Algebra Summary

Rings

Division Algorithm: If $a,b \in R$, $b \neq 0$, then $\exists\ q,r \in Z$ st. $a=bq+r$. q and r are unique if R is an integral domain

In the integers: $0 \leq r < b$

In Q[x]: r is of a lower degree than b.

Irreducible: p is irreducible if p is not 0, 1, or -1, and if there is not an a st. (p) is a proper subset of (a) which is itself a proper subset of R. (ie. P is not divisible by anything)

Prime: p is prime if p is not 0, -1, or 1, and whenever $bc \in (p)$, $b \in (p)$ or $c \in (p)$.

Ring: A ring is a set R with 2 binary operations, + and *, st.:

1. R is closed under +
2. + is associative
3. + is commutative
4. There is an additive identity (0_r)
5. For all a, there is a solution, b, to the equation a+b=0
6. R is closed under *
7. * is associative
8. the distributive property holds; a(b+c)=ab+ac

Ring With Identity. There is a 1_R such that a1=1a=a for all a.

Commutative Ring. * commutes.

Integral Domain. A nonzero commutative ring with 1 st. if ab=0, a=0 or b=0 (no zero divisors)

Field. A non-zero commutative ring with 1 in which every non-zero element is a unit.

Proposition. If F is a field and $a,b \in F$ are nonzero, then $ab \neq 0$ (ie. A field is an integral domain.)

Unit. A member of U_n where $U_n=\{x \in R \mid \exists\ y \text{ st. } xy=1\}$ (those which are invertible).

Zero Divisor. If ab=0 and $a \neq 0$ and $b \neq 0$, then a and b are zero divisors.

Additive Inverse. X st. A+X=0

Lemma. If x+y=x+z in R, then y=z

Remark. If x+y=x+z=0, then y=z and this is the additive inverse.

Proposition. $0_R * x = 0_R$

Proposition. -(ab)=(-a)(b)=a(-b); -(-a)=a; -(a-b)=-a-b; -(a-b)=b-a; (-a)(-b)=ab

Subring. If R is a ring and $S \subseteq R$, S is a subring of R if the + and * of R make S a ring.

Proposition. If $S \subseteq R$, S is a subring iff:

(1) S is closed under +
(2) S is closed under *
(3) S contains 0
(4) if $a \in S$, then $-a \in S$

Proposition. If S is a nonempty subset of R, S is a subring iff:

(1) S is closed under subtraction
(2) S is closed under multiplication

Theorem. If R is a ring, $a_1a_2\ldots a_n$ has a unique value, and association does not change it.

Lemma. If $e,f \in R$ st. ea=ae=1 and fa=af=1, then e=f. (Multiplicative identities are unique.)

Corollary. If there are both left and right identities, then the left identity equals the right identity.

Proposition. If S is a subring of R and $1_R \in S$, then 1_R is an identity for S.

Ideals. Let R be a commutative ring:

If $a \in R$, $(a)=\{ar \mid r \in R\}$

If $A \subseteq R$ ($A=\{a_1, a_2, \ldots a_n\}$), $(A) = \{\sum a_i r_i \mid r_i \in R, a_i \in A$, there are a finite number of terms in the sum$\}$

$(0)=\{0\}$, $(R)=R$; If $1_R \in A$, then $(A)=R$

(A) absorbs other elements of R (ie. If $i \in (A)$ and $r \in R$, then $ir \in (A)$)

(A) is an ideal (*Definition.* An ideal is a subring of R which absorbs.)

All ideals in the polynomials of fields and integers are principal (can be generated by 1 element).

Definition. I is <u>prime</u> $\Leftrightarrow$ R/I is an integral domain $\Leftrightarrow$ whenever $a*b \in I$, $a \in I$ or $b \in I$

Definition. I is <u>maximal</u> $\Leftrightarrow$ R/I is a field $\Leftrightarrow$ there no other ideals in R that contain I

Equivalence and Ideals.

$[a]_I = \{a+i \mid i \in I\}$

TFAE: $b \in [a]_I$, $[b]_I \cap [a]_I \neq \varnothing$; $[b]_I = [a]_I$; $a \equiv b \pmod I$

R/I is called a quotient ring.

