Math 412 - Introduction to Abstract Algebra

Midterm 2 Review Sheet - You must know definitions!

Theorem 4.2: If R is an integral domain and $f(x), g(x) \in R[x]$ are nonzero, then

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

Corollary 4.3: If R is an integral domain, then $R[x]$ is an integral domain.

Corollary 4.4: If R is a ring and $f(x), g(x), f(x)g(x) \in R[x]$ are nonzero, then

$$\deg f(x)g(x) \leq \deg f(x) + \deg g(x).$$

Corollary 4.5: Let R be an integral domain and $f \in R[x]$. The polynomial $f(x)$ is a unit iff $f(x)$ is a constant polynomial that is a unit in R.

Theorem 4.6: (The Division Algorithm) Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x)$ such that

$$f(x) = g(x)q(x) + r(x) \text{ and either } r(x) = 0 \text{ or } \deg r(x) < \deg g(x).$$

Theorem 4.7: Let F be a field with $a(x), b(x) \in F[x]$ with $b(x) \neq 0$. If $b(x)|a(x)$, then $cb(x)|a(x)$ for each nonzero $c \in R$.

Theorem 4.8: Let F be a field with $a(x), b(x) \in F[x]$ not both zero. Then there is a unique gcd $d(x)$ of $a(x)$ and $b(x)$. Moreover, there exist polynomials $u(x), v(x)$ such that

$$d(x) = a(x)u(x) + b(x)v(x).$$

Theorem 4.10: Let F be a field and $a(x), b(x), c(x) \in F[x]$. If $a(x)|b(x)c(x)$ and $a(x)$ and $b(x)$ are relatively prime, then $a(x)|c(x)$.

Theorem 4.11: A nonzero polynomial is reducible in $F[x]$ iff it can be written as the product of two polynomials of lower degree.

Theorem 4.12: Let $p(x) \in F[x]$ be nonconstant. TFAE:

1. $p(x)$ is irreducible.
2. If $b(x)$ and $c(x)$ are any polynomials such that $p(x)|b(x)c(x)$, then $p(x)|b(x)$ or $p(x)|c(x)$.
3. If $r(x)$ and $s(x)$ are any polynomials such that $p(x) = r(x)s(x)$, then $r(x)$ or $s(x)$ is a nonzero constant polynomial.

Theorem 4.14: Polynomials in $F[x]$ factor uniquely up to reordering and multiplication by units.

Theorem 4.15: (The Remainder Theorem) The remainder when a polynomial $f(x) \in F[x]$ is divided by $(x - a)$ equals $f(a)$.

Theorem 4.16: (The Factor Theorem) An element $a \in F$ is a root of $f(x) \in F[x]$ iff $(x - a)$ is a factor of $f(x)$ in $f[x]$.

Theorem 4.21: (Rational Root Test) If the rational number $r/s \neq 0$ is a root of $f(x) = a_n x^n + \cdots a_1 x + a_0 \in \mathbb{Z}[x]$, then $r|a_0$ and $s|a_n$.

Theorem 4.24: (Eisenstein's Criterion) If $f(x) = a_n x^n + \cdots a_1 x + a_0 \in \mathbb{Z}[x]$ and a prime p divides each of $a_0, a_1, \ldots, a_n - 1$, but p does not divide a_n and p^2 does not divide a_0, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Theorem 4.26: (The Fundamental Theorem of Algebra) Every nonconstant polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$.

Theorem 5.1: The relation of congruence modulo a nonzero $p(x) \in F[x]$ is an equivalence relation.

Theorem 5.2: For a nonzero $p(x) \in F[x]$, if $f(x) \equiv g(x) \mod p(x)$ and $h(x) \equiv k(x) \mod p(x)$, then $f(x) + h(x) \equiv g(x) + k(x) \mod p(x)$ and $f(x)h(x) \equiv g(x)k(x) \mod p(x)$.

Theorem 5.3: The congruence $f(x) \equiv g(x) \mod p(x)$ holds iff $[f(x)] = [g(x)] \in F[x]/p(x)$.

Theorem 5.6: For nonconstant $p(x) \in F[x]$, if $[f(x)] = [g(x)]$ and $[h(x)] = [k(x)]$ in $F[x]/p(x)$, then $[f(x)+h(x)] = [g(x)+k(x)]$ and $[f(x)h(x)] = [g(x)k(x)]$.

Theorem 5.7: For nonconstant $p(x) \in F[x]$, the set $F[x]/p(x)$ is a commutative ring with 1. Moreover, the ring $F[x]/p(x)$ contains a subring isomorphic to F.

Theorem 5.9: For nonconstant $p(x) \in F[x]$, if $f(x) \in F[x]$ is relatively prime to $p(x)$, then $[f(x)]$ is a unit in $F[x]/p(x)$.

Theorem 5.10: For nonconstant $p(x) \in F[x]$, TFAE:

1. $p(x)$ is irreducible in $f[x]$
2. $F[x]/p(x)$ is a field
3. $F[x]/p(x)$ is an integral domain.

Theorem 5.11: If $p(x)$ is irreducible in $F[x]$, then $F[x]/p(x)$ is a field extension of F that contains a root of $p(x)$.