# Math 113, Fall 2019
## Midterm 2 definitions, 11/19/2019

**Definition: Direct Product of Groups -**

$$G_1 \times G_2 \times \cdots G_i \times \cdots \times G_n$$

**Definition: Least Common Multiple (lcm) -**

Our familiar definition; for example: $\text{lcm}(12, 30) = 60$.

**Definition: Group Homomorphism -**

Let $\phi : A \to B$ be a homomorphism of groups (that is, $A, B$ are groups). Then

$$\phi(a * b) = \phi(a) *' \phi(b),$$

where $a, b \in A$ and $*, *'$ are the binary opertions on $A, B$, respectively.

**Definition: $\phi[A]$ -**

Image of $A$ under homomorphism $\phi : A \to B$, and $\phi[A] = \text{Im}(\phi) \subset B$.

**Definition: $\phi^{-1}[B]$ -**

Inverse image of $B$ under homomorphism $\phi$. If $\phi$ not one-to-one, this might be $\phi^{-1}[B] \subsetneq A$.

**Definition: Kernel of a Homomorphism -**

$$\{a \in A : \phi(a) = e'\},$$

where $\phi : A \to B$ and $e'$ is the identity in $B$.

**Definition: Normal Subgroup -**

From a theorem, we have three equivalent conditions for a normal subgroup. Let $N$ be a normal subgroup of group $G$. Then:
1) $gng^{-1} \in N, \forall_{g \in G}$
2) $gNg^{-1} = N, \forall_{g \in G}$ (often take this as definition)
3) $gN = Ng, \forall_{g \in G}$ (that is, all left and right cosets of $N$ coincide)

**Definition: Canonical Map -**

Let $\phi : G \to \phi[G]$ be a homomorphism of groups. Let $H := \ker(\phi)$ (this is a normal subgroup by property of the identity in codomain). Then there are two canonical maps. First, we have

$$\gamma : G \to G/H$$
$$\gamma(g) := gH,$$

which maps each element of $G$ to its coset modulo $H$. Also, we have the other canonical map

$$\mu : G/H \to \phi[G]$$
$$\mu(gH) := \phi(g).$$

**Definition: Automorphism -**

An automorphism is a self-map homomorphism $\phi : A \to A$.

**Definition: Inner Automorphism -**

An inner automorphism in a group is of the form

$$i_g(x) = gxg^{-1},$$

for a fixed $g \in G$ and all $x \in G$ and the automorphism $i_g : G \to G$.

**Definition: Action of $G$ on itself by conjugation -**

As defined in "inner automorphism" above.

**Definition: Factor/Quotient Group $(G/H)$ -**

Let $H$ be a normal subgroup of $G$ (or let $H$ be the kernel of a homomorphism of group $G$). Then the **quotient group** $G/H$ is defined via

$$(aH)(bH) := (ab)H,$$

for $a, b \in G$.

**Definition: Simple Group -**

A **simple group** is one that is **itself nontrivial** and **has no proper normal subgroups**.

**Definition: Center $Z(G)$ -**

The 'zentrum' or center of a group $G$ is the set

$$\{z \in G : zg = gz, \forall_{g \in G}\}.$$

**Definition: Commutator -**

A commutator of group $G$ is of the form $aba^{-1}b^{-1}$ for some $a, b \in G$.

**Definition: Commutator Subgroup -**

The commutator subgroup is the **subgroup generated by** the set of commutators in $G$:

$$\{aba^{-1}b^{-1} : a, b \in G\}.$$

**Definition: Group Action -**

Let $X$ be a set and $G$ be a group, and let $* : G \times X \to X$. A **group action** is one that satisfies the following:
1) $ex = x, \forall_{x \in X}$.
2) $(g_1 g_2)(x) = g_1(g_2(x)), \forall_{g_1, g_2 \in G, x \in X}$.

**Definition: $G$-set -**

Under the above definition of a group action, $X$ is a $G$ set if it satisfies those two properties for all $x \in X$.

**Definition: Faithful Action -**

A group action is **faithful** (or the group is faithful) if the only $g \in G$ with $gx = x$ is $e$.

**Definition: Transitive Action -**

A group action is **transitive** (or the group is transitive) if

$$\forall_{x_1, x_2 \in X} \exists_{g \in G} : g(x_1) = x_2.$$

**Definition: Isotropy Subgroup -**

The isotropy subgroup of group $G$ is the subgroup generated by the set

$$\{g : gx = x, \forall_{x \in X}\}.$$

**Definition: Ring -**

A ring is a set $\langle R, +, \cdot \rangle$ with the following axioms for $a, b, c \in R$:
R1) $\langle R, + \rangle$ is abelian (addition is commutative).
R2) $\cdot$ is associative.
R3) Left and right distributivity laws hold: $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$.