Operations: [a]+[b]=[a+b]; [a][b]=[ab]

Special Case: Integers

Theorem. If $b \neq 0$, then $\exists$ a smallest non-negative element $r \in [a]_b$ and $0 \leq r < b$.

Theorem. If a and b are not both 0, the (a,b) has a smallest positive element d. d | a and d | b. If c | a and c | b, the d | c. Also, (a,b) = (d)

Theorem. In the integers, prime and irreducible are equivalent.

Theorem. Every integer other than 0 and ±1 can be written uniquely as a product of primes.

Special Case: Polynomials

Formal Power Series. $R[[x]]=\Sigma$ (i=0 to i=∞) $a_i x^i$ where $a_i \in R$ and x is not; *Polynomial* is from i=0 to i=n.

Addition. $a(x) + b(x) = \sum$(i=0 to i=n) $(a_i+b_i)x^i$

Multiplication. $a(x)b(x)=\sum$(i=0 to m+n) $(\sum (j \le i)\ a_j b_{i-j}))\ x^i$

Leading Coefficient. $a_n x^n$ where a(x) is the sum from i=0 to n (the term with highest power of x)

Proposition. If $f(x)\neq 0$, then deg(f(x)) is the smallest element of $\{\deg(g(x)) \mid g(x)\in(f(x))\}$

Associates. f(x) and g(x) are associates iff f(x)=u*g(x) where u is a unit.

Monic. The leading coefficient is 1. (In F[x], there is always a unique monic associate.)

Every polynomial can be factored into monic irreducibles.

If p(x) is irreducible then any associate of p(x) is irreducible.

If p(x) and q(x) are irreducible and p(x)|q(x), they are associates.

If R is an integral domain, prime => irreducible; in a field, irreducible => prime.

When $f(r) = 0_R$, r is a root of f(x) and (x-r)|f(x).

If deg(f(x))= 2 or 3, f(x) is irreducible ⇔ f(x) has no roots.

Let $\varphi_n(f(x)) = \sum[a_i]_n x^i$. If $\varphi_n(f(x))$ is reducible , then f(x) is irreducible. (But not the reverse.)

Gauss's Lemma

Eisenstein's Criterion: If p does not divide a_k, and p divides a_0, a_1, …, a_{k-1}, and p^2 does not divide a_0, then f(x) is irreducible.

Suppose $F\subseteq G$ are fields, and $\alpha\in G$. $F[\alpha] = \{\sum f_i\alpha^i \mid f_i\in F\}$

F[x] → F[α] is a homomorphism

If p(x) is a polynomial of lowest degree st. p(α)=0, F[x]/p(x) → F[α] is an isomorphism

F[x] can be extended to (F[x]/(p(x)))[y].

Homomorphisms and Isomorphisms

Homomorphism of Rings.. If f is a mapping from R to S, and f(a+b)=f(a)+f(b) and f(ab)=f(a)f(b), then f is a homomorphism of rings.

Homomorphism of Groups. A function f: G→H is a homomorphism if f(a*b)=f(a)*f(b).

Isomorphism. If f is bijective and a homomorphism, it is an isomorphism.

Automorphisms. Any isomorphism from G to itself is an automorphism. The set of all automorphisms of G is a group, Aut(G).

Injective = Monomorphism = One-to-one

Surjective = Epimorphism = Onto

Bijective = Isomorphism = One-to-one and Onto

Proposition. The composition of homomorphisms is a homomorphism.

Proposition. The inverse of an isomorphism is an isomorphism.

Proposition. Isomorphism is an equivalence relation.

