorphism. The isomorphic image of an abelian group is abelian. Isomorphisms preserve the order of elements.

Problem Session 1. A permutation has order 2 if and only if its canonical decomposition only contains permutations. Presentation of $\mathbb{Z}/n\mathbb{Z}$.

Lecture 6. [**DF**, §2.1-§2.2]
Subgroups: definition, examples, simple groups, the Subgroup Criterion.
Subgroups of $\mathrm{SL}(2, \mathbb{R})$ isomorphic to $\{z \in \mathbb{C}\ ,\ |z| = 1\}$, $\mathbb{R}_+^\times$, and $\mathbb{R}$.
Images and kernels of homomorphims are subgroups (generalizing the case of linear maps between vector spaces). Characterization of injectivity via the kernel.

Week 3

Lecture 7. [**DF**, §2.3]
Cyclic groups: classification by the cardinality, characterization of generators, subgroups.

Lecture 8. [**DF**, §2.4 - §3.1]
Group $\langle A \rangle$ generated by a subset A of a group G: definition as minimal subgroup containing A, characterisation by the intersections of all subgroups containing A, general form of the elements.
Equivalence relation $\sim_H$ on G, with $H < G$. Left cosets: gH is the class of $g \in G$ for this relation. Composition of cosets $g_1H \star g_2H = g_1 \cdot g_2H$ is well defined if and only if $gH = Hg$ for all $g \in G$. Normal subgroups.

Problem Session 2. A subgroup H of $\mathbb{Q}$ such that $x \in H \Rightarrow \frac{1}{x} \in H$ must be $\{0\}$ or $\mathbb{Q}$.

Lecture 9. [**DF**, §3.1 - §3.2 - §3.3]
Characterizations of normal subgroups, quotients. Normal subgroups are exactly kernels of homomorphisms. The First Isomorphism Theorem. Application: $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{T}$.

Week 4

Problem Session 3. Subgroups of $\mu_n = \{z \in \mathbb{C}\ ,\ z^n = 1\}$. Subgroups of D_{2n} generated by various subsets. $\mathrm{SL}(n, F) \lhd \mathrm{GL}(n, F)$ and $\mathrm{GL}(n, F)/\mathrm{SL}(n, F) \simeq F^\times$.

Lecture 10. [**DF**, §3.2]
Lagrange's Theorem and corollaries: the order of an element divides the order of the group, a group with prime order is cyclic. The index of a subgroup. Finite case: $[G : H] = \frac{\#G}{\#H}$, examples. A subgroup with index 2 is normal. There is no general converse for Lagrange's Theorem: the tetrahedron group, of order 12, as no subgroup of order 6.

Lecture 11. [**DF**, §3.5]
Cycles and transpositions generate $\mathfrak{S}_n$; there is no uniqueness in the way a given permutation decomposes into transpositions. Action of $\sigma \in \mathfrak{S}_n$ on $\Delta = \prod_{1 \leq i < j \leq n} (X_i - X_j)$. Definition of the signature: $\sigma \cdot \Delta = \varepsilon(\sigma)\Delta$. This defines a homomorphism $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$, whose kernel is called the *alternating group* $\mathfrak{A}_n$ with cardinality $\frac{n!}{2}$. Transpositions have signature -1, notion of even and odd transposition.

Week 5

Lecture 12. [**DF**, §1.7,§4.1]
Action of a group on a set: definition and examples. The kernel of $G \curvearrowright X$ is the kernel of the homomorphism $g \mapsto \sigma_g$, where $\sigma_g(x) = g \cdot x$; faithful actions.
The stabilizer $\mathrm{Stab}_G(x)$ of an element $x \in X$ is a subgroup of G with index the cardinality of the orbit of x. Transitive actions.

Lecture 13. [**DF**, §4.2]
Any group acts on itself by left multiplication. Example of Klein's group V_4.
More generally, if $H < G$, the action $G \curvearrowright G/H$ given by left multiplication is transitive. The stabilizer of 1_GH is H, the kernel is $N = \bigcap_{g \in G} gHg^{-1}$ and N is the largest normal subgroup of G contained in H.
Corollary (Cayley): every finite group is isomorphic to a subgroup of $\mathfrak{S}_n$ for some n.

Lecture 14. [**DF**, §4.3]
Equivariant maps and isomorphisms in the category of G-sets. Centralizers and normalizers, action by conjugation. Examples: similar matrices, equivalences classes and rank. The Class Equation and applications: a group of order p^α with p prime has non-trivial center. A group of order p^2 with p prime is abelian, isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Week 6

Lecture 15. [**DF**, §3.4]
Cauchy's Theorem: if G is a finite group and p prime divides $\#G$, then G contains an element (hence a subgroup) of order p. Proof in the abelian case. Simple groups, composition series, Jordan-Hölder Theorem. Hölder's classification program.
Feit-Thompson's Theorem: simple groups of odd order are cyclic.

Lecture 16. [**DF**, §4.5, §5.2, §5.4]
Maximal p-subgroups: Sylow's theorems. Structure of finitely generated abelian groups. Structure of compactly generated abelian groups. Characterization of direct products. Structure of the group H_1H_2 when $H_1 \lhd G$, $H_2 < G$ and $H_1 \cap H_2 = \{1\}$.