**Definition: Commutative Ring -**

A ring where multiplication $\cdot$ is commutative as well.

**Definition: Ring Homomorphism -**

Let $\phi : R \to R'$ be a morphism between rings $R, R'$. Then $\phi$ is a ring homomorphism if we have the following (2) properties for $a, b \in R$:
1) $\phi(a+b) = \phi(a) + \phi(b)$ .
2) $\phi(ab) = \phi(a)\phi(b)$.

**Definition: Ring Isomorphism -**

A ring homomorphism where $\phi$ is bijective.

**Definition: $\mathbb{Z}_n$ -**

This is $\mathbb{Z}_n := \langle \mathbb{Z}_n, +, \cdot \rangle = \{0, 1, 2, \ldots, n-1\}$.

**Definition: Unity, Ring With Unity Element, Ring With Unity Element 1, Ring With Unity Element $1 \neq 0$ -**

The unity element of a ring is the **unique multiplicative identity**. By convention, in a ring we call this 1 and save 0 to denote the additive identity. It may happen that the multiplicative and additive identity are the same, in which case we have $1 = 0$. However, we often want $1 \neq 0$ and specify as such.

**Definition: Multiplicative Inverse -**

Let $a$ be an element in ring $R$ with unity 1. Then $a^{-1}$ is a multiplicative inverse of $a$ if $aa^{-1} = a^{-1}a = 1$.

**Definition: Unit -**

Let $a, b \in R$ with unity 1. Then $a, b$ are units of ring $R$ if $ab = ba = 1$.

**Definition: Group of Units -**

Collection of units of a ring with unity.

**Definition: Division Ring (Skew Field), Field -**

A **division ring** is a ring with unity where all elements are units (have multiplicative inverses). If this division ring is commutative, we call this a **field**.

**Definition: Direct Product of Rings -**

Simply $R_1 \times R_2 \times \cdots \times R_i \times \cdots \times R_n$, where all $R_i$ are rings. We have that the direct product is commutative or has unity if and only if all of the $R_i$ are commutative or have unity, respectively.

**Definition: Subring, Subfield -**

A subring is a subset of ring $\langle R \rangle$ under the induced operations of the enclosing ring $R$. We define a subfield similarly.

**Definition: Zero Divisor -**

Let $a, b$ be **nonzero** elements of ring $R$ with additive identity 0. If $ab = 0$ (not necessarily in both ways), then $a, b$ are zero divisors.

**Definition: Ring with No Zero Divisors -**

A ring has no zero divisors **if and only if** (multiplicative) cancellation laws hold.

**Definition: Integral Domain -**

An integral domain is a commutative ring **with unity** $1 \neq 0$ with no zero divisors.

**Definition: Integral Subdomain -**

A subdomain of $\langle R, +, \cdot \rangle$ is a **subset** $S$ of $R$ such that $\langle S, +_S, \cdot_S \rangle$ is an integral domain.

**Definition: Characteristic of a Ring -**

For $n$ summands $a+a+\cdots+a$, we write this as $n \cdot a$, keeping the dot because $n$ might not be an element of $R$. If there exists some $n$ for which $n \cdot a = 0$ for all $a \in R$, then the least such $n$ is the characteristic of the ring. If no such $n$ exists, by convention we take the characteristic of the ring to be 0.

**Definition: Euler's totient function $\varphi(n)$ -**

We assume this to denote Euler's totient function, where $\varphi(n)$ denotes the number of positive integers $k$ less than or equal to $n$ where $\gcd(k, n) = 1$ (number of lesser positive integers relatively prime to $n$).
We use this in Euler's generalization of Fermat's little theorem, where Euler's generalization gives

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where $\varphi(p) = p - 1$ when $p$ is prime. Also, the number of nonzero elements of $\mathbb{Z}_n$ that are **not zero-divisors** is given by $\varphi(n)$.

The set $G_n$ of nonzero elements of $\mathbb{Z}_n$ that are not zero-divisors forms a group under multiplication, modulo $n$.

This theorem is the basis behind Euler's generalization.

**Definition: Field of Quotients -**

Every integral domain $D$ can be **enlarged to** a field $F$ where every element of $F$ can be expressed as a **quotient** of two elements in $D$.

We call this field $F$ a **field of quotients** of $D$.

**Definition: Polynomial -**

For our purposes, we define a polynomial $f(x) \in F[x]$ to be the linear combination of $a_i \in F$ and indeterminate $x$, given by

$$\sum_{i=0}^{\infty} a_i x^i,$$

where $a_i = 0$ for all $i > n$ where $n$ is the "degree" of the polynomial. Hence a polynomial has a finite number of nonzero terms.