Proposition. In a homomorphism of rings:

1. $f(0_R)=0_S$
2. f(-a)=-f(a)
3. f(a-b)=f(a)-f(b)
4. f(r) is a subring of S
5. If R has an identity, then $f(1_R)$ is an identity for f(R), but not necessarily for S
   If f is an isomorphism, it is the identity.
6. If a is a unit in R then f(a) is a unit is f(R)

Proposition. If f: G→H is a homomorphism:

1. $f(e_G)=e_H$
2. $f(a^{-1})=(f(a))^{-1}$
3. $f(a^n)=f(a)^n$
4. Im f is a subgroup of H
5. ker f is a subgroup of G
6. If f is one to one, then G is isomorphic to Im f

Proposition. In an isomorphism (f: R → S):

1. $a=1_R \Leftrightarrow f(a)=1_S$
2. $a=0_R \Leftrightarrow f(a)=0_S$
3. a is a unit in R ⇔ f(a) is a unit in S
4. $a^i = 1_R \Leftrightarrow (f(a))^i = 1_S$

5. The number of elements in R and S is the same (#R=#S)
6. The number of units in R equals the number of units in S

If f: R → S is a homomorphism of rings, ker(f) is an ideal. If I is an ideal, then it is the kernel of the homomorphism f(a)=$[a]_I$.

Pf. f(a)=0 ⇔ [a]=[0] ⇔ a≡0 (mod I) ⇔ a-0∈I ⇔ a∈I. So a∈ker f ⇔ a∈I.

Im (f) = {s∈S | ∃r st. f(r) = s}

f is onto ⇔ Im f = S; Im f is always a subring and isomorphic to R (not usually an ideal, though)

Theorem. If f is a homomorphism, then ker f is normal in G.

First Isomorphism Theorem. If f: R → S is a homomorphism, then f: R/(ker f) → Im f st. [a] → f(a) is an isomorphism of rings.

R → R/(ker f) is a surjective homomorphism.

f: R/(ker f) → S is injective (since the kernel is being reduced to 1 element)

f: R → S is an isomorphism if it is a homomorphism, ker f={0} and Im f=S

First Homomorphism Theorem. Let f be a homomorphism. Then the map from G/ker f to Im f is an isomorphism.

Third Homomorphism Theorem of Groups. Let K and N be normal subgroups, such that N is contained in K. Then, K/N is a normal subgroup of G/N and (G/N)/(K/N) is isomorphic to G/K.

Groups

Group. A group is a set S with an operation * such that:

1. for all s,t ∈ S, s*t ∈ S (closure)
2. ∃ e∈S such that s*e=e*s=s for all s (identity)
3. for all s∈S, there exists a t∈S such that st=ts=e. (inverses)
4. for all s,t,u∈S, (s*t)*u=s*(t*u) (association)

A group is <u>abelian</u> if:

5. a*b=b*a (commutes)

Proposition. Identities and inverses are unique in groups. Cancellation holds (because of inverses).

Corollary. $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$.

Order. The order of g, |g|, = |{e, g, g^2, g^3, …}|. |G| = the number of elements in G.

Lagrange's Theorem. If g∈G, then the order of g divides the order of G.

Theorem. If a∈G, then $a^i = a^j$ ⇔ i=j mod |a|.

Corollary. In an Abelian group:

$|a^t| = |a|/t$ if t divides |a|.

If ab=ba and (|a|,|b|)=1, then |ab|=|a||b|.

If c is an element of maximum order in G and |c| is finite, then |a| divides |c| for all a∈G.

If (|a|, |b|)=d, then $|a(b^d)| = |a^db|$ = lcm(|a|, |b|).

Subgroup. If G is a group and H is a subset of G, then H is a subgroup of G if H is a group under G's operation.

Subgroups: H⊆G is a subgroup if H is closed under the group operation and contains inverses (and is non-empty.)

H is a subgroup of G (1) if H is non-empty and (2) if ab^{-1}∈H when a,b∈H.

If |H| is finite and H is closed, then H is a subgroup.

Cyclic Subgroup. If a∈G, then <a>={a^n | n∈**Z**} is a subgroup. <a> is a cyclic group and a is the generator.

Theorem. Ever subgroup of a cyclic group is cyclic.

Definition. If S⊆G, <S> = {all possible products of all elements in S and their inverses, with repeats in any order}.

Fact. <S> = ∩ H, where S⊆H≤G. ie. <S> is the intersection of all subgroups that contain S.

Lemma. The intersection of any set of subgroups is a subgroup.

