MAT1100 Glossary of Terms

Unit: An invertible element in a ring that has an inverse element under the multiplicative operation.

Unity: An element 1 in the ring that acts as the identity under multiplication. Also note that $(-1)a = -a$ and $(-1)(-1) = 1$.

Integral Domain: A **commutative ring** with unity and no zero-divisors.

Zero-Divisors: A nonzero element a of a **commutative** ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Cancellation in IDs: Let a, b, and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

Ideal: A subring A of a ring R is called a (two-sided) ideal of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A.

Ideal Test: A nonempty subset A of a ring R is an ideal of R if:
1) $a - b \in A$ whenever $a, b \in A$
2) ra and ar are in A whenever $a \in A$ and $r \in R$

Prime Ideal: Is a proper Ideal of a commutative ring R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$.

Maximal Ideal: Is a proper Ideal of a commutative ring R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

Principal Ideal Domain (PID): An integral domain R in which every ideal has the form $\langle a \rangle = ra | r \in R$ for some a in R. In other words every ideal is principal meaning that it can be generated by a single element.

a divides b or $a|b$: $a|b$ means $a \neq 0$, $\exists q$ such that $aq = b$. It has the property that if $a|b$ and $b|a \leftrightarrow \exists u \in R^*$ such that $a = ub$ (where R^* is the set of units of R).

Greatest Common Divisor (gcd): For $a, b \in R$ $gcd(a, b)$ is a $q \in R$ such that:
1) $q|a$ and $q|b$
2) $q'|a$ and $q'|b$ implies that $q'|q$

Associates: Elements a and b of an integral domain R are associates if $a|b$ and $b|a \leftrightarrow \exists u \in R^*$ such that $a = ub$. If a and b are associates we write $a \sim b$.

Irreducible : A nonzero element a of an integral domain D is irreducible if a is not a unit and, whenever $b, c \in D$ with $a = bc$, then b or c is a unit.

Prime : A nonzero element a of an integral domain D is called prime if a is not a unit and $a|bc$ implies $a|b$ or $a|c$ which is equivalent to saying $\langle p \rangle = R_p$ is a prime ideal.

Prime implies Irreducible : In an integral domain, every prime is an irreducible.

Unique Factorization Domain (UFD) : An integral domain is a UFD if:
1) every nonzero element of D that is not a unit can be written as a product of irreducibles
2) the factorization into irreducibles is unique up to associates and the order in which that factors appear

Euclidean Domain : An integral domain D that has a function d (called the measure) from the nonzero elements of D to the nonnegative integers such that:
1) $d(a) \leq d(ab)$ for all nonzero $a, b \in D$
2) if $a, b \in D, b \neq 0$, then there exist elements q and r in D such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

Dedekind-Hasse norm : A function on an integral domain that generalizes the notion of a Euclidean function on Euclidean domains. $d : R\ \{0\} \to \mathbb{N}_{>0}$ (or add $d(0) = 0$) such that if $a, b \neq 0$ either $b|a$ ($a \in \langle b \rangle$) or $0 \neq x \in \langle a, b \rangle$ with $d(x) < d(a)$.

Module : A module over a ring R is "a vector space over R" a set M with $0 \in M$, $+ : M \times M \to M$, $\times : R \times M \to M$ such that:
1) $(M, +, 0)$ is an abelian group
2) $1_R m = m$ where $m \in M$ $a(bm) = (ab)m$ where a, b are scalars.
3)$(a + b)m = am + bm$ and $a(m + n) = am + an$

Direct Sum : Given two modules M, N over the same ring we can construct a new module $M \oplus N = \{(m, n) : m \in M, n \in N\}$ such that:
1)$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)$
2)$a(m, n) = (am, an)$

Sylow Theorems :

Theorem 1 : For any prime factor p with multiplicity n of the order of a finite group G, there exists a Sylow p-subgroup of G, of order p^n.

Corollary (Cauchy's Theorem) : Given a finite group G and a prime number p dividing the order of G, then there exists an element (and hence a subgroup) of order p in G.

Theorem 2 : Given a finite group G and a prime number p, all Sylow p-subgroups of G are conjugate to each other, i.e. if H and K are Sylow p-subgroups of G, then there exists an element g in G with $g^{-1}Hg = K$.