**Definition: $R[x]$ -**

We define $R[x]$ as the set of all "polynomials in $x$" with coefficients in the ring $R$. If $R$ is commutative, then so is $R[x]$; if $R$ has unity $1 \neq 0$, then 1 is also unity for $R[x]$.

**Definition: Evaluation Homomorphism $\phi_\alpha(f)$ -**

This is a very formal definition but probably important for field theory.

Let $F$ be a subfield of a field $E$, let $\alpha \in E$, and let $x$ be an indeterminate. The map

$$\phi_\alpha : F[x] \to E$$
$$\phi_\alpha(a_0 + a_1 x + \cdots + a_n x^n) := a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

for $(a_0 + a_1 x + \cdots + a_n x^n) \in F[x]$ is a **homomorphism of $F[x]$ into $E$.** The homomorphism $\phi_\alpha$ is **evaluation at $\alpha$.**

When in doubt, probably take the definition simply as evaluation at $\alpha$.

**Definition: Zero of a polynomial -**

Let $f(x) := a_0 + a_1 x + \cdots + a_n x^n \in F[x]$ and let $\phi_\alpha : F[x] \to E$ be an evaluation homomorphism, where $F$ is a subfield of field $E$. Define

$$f(\alpha) := \phi_\alpha(f(x)) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

so that if $f(\alpha) = 0$, then $\alpha$ is a **zero of the polynomial** $f(x)$.

**Definition: Degree of a polynomial -**

We defined $f(x) := a_0 + a_1 x + \cdots + a_n x^n$. The degree is $n$ (guaranteed to be finite). Now if $f(x) = 0$, the zero polynomial, the degree is undefined, but sometimes defined as $-1$ or $-\infty$ (where the latter makes it so the product of a zero polynomial with another gives the sum of each polynomial's degree).

**Definition: Irreducible over $F$, Reducible Polynomials -**

A nonconstant polynomial $f(x) \in F[x]$ is **irreducible over** $F$ (or an irreducible polynomial in $F[x]$) if $f(x)$ cannot be expressed as a product $g(x)h(x)$ where $g(x), h(x)$ have lesser degree than $f(x)$. If $f(x)$ is not irreducible over $F$, then it is reducible over $F$.

**Definition: Kernel of a Ring Homomorphism -**

Let $\phi : R \to R'$ be a homomorphism of rings. Then we define the kernel as

$$\ker(\phi) := \{a \in R : \phi(a) = 0'\},$$

where $0'$ is the additive identity in the target $R'$. We equivalently write $\ker(\phi) = \phi^{-1}[0']$.

Now this $\ker(\phi)$ is the same as the kernel of the group homomorphism of $\langle R, + \rangle$ into $\langle R', + \rangle$, given by $\phi$.

**Definition: Ideal -**

An ideal of a ring is **the additive subgroup** $N$ of ring $R$ with

$$aN \subseteq N, \quad Nb \subseteq N, \quad \forall_{a,b \in R}.$$

Now this is analogous to the definition of a Normal subgroup (which allowed us to form a factor group). Notice that the Kernel of a ring homomorphism is an ideal, just as the Kernel of a group homomorphism is a normal subgroup.

**Definition: Prime Ideal -**

An ideal $N \neq R$ in a commutative ring $R$ is a **prime ideal** if $ab \in N$ implies EITHER $a \in N$ OR $b \in N$, for all $a, b \in R$.

For the following, we only care for the "Ideal Structure in $F[x]$"; however, the definitions will be general for commutative rings. But assume $F$ is a field.

**Definition: Principal Ideal -**

Let $R$ be a commutative ring with unity and take $a \in R$. Then the principal ideal generated by $a$ is:

$$\langle a \rangle := \{ra \mid r \in R\},$$

which is the ideal of all multiples of $a$. Alternatively, $N$ is a principal ideal of $R$ if $N = \langle a \rangle$ for some $a \in R$.

**Definition: Factor (Quotient) Ring -**

Let $N$ be an ideal of ring $R$. Then the additive cosets of $N$ form a **factor (quotient) ring** $R/N$ (**of** $R$ **by** $N$) with the binary operations defined for $a, b \in R$ as:

$$(a+N)+(b+N)=(a+b)+N$$
$$(a+N)(b+N)=ab+N.$$

**Definition: Canonical Map $R \to R/N$ -**

Let $N$ be an ideal of $R$. This gives rise to the canonical map

$$\gamma : R \to R/N$$
$$\gamma(x) := x+N,$$

where $\gamma$ is a ring homomorphism with kernel $N$.

Then this gives rise to another canonical map $\mu : R/N \to \phi[R]$ given by $\mu(x+N) := \phi(x)$ so that

$$\phi(x) + \mu\gamma(x).$$