Cosets. For K ≤ G and a ∈ G, Ka ={ka | k∈K}. Note that aK is not necessarily Ka if K is not a normal subgroup. Also, a=b (mod K) if ab^{-1}∈K. G/K = {distinct Ka}

Theorem. The following are equivalent, if K is a subgroup of G:

1. Ka ∩ Kb ≠ ∅

2. $b \in Ka$
3. $Kb = Ka$
4. $a = b \pmod K$

Note. For all $a \in G$, $|Ka|=|K|$. Also, $|K|$ divides $|G|$. So, the number of cosets of K is $[G:K]$, always an integer.

Normal Subgroup. K is a normal subgroup of G if, for all $k \in K$ and all $a \in G$, $aka^{-1} \in K$.

Simple. If G has no normal subgroups, then G is simple.

Corollary. Every subgroup of an abelian group is normal.

Theorem. If $[G:K]=2$, then K is normal in G.

Proposition. K is normal in G $\Leftrightarrow$ $aKa^{-1}=K$ for all a in G.

Theorem. G/K is a group (with operation $Ka*Kb=K(a*b)$) if K is normal.

Theorem. Suppose N is normal in G and K is a subgroup of G which contains N, then N is normal in K.

Theorem. Suppose N and K are normal in G, and K is contained in N. Then K is normal in N, N/K is normal in G/K and $(G/K)/(N/K) \cong (G/N)$.

Theorem. Suppose N is normal in G. Then there is a one-to-one correspondence between subgroups of G/N and subgroups of G containing N, which sends normal subgroups to normal subgroups.

Corollary. Suppose G is finite, and $G_1 < G$ is a proper normal subgroup of G with largest possible order. The, G/G_1 is simple. (This leads to decomposition…)

Theorem. If G is finite, then any two composition series of G will have the same factors.

Conjugation and Inn. Let $\varphi_c(g)=cgc^{-1}$. Then φ_c is conjugation by c. $Inn(G) = \{\varphi_c \mid c \in G\}$ ("Inner automorphism")

Theorem. The center of G (ie. Z(G)) is the kernel of the map from c to conjugation by c.

Conjugacy Class. The conjugacy class of a is all b, such that $b=gag^{-1}$, for some $g \in G$.

Theorem. Conjugacy is an equivalence relation.

Note. G is the union of all conjugacy classes. $|G| = |C_1| + |C_2| + \ldots = |Z(G)| + |C_2| + \ldots$.

Note. For all i, $|C_i|$ divides $|G|$.

Note. All elements in Z(G) are in conjugacy classes by themselves.

Note. Just because two elements are conjugate in G doesn't mean they're conjugate in a subgroup of G.

Note. A subgroup of G is normal if and only if it is a union of conjugacy classes. (ie., no partial ones)

Center. If G is any group, the center of G, $Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$.

Theorem. The center of G is a normal subgroup.

Theorem. If f is a homomorphism, then ker f is normal in G.

Permutation. A rearrangement of elements. The group of all permutations on n elements is S_n.

Cayley's Theorem. Every group is isomorphic to a subgroup of A(G), where A(G) is the map from G to a permutation of G.

Theorem. If $\tau \in S_n$, then the conjugacy class of τ is all elements in S_n with the same cycle structure.

Alternating Group. The set of all permutations that can be written as the product of an even number of transpositions. (Where a transposition is (ab)—a flip of elements.)

Theorem (of Signs). From each n>1, there is a unique epimorphism of groups $S_n \rightarrow \{1, -1\}$. +1 corresponds to permutations which can be written as an even number of transpositions.

Theorem. The alternating group (A_n) is the kernel of sign and therefore a normal subgroup of S_n.

Theorem. A_n is simple iff $n \neq 4$.

Lemma. If $n \geq 5$, all 3-cycles are conjugate in A_n.

Lemma. If $n \geq 4$, all products of 2 disjoint transpositions are conjugate in A_n.

Commutator. $aba^{-1}b^{-1}$ is a commutator.

Theorem. Suppose N is normal in G. G/N is abelian $\Leftrightarrow$ $\forall a,b \in G$, $aba^{-1}b^{-1} \in N$. (ie. all commutators are in N)

Centralizer. $C(a) = \{g \in G \mid ag = ga\}$.

Lemma. $C(a) \leq G$ (where C(a) is the centralizer of a)

Theorem. $[G:C(a)]$ = the number of elements conjugate to a

Lemma. Every cyclic group is Abelian and isomorphic to $\mathbf{Z}_n$ where $n=|a|$.

