MA 294: Applied Abstract Algebra / Spring 2022
Definitions you should know

Definitions from before the midterm

- Let S, T be sets. A function $f : S \to T$ is *injective* if for any $a, b \in S$ if $f(a) = f(b)$, then $a = b$.
- Let S, T be sets. A function $f : S \to T$ is *surjective* if for any $t \in T$ there exists $s \in S$ so that $f(s) = t$.
- Let S, T be sets. A function $f : S \to T$ is *bijective* if f is both injective and surjective.
- Let S be a set. A relation $\sim$ on S is *reflexive* if for all $a \in S$ we have $a \sim a$.
- Let S be a set. A relation $\sim$ on S is *symmetric* if for all $a, b \in S$, if $a \sim b$ then $b \sim a$.
- Let S be a set. A relation $\sim$ on S is *transitive* if for all $a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$.
- Let S be a set. A relation $\sim$ on S is an *equivalence relation* if $\sim$ is reflexive, symmetric, and transitive.
- Let G be a set with a binary operation $* : G \times G \to G$. Then $*$ is *associative* if for all $a, b, c \in G$ we have $(a * b) * c = a * (b * c)$.
- Let G be a set with a binary operation $* : G \times G \to G$. The elements a and b of G *commute* if $a * b = b * a$. The operation $*$ is *commutative* if for all $a, b \in G$ we have $a * b = b * a$.
- Let G be a set with a binary operation $* : G \times G \to G$. An element $e \in G$ is an *identity* element for $*$ if for all $g \in G$ we have $e * g = g * e = g$.
- Let G be a set with an associative binary operation $* : G \times G \to G$ that has an identity element $e \in G$. An element $g \in G$ is *invertible* if there exists $g' \in G$ such that $g * g' = g' * g = e$. The element g' is then the *inverse* of g.
- A set G with a binary operation $* : G \times G \to G$ (G1) is a *group* if $*$ is associative (G2), if G has an identity element for $*$ (G3), and every element of G has an inverse in G (G4).
- The *order* of a group G is the number of elements in G, if this is finite; otherwise the *order* of G is *infinite*.
- A group G under the binary operation $*$ is an *abelian group* if $*$ is a commutative operation.
- Let G be a group and $a \in G$. The *order* of a is the least positive integer n so that $a^n = 1$, if such an integer exists; otherwise the *order* of a is *infinite*.

- A group G is *cyclic* if there is an element $a \in G$ so that every element of G is an integer power of a. In this case, a is a *generator* of G.
- If G is a group and $a \in G$, then the *cyclic subgroup of* G *generated by* a, denoted $\langle a \rangle$, is the set of all integer powers of a.
- Let G be a group. A subset $H \subset G$ is said to be a *subgroup*, written $H \leq G$, if H is a group in its own right with the operation from G. In other words, H is a subgroup if H is nonempty, closed under the group operation (S1) and closed under inversion (S2).
- Let G be a group and $H \leq G$ be a subgroup. The *left coset of* H *in* G spanned by an element $g \in G$ is the subset $gH = \{gh : h \in H\}$ of G.
- Let G be a group and $H \leq G$ be a subgroup. The *right coset of* H *in* G spanned by an element $g \in G$ is the subset $Hg = \{hg : h \in H\}$ of G.
- Let G be a group and $H \leq G$ a subgroup. The *index* of H in G, denoted $[G : H]$, is the number of distinct left cosets of H in G.

Definitions from the second half of the course[1]

- Let G and H be groups. A map $f : G \to H$ is an *isomorphism* if f is bijective and $f(ab) = f(a)f(b)$ for every $a, b \in G$.
- Groups G and H are *isomorphic* if there exists an isomorphism $f : G \to H$.
- A *permutation* of a set X is a bijective function $\sigma : X \to X$.
- The *symmetric group (on n letters)* is the group of all permutations of the set $\{1, \dots, n\}$.
- If σ is a permutation of a finite set X and $k \geq 2$, then σ is a *k-cycle* if there are k distinct elements $x_1, x_2, \dots, x_k$ of X with $\sigma(x_1) = x_2$, ..., $\sigma(x_{n-1}) = x_n$, and $\sigma(x_n) = x_1$; and for every $x \in X$ with $x \notin \{x_1, \dots, x_k\}$ we have $\sigma(x) = x$.
- A permutation σ of a finite set X is a *transposition* if σ is a 2-cycle.
- A permutation σ of a finite nonempty set X is *even* if σ can be expressed as a product of an even number of transpositions.
- A permutation σ of a finite nonempty set X is *odd* if σ can be expressed as a product of an odd number of transpositions.
- The *sign* of a permutation σ of a finite nonempty set X is 1 if σ is even and -1 if σ is odd.