Lecture 17. [**DF**, §5.5]
Semi-direct products: general case. Application: if p and q are prime numbers and $p|(q-1)$, there exists a non-abelian group of order pq.

Lecture 18. [**DF**, §7.1]
Rings: definition, basic examples. Fields, division rings, example of the quaternions $\mathbb{H}$. Rings of functions with values in a ring. Zero divisors and units.

Week 7

Lecture 19. [**DF**, §7.1, §7.2]
Integral domains. Cancellation laws. A finite integral domain with identity is a field. Wedderburn's Theorem: a finite division ring is abelian, hence a field.
Subgrings and ring morphisms. The kernel of a ring homomorphism is absorbent.
Ideals. If I is an ideal in A, the quotient group A/I is a ring for the multiplication $(a+I)(b+I) = ab + I$. Natural projection $A \longrightarrow A/I$, First Isomorphism Theorem.

Lecture 20. [**DF**, §7.1, §7.4]
Finitely supported sequences in a ring: polynomials.
Ideal generated by a subset: definition, characterization, commutative case.
Principal ideals. $b \in (a) \Leftrightarrow a|b \Leftrightarrow (b) \subset (a)$. If I is an ideal in A, then $I = A$ if and only if I contains a unit. A commutative ring with unit is a field if and only if has no other ideals than $\{0\}$ and A.

Lecture 21. [**DF**, §7.4]
Maximal ideals; I is maximal if and only if A/I is a field. Examples: (X) is not maximal in $\mathbb{Z}[X]$, the ideal generated by 2 and X is. Prime ideals in a commutative ring.

Week 8

Lecture 22. [**DF**, §8.1]
Euclidean domains, division algorithm. Examples: $\mathbb{Z}$, $\mathbb{R}[X]$, fields. In a Euclidean domain, every ideal is principal. Example: $\mathbb{Z}[X]$ carries no Euclidean division.
Multiples, divisors, notion of g.c.d. Uniqueness up to a unit. The division algorithm allows to compute a g.c.d., Bézout relation.
More about polynomial rings: if A is a commutative ring with identity and I is an ideal, then $(I) = I[X]$ and $A[X]/I[X] \simeq A/I[X]$. Polynomials in several variables.

Lecture 23. [**DF**, §8.2]
A principal ideal domain (PID) is an integral domain in which every ideal is principal. Euclidean rings are PIDs, but $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ is a PID that is not Euclidean. For a and b, in a PID, any generator of (a, b) is a g.c.d. It is unique up to multiplication by a unit and satisfies a Bézout relation. In a PID, every prime ideal is maximal.
Corollary: if A is a commutative ring, then $A[X]$ is a PID $\Rightarrow$ A is a field. Conversely, if A is a field, then $A[X]$ is a Euclidean domain hence a PID.

Fun: group rings and convolution.

Lecture 24. [**DF**, §8.3]
Notice that in $\mathbb{Z}$, an alternate way to compute the g.c.d. of two elements is to compare their prime factors decompositions. Irreducibles and primes in an integral domain, associate elements. General fact: prime $\Rightarrow$ irreducible. The converse does not hold in $\mathbb{Z}[i\sqrt{5}]$ as 3 is irreducible but not prime: $3^2 = (2+i\sqrt{5})(2-i\sqrt{5})$. In a PID, prime $\Leftrightarrow$ irreducible.
Unique factorization domains (UFD): definition, examples. In a UFD, prime $\Leftrightarrow$ irreducible. Computation of g.c.d.'s in a UFD.

Week 9

Lecture 25. [**DF**, §8.3, §7.5]
Every principal ideal domain has the unique factorization property.
Rings of fractions: general construction and universal property.
Fields of fractions: examples of $\mathbb{Q}$ and $F(X)$.

Lecture 26. [**DF**, §9.3]
Given a ring A with field of fractions F can results obtained in $F[X]$ be used in $A[X]$?
Gauss' Lemma: if A is a UFD and P is reducible in $F[X]$, then it is reducible in $A[X]$.
Corollary: if A is a UFD and the coefficients of P have g.c.d. 1, then P is irreducible in $F[X]$ if and only if it is irreducible in $A[X]$. Transfer theorem: A UFD $\Leftrightarrow$ $A[X]$ UFD.
Corollary: if A is a UFD, so is $A[X_1, \ldots, X_n]$.

Problem session 4. Quotients of $A[X]$, nilpotent elements.

Lecture 27. [**DF**, §13.1]
Two constructions of $\mathbb{C}$: as a subring of $\mathrm{M}_2(\mathbb{R})$ and as $\mathbb{R}[X]/(X^2+1)$.
Fields extensions, degree. If F is a field and $P \in F[X]$ is irreducible, then $F[X]/(P)$ is an extension of degree $\deg(P)$ of F in which P has a root. Conversely, if K is an extension of F in which P has a root α, then $F(\alpha) \simeq F[X]/(P)$.

Week 10

Lecture 28. Introduction to representation theory.
Fun: definitions and examples of representations (permutations, left regular).
Irreducibles, Schur's Lemma. Fourier analysis on abelian groups, projective representations of SO(3), representations of SU(2) and spin of particles.