Proposition. If G is cyclic and $G=\langle a \rangle$, then either G is infinite and $\mathbf{Z} \cong G$ or G is of order k, and $G \cong \mathbf{Z}_k$.

Corollary. Any two cyclic groups of the same order are isomorphic.

Theorem. If G is a group, then G is simple and abelian $\Leftrightarrow$ $G \cong \mathbf{Z}_p$

Theorem. $\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn} \Leftrightarrow (m,n)=1$.

Classification Theorem for Finite Abelian Groups. If $|G|=n$ and G is abelian, the $G \cong Z_a \times Z_b \times \ldots$, where the product of the subscripts is n.

Note. G is finite and $|g|=p^k$ for all $g \Leftrightarrow |G|=p^n$.

Cauchy's Theorem. If $|G|=n$ and $p|n$, then $\exists g \in G$ such that $|g|=p$.

Sylow p-Subgroup. If $p^k|G$ and k is the highest power of p which divides G, then $H \leq G$ such that $|H|=p^k$ is called a Sylow p-subgroup. (it might not be normal.)

First Sylow Theorem. If p^k divides $|G|$, then $\exists H \leq G$ such that $|H|=p^k$. H may not be normal.

Second Sylow Theorem. Any two Sylow p-subgroups are conjugate.

Third Sylow Theorem. The number of Sylow p-subgroups is 1+mp (ie., 1 mod p) AND divides G.

Simple with Sylow? If there must be only 1 Sylow p-subgroup of some order, then that subgroup is normal.

12 trick. Show that enough elements must be contained in some subgroups (and therefore have certain orders), that there can be only one of a different subgroup.

24 trick. Let H be a Sylow p-subgroup. Consider the homomorphism $G \rightarrow A(G/H)$. Show that this must have a kernel which is proper. This is a normal subgroup.

Isomorphism Classes (and Reasons for Non-Simplicity) for Selected Orders.

Orders of p have only $\mathbf{Z}_p$

Orders of 2p have only $\mathbf{Z}_{2p}$ and D_p

Corollary to Cauchy's Theorem. If $|G|=2p$, then wither $G \cong \mathbf{Z}_{2p}$ or $G \cong D_p$.

Orders of p^2 have only $\mathbf{Z}_{p*p}$ and $\mathbf{Z}_p \times \mathbf{Z}_p$

Theorem. If $|G| = p^k$ then $|Z(G)| > 1$, and the center is non-trivial.

Lemma. If G/Z(G) is cyclic, then G is abelian.

Corollary. If $|G|=p^2$ then G is abelian.

Orders of p^n and pq (p and q primes) have no simple groups (by *Third Sylow Theorem*)

Examples

Rings

Rings: zero ring, $M_n(R)$ [which has an identity if R does]

$R \times S = \{(r,s) \mid r \in R \text{ and } s \in S\}$

$0_{R\times S} = (0_R, 0_s)$

$1_{R\times S} = (1_R, 1_s)$, if both rings have identities

The ring of $(r, 0_S)$ is a subring, with a different identity element.

R[[x]] and R[x]

Commutative rings with identity: $\mathbf{Z}_n$, F[x]/(p(x))

Integral Domains: integers, F[x]

Fields: rationals, reals, $\mathbf{Z}_p$

Isomorphisms

$Z_{mn} \rightarrow Z_m \times Z_n$ (where (m,n)=1)

R and the constant polynomials of R[x]

$F[x]/(p(x)) \rightarrow F[a]$, where p(a)=0

Groups

A ring together with + is abelian.

The units of a ring with identity is a group. (*Theorem*. If F is a finite field then U(F) (all elements except 0) is cyclic.)

the positive (or nonzero) elements of **R** or **C** with multiplication

$GL_n(F)$ = invertible n by n matrices with entries in F

S_n, A_n

Aut(G) [automorphisms], Inn(G) [conjugation], A(G) [permutations]

Z, $\mathbf{Z}_n$ (cyclic groups)

$\mathbf{Z}_a \times \mathbf{Z}_b \times \ldots$
D_n (dihedral groups)
$\mathbf{H}$ (quaternions)

Rings

Ring: A ring is a set R with 2 binary operations, + and *, st.:

1. R is closed under +
2. + is associative
3. + is commutative
4. There is an additive identity (0_r)
5. For all a, there is a solution, b, to the equation a+b=0
6. R is closed under *
7. * is associative
8. the distributive property holds; a(b+c)=ab+ac

Field. A non-zero commutative ring with 1 in which every non-zero element is a unit.