[1] The notion of isomorphism is from the first half the course but was left off the original list by mistake.

- The *alternating group (on n letters)* is the group of all even permutations of the set $\{1, \ldots, n\}$.
- A set of permutations of a set X that is a group under composition of permutations is a *group of permutations of* X.
- If G is a group of permutations of a set X, and $x \in X$, then the *orbit* of x is the subset $\{gx : g \in G\}$ of X.
- If G is a group of permutations of a set X, then $g \in G$ *fixes* $x \in X$ if $gx = x$.
- If G is a group of permutations of a set X, and $x \in X$, then the *stabilizer* of x is the set of elements of G that fix x.
- A *ring* R is a set with two binary operations $+$ and $\times$ satisfying the following: $(R, +)$ is an abelian group with identity element 0 (R1), $\times$ is an associative binary operation on R with identity element 1 (R2), and $\times$ *distributes over* $+$ in the sense that for all $a, b, c \in R$ we have $a \times (b+c) = (a \times b) + (a \times c)$ and $(a+b) \times c = (a \times c) + (b \times c)$ (R3).
- A *commutative ring* is a ring R in which the binary operation $\times$ is commutative.
- An element x of a ring R is *invertible* if x has a multiplicative inverse (that is, if there exists $y \in R$ so that $xy = yx = 1$).
- A *field* is a commutative ring that has at least two elements and where every nonzero element is invertible. (Equivalently, a field is a commutative ring R so that the set of invertible elements $U(R)$ is precisely the same as the set of nonzero elements $R - \{0\}$.
- The *additive group* of a field F is the group $(F, +)$.
- The *multiplicative group* of a field F is the group $(F - \{0\}, \times)$.

Now let R be a ring and $R[x]$ the algebra of all polynomials with coefficients in R.

- The *coefficients* of a polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ in $R[x]$ is the elements $a_0, a_1, \ldots, a_n$ of R.
- The *degree* of a nonzero polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in R[x]$ is the maximal index $n \geq 0$ so that $a_n \neq 0$.
- A *constant* polynomial in $R[x]$ is an element of R viewed as an element of $R[x]$. In other words, a constant polynomial is either the zero polynomial or a polynomial of degree 0.
- The *leading coefficient* of a polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ of degree n in $R[x]$ is the coefficient a_n.
- A nonzero polynomial in $R[x]$ is *monic* if its leading coefficient is 1.

Now let F be a field.

- If $a(x)$ and $b(x)$ are polynomials in $F[x]$, then $a(x)$ is a *divisor* (or *factor*) of $b(x)$ if there exists a polynomial $c(x) \in F[x]$ with $a(x)c(x) = b(x)$.
- If $a(x)$ and $b(x)$ are polynomials in $F[x]$, then $c(x) \in F[x]$ is a *common divisor* of $a(x)$ and $b(x)$ if $c(x)$ divides both $a(x)$ and $b(x)$.
- If $a(x), b(x) \in F[x]$ are nonzero then a *greatest common divisor* (or *gcd*) of $a(x)$ and $b(x)$ is a common divisor of $a(x)$ and $b(x)$ of maximal degree.
- If $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n$ then the *evaluation* of $f(x)$ at an element $\alpha \in F$ is the element $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$ of F.
- If $f(x)$ is in $F[x]$, then an element $\alpha \in F$ is a *root* of F if $f(\alpha) = 0$.
- A polynomial $f(x)$ in $F[x]$ is *irreducible* if it is not constant and in every factorization $f(x) = a(x)b(x)$ either $a(x)$ or $b(x)$ is constant.
- For a finite field F, a *primitive element* of F is a generator of the cyclic group $U(F)$.