Tentative study guide for Bruno's math 461d course (to the right: Cooperstein's book)

PART 1 – GROUPS

Week 0	**Preliminaries**. Injective, surjective, bijective functions.	Ch. 1.3
	Natural numbers. Proof by induction	Ch. 1.4
	Euclidean division algorithm. Greatest common divisor	pp. 35,37--39
	Fundamental theorem of Algebra (prime decomposition)	41-42
	Finding all integer solutions of a linear equation aX + bY =1	Missing
	Modular arithmetic: $Z_{n.}$ How to find the last digit of 9^{17}, say.	Missing. See 44-45
	Divisibility criteria	missing
Week 1	**Groups**: definition, uniqueness of inverse/identity, cancelation law	67—68, 77—80
	Examples: (Z,+), (Q,+), (R,+), (Q*, ×), (R*, ×), $GL_n(R)$, {f:A --> A bijective}.	66, 74
	Examples: Cayley table of four 4-element groups	
	Subgroups: definition	84-85
	3x1-criterion	missing
	Characterization of the subgroups of Z	?
	Cyclic groups	96-97
	Cyclic implies abelian	?
Week 2	Period (or order) of an element	96—97, 92—93
	LEMMA. x^m=e IFF the period of x divides m.	93 (cor. 2.3.12)
	Group homomorphisms: Definition of and examples	137-139
	Definition of isomorphic groups	143
	Every cyclic group is isomorphic to either Z, or some Z_n	?
	Between any two groups there is always a homomorphism (the "zero" homomorphism, mapping everything to the identity)	?
	LEMMA. For any homomorphism f, the period of f(x) divides the period of x.	145 (ex.4)
	Application: Number of homomorphisms from Z_6 to Z_8, say	?
Week 3	Definition of ker f and Im f	139—140
	Normality. (Example: Ker f is always normal)	122—124
	All subgroups of abelian groups are normal.	124 (rem. 2.7.1)
	REVISION: The group S_n of **permutations** (non-abelian for n > 2)	104—105
	How to write a permutation (3 ways): two-line notation, as product of disjoint cycles, as product of transpositions.	Cf.108—111
	Even permutations: the group $A_{n\,.}$ Sketch of what a 'simple' group is.	

Tentative study guide for Bruno's math 461d course (to the right: Cooperstein's book)

Week 4	Left cosets of a subgroup. Definition; characterization as equivalence classes of a relation of equivalence ($a \sim b \Leftrightarrow a^{-1} b$ is in the subgroup)	90-91
	Lemma: Any two left cosets of a finite group have same number of elements	Lemma 2.3.8
	Lagrange Theorem. The size of any subgroup divides the size of the group.	91 (thm. 2.3.9)
	Corollary. If x is in G, the period of x divides the size of G.	
	Right cosets of a subgroup. Characterization as equivalence classes of a relation of equivalence ($a \sim b \Leftrightarrow a b^{-1}$ is in the subgroup)	
	H is normal if and only if left cosets and right cosets coincide	127 (Lem. 2.7.6)
	Prop. If a subgroup of G has half the elements of G, then it is normal.	Ex. 4 p. 128
	Quotient groups	131—132
	{Normal subgroups} = {kernels of homomorphisms}	?
Week 5	Products	190—191
	Generators, linearly independent elements, bases	
	"Diagonalization" of integral matrices. THEOREM. Let A be any nonzero rectangular matrix with entries in Z. There are square integer matrices U, V, with determinant either 1 or -1, such that the matrix D=UAV is a (rectangular) matrix in which d_{11}, …, d_{tt} are positive integers, whereas all other entries are zero.	
Week 6	THEOREM. Let H be a subgroup of Z^n. Then there are positive integers $d_1, d_2 \dots d_t$ and there is a basis $\{v_1, v_2 \dots v_n\}$ of Z^n such that $\{d_1v_1, d_2v_2 \dots d_tv_t\}$ are a basis of H.	
	STRUCTURE THEOREM. Every finitely generated abelian group is isomorphic to some product of cyclic groups.	Cf. p. 207
	LEMMA. $Z_a \times Z_b$ is isomorphic to Z_{ab} if and only if GCD(a,b)=1.	
	THEOREM. (**Converse of Lagrange for Abelian groups**). Let m be a number dividing the cardinality of an Abelian group G. Then, there exists a subgroup H of G that has cardinality m.	
	REMARK. [Converse of Lagrange is false in general] There is no cardinality-6 subgroup of the 12-element group A_4 (the group of the even permutations of 4 elements.)	
	Structure Theorem, **uniqueness version.** Every finite abelian group can be decomposed in a unique way as product of cyclic groups whose sizes are prime powers.	