Integral Domain. A nonzero commutative ring with 1 st. if ab=0, a=0 or b=0

Proposition. If $S \subseteq R$, S is a subring iff:

(1) S is closed under + (2) S is closed under *

(3) S contains 0 (4) if $a \in S$, then $-a \in S$

Proposition. If S is a nonempty subset of R, S is a subring iff:

S is closed under subtraction and under multiplication.

Definition. An ideal is a subring of R which absorbs. (If $a \in R$ and $i \in I$ then $ai \in R$ and $ia \in R$)

Definition. I is <u>prime</u> $\Leftrightarrow$ R/I is an integral domain $\Leftrightarrow$ whenever $a*b \in I$, $a \in I$ or $b \in I$

Definition. I is <u>maximal</u> $\Leftrightarrow$ R/I is a field $\Leftrightarrow$ there no other ideals in R that contain I

Polynomials

Formal Power Series. $R[[x]]=\Sigma$ (i=0 to i=∞) $a_i x^i$ where $a_i \in R$ and x is not; *Polynomial* is from i=0 to i=n.

Multiplication. $a(x)b(x)=\sum$(i=0 to m+n) $(\sum (j \le i)\ a_j b_{i-j})\ x^i$

Proposition. If $f(x) \neq 0$, then deg(f(x)) is the smallest element of $\{\deg(g(x)) \mid g(x) \in (f(x))\}$

Every polynomial can be factored into monic irreducibles.

If p(x) is irreducible then any associate of p(x) is irreducible.

If p(x) and q(x) are irreducible and p(x)|q(x), they are associates.

If R is an integral domain, prime => irreducible; in a field, irreducible => prime.

When $f(r) = 0_R$, r is a root of f(x) and (x-r)|f(x).

If deg(f(x))= 2 or 3, f(x) is irreducible $\Leftrightarrow$ f(x) has no roots.

Let $\varphi_n(f(x)) = \sum[a_i]_n x^i$. If $\varphi_n(f(x))$ is irreducible , then f(x) is irreducible. (But not the reverse.)

Eisenstein's Criterion: If p does not divide a_k, and p divides a_0, a_1, …, a_{k-1}, and p^2 does not divide a_0, then f(x) is irreducible.

Suppose $F \subseteq G$ are fields, and $\alpha \in G$. $F[\alpha] = \{\sum f_i \alpha^i \mid f_i \in F\}$

$F[x] \rightarrow F[\alpha]$ is a homomorphism

If p(x) is a polynomial of lowest degree st. $p(\alpha)=0$, $F[x]/p(x) \rightarrow F[\alpha]$ is an isomorphism

Homomorphisms/Isomorphisms

Proposition. In a homomorphism:

1. $f(0_R) = 0_S$; $f(e_G) = e_H$
2. $f(-a)=-f(a)$; $f(a^{-1})=f(a)^{-1}$
3. $f(a-b)=f(a)-f(b)$; $f(ab^{-1})=f(a)f(b)^{-1}$
4. f(r) is a subring/subgroup of S
5. If R has an identity, then $f(1_R)$ is an identity for f(R), but not necessarily for S
   If f is an isomorphism, $f(1_R)$ is the identity.
6. If a is a unit in R then f(a) is a unit is f(R)

Proposition. In an isomorphism ($f: R \rightarrow S$):

1. $a=1_R \Leftrightarrow f(a)=1_S$
2. $a=0_R \Leftrightarrow f(a)=0_S$
3. a is a unit in R $\Leftrightarrow$ f(a) is a unit in S
4. $a^i = 1_R \Leftrightarrow (f(a))^i = 1_S$
5. The number of elements in R and S is the same (#R=#S)
6. The number of units in R equals the number of units in S

Every ideal/normal subgroup is the kernel of $f: R \rightarrow R/I$. Every kernel is an ideal/normal subgroup.