Theorem 3 : Let p be a prime factor with multiplicity n of the order of a finite group G, so that the order of G can be written as $p^n m$, where $n > 0$ and p does not divide m. Let n_p be the number of Sylow p-subgroups of G. Then the following hold:
1) n_p divides m, which is the index of the Sylow p-subgroup in G.
2) $n_p \equiv 1 \pmod{p}$.
3) $n_p = |G : N_G(P)| = \frac{|G|}{|N_G(P)|}$, where P is any Sylow p-subgroup of G and N_G denotes the normalizer.

Centralizer : The centralizer of a subset S of a group G is defined to be $C_G(S) = \{g \in G | sg = gs foralls \in S\}$.

Normalizer : The normalizer of S in the group G is defined to be $N_G(S) = \{g \in G | gS = Sg\}$.

Normal Subgroup : A subgroup N of a group G is called a normal subgroup if it is invariant under conjugation; that is, for each element n in N and each g in G, the element gng^{-1} is still in N. This can be written as $N \triangleright G \leftrightarrow \forall n \in N, \forall g \in G, gng^{-1} \in N$.

Group Homomorphism : A homomorphism ϕ from a group G to a group $\bar{G}$ is a mapping from G to $\bar{G}$ that preserves the group operation. That is $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Kernel of a Homomorphism : The kernel of a homomorphism ϕ from a group G to a group with the identity e is the set $\{x \in G | \phi(x) = e\}$. The kernel of ϕ is denoted $Ker\phi$ and is a normal subgroup of G.

Simple Group : A simple group is a nontrivial group G that has no normal subgroups other than itself and $\{e\}$.

Isomorphism Theorems for Groups :

Theorem 1 : If $\phi : G \to H$ then $G/Ker\phi \cong im\phi$.

Theorem 2 : If $H, K < G$ and $H < N_G(K)$ then $HK/K \cong H/(H \cap K)$.

Theorem 3 : If $K, N \triangleright G$ and $K \subseteq N \subseteq G$ then $\frac{G/K}{H/K} \cong G/H$.

Theorem 4 : If $N \triangleright G$ then $\pi : G \to g/N$ induces a "faithful" bijection between subgroups $\{H : N < H < G\}$ and subgroups of G/N. This means that if $N < H < G$ then $\pi(H) < G/N$ and this is a bijection with all subgroups of G/N.
1) $N < A < B < G \Rightarrow \pi(A) < \pi(B)$
2) $A \triangleright B \Rightarrow \pi(A) \triangleright \pi(B)$
3) $\pi(A \cap B) = \pi(A) \cap \pi(B)$

Isomorphism Theorems for Rings :

Theorem 1 : If $\varphi : R \to S$ then $R/Ker\varphi \cong im\varphi$.

Theorem 2 : If A is a subring of R and I is a proper ideal, then $\frac{A+I}{I} \cong \frac{A}{A\cap I}$ and $a + I \to a + (A \cap I)$.

Theorem 3 : If $I \subset J \subset R$ are proper ideals then $\frac{R/I}{J/I} \cong R/J$ (note that $J/I = j + I$).

Theorem 4 : Given a proper ideal $IsubsetR$, there is a bijection between ideals J such that $I \subset J \subset R$ and ideals in R/I.

Isomorphism Theorems for Modules :

Theorem 1 : If $\varphi : M \to N$ then $M/Ker\varphi \cong im\varphi$.

Theorem 2 : If $A, B \subset M$ then $\frac{A+B}{B} \cong \frac{A}{A\cap B}$.

Theorem 3 : If $A \subset B \subset M$ then $\frac{M/A}{B/A} \cong M/B$ (note that $J/I = j+I$).

Theorem 4 : Same as the fourth isomorphism theorem only for modules.

Submodules : Suppose M is a left R-module and N is a subgroup of M. Then N is a submodule (or R-submodule, to be more explicit) if, for any $n \in N$ and any $r \in R$, the product $rn \in N$.

Semi-Direct Product : If N and H are arbitrary groups (or more specifically $N, H < G$ where $N \triangleright G$) and $\phi : H \rightarrow Aut(N)$ is a homomorphism, $N \rtimes_\phi H$ (triangle points to normal side) $:= n \times H = \{nh : n \in N, h \in H\}$ (note that nh is an ordered pair and not a product!). These ordered pairs have the following product $(n_1 h_1) \cdot (n_2 h_2) := (n_1 \phi_{h_1}(n_2))(h_1 h_2)$. Semi-direct products have the following properties:
1) $N \rtimes H$ is indeed a group with $e_{N \rtimes H} = e_n e_h = e$.
2) $H < N \rtimes H$
3) $N \triangleright N \rtimes H$, $\frac{N \rtimes H}{N} \cong H$
4) $N \cap H = \{e\}$