Tentative study guide for Bruno's math 461d course (to the right: Cooperstein's book)

Midterm

PART 2 – RINGS

Week 1	Rings: definition, examples, arithmetic properties. Commutative rings; Rings with 1.	213-215
	Domains: definition. [The book calls them "integral domains"]	226-229
	Def. **Field**. Every finite domain is a field.	218, 229
	Polynomials. Formal definition (as sequences). The indeterminate "X" stands for the sequence (0,1, 0….)	(something similar on pages 234-240)
	Degree of polynomials. Degree of sum. Degree of product.	234; see also exercise 1 on page 240
	Exercise: if the leading term of F is invertible, deg(FG) $\geq$ deg G.	
	A is a domain IFF A[x] is a domain.	
Week 2	**Euclidean division of polynomials**. Let A be any commutative ring with 1. Let F,G be two polynomials in A[X], such that the leading coefficient of G is invertible in A. Then there exists a unique pair (Q,R) of polynomials such that: (1) F=QG + R (2) either R=0, or deg R < deg G.	287—290; the book does it only in the special case where the ring is a field (so leading coefficient's obviously invertible).
	Corollary: Ruffini's theorem. Let a be an element of a commutative ring A with 1. Let F be a polynomial in A[X]. Then F(a)=0 if and only if F is a multiple of (X-a)	293-294. Note: Works for any ring F, whether F is a field (as the book states) or not.
	Theorem. In a domain A[x], every polynomial with n distinct roots has degree at least n. (This is false if A is not a domain: e.g. x^2-4 has four roots in Z_{12}).	
	Def: subring, ideal.	222, 244
	Ring homomorphisms. (Example: the projection from Z to Z_n; the "evaluation" homomorphism" from A[X] to A.) The image is always a subring, the kernel is even an ideal.	241-244
	LEMMA. If an ideal contains 1, it coincides with the whole ring.	Ex. 4 p. 247
	Corollary. A is a field IFF the only ideals of A are {0} and A itself.	
Week 3	Principal ideals. All ideals of Z are principal.	245 (ex. 3.4.8, 3.4.9)
	Definition of PID. Some ideals of Z[X] are not principal, e.g. the ideal of polynomials whose constant term is even, (X,2) .	
	Theorem. A is a field IFF A[X] is a PID.	The direction "if A is a field, A[x] is a PID" is basically Thm 3.9.2, p.288, coupled with Thm 3.8.2, page 277. The other direction is not done in the book.

Tentative study guide for Bruno's math 461d course (to the right: Cooperstein's book)

	Consequence: R[x,y] is not a PID.	
Week 4	Quotient rings. First homomorphism theorem for rings	250-254
	Some remarkable isomorphism: A[x] mod (X-a) is isomorphic to A. R[x] mod (X^2+1) is isomorphic to C (complex number).	
	Prime ideals.	258
	PROP. The ideal (n) is prime in Z IFF n is a prime number.	259
	An ideal I is prime IFF the quotient A/I is a Domain	259
	Sum of two ideals	254
	Maximal ideals.	260; 275
	An ideal I is maximal IFF A/I is a field.	260
	All maximal ideals are prime. **Theorem**: in a PID ring, all **nonzero** prime ideals are maximal.	Remark 3.6.1, p. 260; the theorem is very similar to Theorem 3.8.7, p.280
	(X) is prime in Z[x], but not maximal. (In fact, Z[x] is not a PID.)	
	Irreducible elements.	280
	Irreducible elements in C[X] are precisely polynomials of degree 1. Irreducible elements in R[X] are precisely polynomials of degree 1, and also, polynomials of degree 2 with negative Delta.	
	Prop. If A domain, and (a) is prime, then a is irreducible. (The converse is false, e.g. 2 is irreducible in Z[√-5], but not prime, basically because in this ring the number 6 factors in two different ways: 2 3 = 6 = (1 + √-5) (1 + √-5). The two factors on the right do not belong to the ideal (2), whereas their product (namely, 6) does.	Missing (cf. also theorem below)
	Theorem. If A PID, and a≠0, the following three facts are equivalent: 1. the element a is irreducible; 2. the ideal (a) is prime; 3. The ideal (a) is maximal.	Theorem 3.8.7, p. 280
	UFD rings. Examples: Z, Z[X], R, R[X], Q, Q[X], C, C[X]… Non-examples: Z[√-5], which is a domain, is not UFD.	304
	Lemma: in a PID, every ascending chain of ideals stabilizes.	missing
	Theorem. PID implies UFD.	missing
	Theorem [Gauss]. If A is UFD, then A[X] is UFD.	309
	Remark 1. UFD does not imply PID; a counterexample is Z[X].	
	Remark 2. If A is UFD, then any two elements have a greatest common divisor. However, unless A is PID, it is not true that the ideal (a,b) is generated by their GCD! Think of a=X, b=2, inside Z[X].	