First Isomorphism Theorem. If $f: R \rightarrow S$ is a homomorphism, then $f: R/(\ker f) \rightarrow \text{Im } f$ st. $[a]_I \rightarrow f(a)$ is an isomorphism of rings/groups.

Third Homomorphism Theorem of Groups. Let K and N be normal subgroups, such that N is contained in K. Then, K/N is a normal subgroup of G/N and (G/N)/(K/N) is isomorphic to G/K.

Groups

Group. A group is a set S with an operation * such that:

1. for all $s,t \in S$, $s*t \in S$ (closure)
2. $\exists\ e \in S$ such that $s*e=e*s=s$ for all s (identity)
3. for all $s \in S$, there exists a $t \in S$ such that st=ts=e. (inverses)
4. for all $s,t,u \in S$, $(s*t)*u=s*(t*u)$ (association)

A group is <u>abelian</u> if:

5. a*b=b*a (commutes)

Order. The order of g, |g|, = |{e, g, g^2, g^3, …}|. |G| = the number of elements in G.

Lagrange's Theorem. If $g \in G$, then the order of g divides the order of G.

Theorem. If $a \in G$, then $a^i = a^j \Leftrightarrow i=j \bmod |a|$.

Corollary. In an Abelian group:

$|a^t| = |a|/t$ if t divides |a|.

If ab=ba and (|a|,|b|)=1, then |ab|=|a||b|.

If c is an element of maximum order in G and |c| is finite, then |a| divides |c| for all $a \in G$.

If (|a|, |b|)=d, then $|a(b^d)| = |a^d b| = \text{lcm}(|a|, |b|)$.

Subgroups: $H \subseteq G$ is a subgroup if H is closed under the group operation and contains inverses (and is non-empty.)

H is a subgroup of G (1) if H is non-empty and (2) if $ab^{-1} \in H$ when $a,b \in H$.

If |H| is finite and H is closed, then H is a subgroup.

Cyclic Subgroup. If $a \in G$, then $\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$ is a subgroup. $\langle a \rangle$ is a cyclic group and a is the generator.

Theorem. Ever subgroup of a cyclic group is cyclic.

Lemma. The intersection of any set of subgroups is a subgroup.
Cosets. For $K \le G$ and $a \in G$, $Ka = \{ka \mid k \in K\}$. Note that aK is not necessarily Ka if K is not a normal subgroup. Also, a=b (mod K) if $ab^{-1} \in K$. G/K = {distinct Ka}
Theorem. The following are equivalent, if K is a subgroup of G:
1. $Ka \cap Kb \neq \emptyset$ 2. $b \in Ka$
3. Kb = Ka 4. a = b (mod K)

Note. For all $a \in G$, |Ka|=|K|. Also, |K| divides |G|. So, the number of cosets of K is [G:K], always an integer.
Corollary. Every subgroup of an abelian group is normal.
Theorem. If [G:K]=2, then K is normal in G.
Proposition. K is normal in G $\Leftrightarrow aKa^{-1}=K$ for all a in G.
Theorem. G/K is a group (with operation Ka*Kb=K(a*b)) if K is normal.
Theorem. Suppose N is normal in G and K is a subgroup of G which contains N, then N is normal in K.
Theorem. Suppose N is normal in G. Then there is a one-to-one correspondence between subgroups of G/N and subgroups of G containing N, which sends normal subgroups to normal subgroups.
Corollary. Suppose G is finite, and $G_1 < G$ is a proper normal subgroup of G with largest possible order. The, G/G_1 is simple.
Theorem. If G is finite, then any two composition series of G will have the same factors.
Conjugacy Class. The conjugacy class of a is all b, such that $b=gag^{-1}$, for some $g \in G$.
Note. G is the union of all conjugacy classes. $|G| = |C_1| + |C_2| + \ldots = |Z(G)| + |C_2| + \ldots$.
Note. For all i, $|C_i|$ divides |G|.
Note. Just because two elements are conjugate in G doesn't mean they're conjugate in a subgroup of G.
Note. A subgroup of G is normal if and only if it is a union of conjugacy classes. (ie., no partial ones)
Cayley's Theorem. Every group is isomorphic to a subgroup of A(G), where A(G) is the map from G to a permutation of G.
Theorem. If $\tau \in S_n$, then the conjugacy class of τ is all elements in S_n with the same cycle structure.
Theorem. The alternating group (A_n) is the kernel of sign and therefore a normal subgroup of S_n.
Lemma. If $n \ge 5$, all 3-cycles are conjugate in A_n.
Theorem. Suppose N is normal in G. G/N is abelian $\Leftrightarrow \forall a,b \in G, aba^{-1}b^{-1} \in N$. (ie. all commutators are in N)
Centralizer. $C(a) = \{g \in G \mid ag = ga\}$. This is a subgroup of G.
Theorem. [G:C(a)] = the number of elements conjugate to a
Theorem. If G is a group, then G is simple and abelian $\Leftrightarrow G \cong \mathbf{Z}_p$
Theorem. $\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn} \Leftrightarrow (m,n)=1$.
Classification Theorem for Finite Abelian Groups. If |G|=n and G is abelian, the $G \cong Z_a \times Z_b \times \ldots$, where the product of the subscripts is n.
Cauchy's Theorem. If |G|=n and p|n, then $\exists g \in G$ such that |g|=p.
Sylow p-Subgroup. If $p^k | G$ and k is the highest power of p which divides G, then $H \le G$ such that $|H|=p^k$ is called a Sylow p-subgroup. (it might not be normal.)
First Sylow Theorem. If p^k divides |G|, then $\exists H \le G$ such that $|H|=p^k$. H may not be normal.
Second Sylow Theorem. Any two Sylow p-subgroups are conjugate.
Third Sylow Theorem. The number of Sylow p-subgroups is 1+mp (ie., 1 mod p) AND divides G.
Simple with Sylow? If there must be only 1 Sylow p-subgroup of some order, then that subgroup is normal.

12 trick. Show that enough elements must be contained in some subgroups (and therefore have certain orders), that there can be only one of a different subgroup.

24 trick. Let H be a Sylow p-subgroup. Consider the homomorphism $G \rightarrow A(G/H)$. Show that this must have a kernel which is proper. This is a normal subgroup.

Examples
Rings: zero ring, $M_n(R)$ [which has an identity if R does], R[[x]] and R[x]
$R \times S = \{(r,s) \mid r \in R \text{ and } s \in S\}$
$0_{R \times S} = (0_R, 0_s)$; $1_{R \times S} = (1_R, 1_s)$, if both rings have identities
The ring of $(r, 0_S)$ is a subring, with a different identity element.
Commutative rings with identity: $\mathbf{Z}_n$, F[x]/(p(x))
Integral Domains: integers, F[x]
Fields: rationals, reals, $\mathbf{Z}_p$
Isomorphisms
$Z_{mn} \rightarrow Z_m \times Z_n$ (where (m,n)=1)
R and the constant polynomials of R[x]
$F[x]/(p(x)) \rightarrow F[a]$, where p(a)=0
Groups
A ring together with + is abelian.
The units of a ring with identity is a group. (*Theorem*. If F is a finite field then U(F) (all elements except 0) is cyclic.)
the positive (or nonzero) elements of **R** or **C** with multiplication
$GL_n(F)$ = invertible n by n matrices with entries in F
S_n, A_n
Aut(G) [automorphisms], Inn(G) [conjugation], A(G) [permutations]
$\mathbf{Z}$, $\mathbf{Z}_n$ (cyclic groups), $\mathbf{Z}_a \times \mathbf{Z}_b \times \ldots$ (isomorphic to ALL abelian groups)
D_n (dihedral groups), **H** (quaternions)
Isomorphism Classes (and Reasons for Non-Simplicity) for Selected Orders.
Orders have only $\mathbf{Z}_p$

Orders of 2p have only $\mathbf{Z}_{2p}$ and D_p
Orders of p^2 have only $\mathbf{Z}_{p*p}$ and $\mathbf{Z}_p \times \mathbf{Z}_p$
Orders of p^n and pq (p and q primes) have no simple groups