Algebra Theorems

On Rings, Polynomials, and Fields

1 Section 16.2 - Integral Domains and Fields

1. **Prop. 16.15. Cancellation Law.** Let D be a commutative ring with identity. Then D is an integral domain iff for all nonzero elements $a \in D$ with $ab = ac$, we have $b = c$.
2. **Theorem 16.16.** Every finite integral domain is a field.
3. **Lemma 16.18.** Let R be a ring with identity. If 1 has order n, then the characteristic of R is n.
4. **Theorem 16.19.** The characteristic of an integral domain is either prime or zero.

2 Section 16.3 - Ring Homomorphisms and Ideals

1. **Prop. 16.22.** Let $\phi : R \to S$ be a ring homomorphism. Then:
   (a) If R is a commutative ring, then $\phi(R)$ is a commutative ring.
   (b) $\phi(0) = 0$.
   (c) Let 1_R and 1_S be the identities for R and S, respectively. If ϕ is onto, then $\phi(1_R) = 1_S$.
   (d) If R is a field and $\phi(R) \neq \{0\}$, then $\phi(R)$ is a field.
2. **Theorem 16.25.** Every ideal in the ring of integers $\mathbb{Z}$ is a principal ideal.
3. **Prop. 16.27.** The kernel of any ring homomorphism $\phi : R \to S$ is an ideal in R.

3 Section 17.1 - Polynomial Rings

1. **Theorem 17.3.** Let R be a commutative ring with identity. Then $R[x]$ is a commutative ring with identity.

2. **Prop. 17.4.** Let $p(x), q(x) \in R[x]$, where R is an integral domain. Then $\deg p(x) + \deg q(x) = \deg(pq(x))$. Furthermore, $R[x]$ is an integral domain.

3. **Theorem 17.5.** Let R be a commutative ring with identity and $\alpha \in R$. Then we have a ring homomorphism $\phi_\alpha : R[x] \to R$ defined by $\phi_\alpha(p(x)) = p(\alpha) = a_n\alpha^n + \cdots + a_0$, where $p(x) = a_n x^n + \cdots + a_0$.

4 Section 17.2 - The Division Algorithm

1. **Theorem (Division Algorithm).** Let $f(x), g(x)$ be polynomials in $F[x]$, where F is a field and $g(x)$ is a nonzero polynomial. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$, where either $\deg r(x) < \deg g(x)$ or $r(x)$ is the zero polynomial.

2. **Cor. 17.8.** Let F be a field. An element $\alpha \in F$ is a zero of $p(x) \in F[x]$ iff $x - \alpha$ is a factor of $p(x) \in F[x]$.

3. **Cor. 17.9.** Let F be a field. A nonzero polynomial $p(x)$ of degree n in $F[x]$ can have at most n distinct zeros in F.

4. **Prop. 17.10.** Let F be a field and suppose $d(x) = \gcd(p(x), q(x))$ with $p(x), q(x) \in F[x]$. Then there exists polynomials $r(x), s(x)$ such that $d(x) = r(x)p(x) + s(x)q(x)$. Furthermore, $\gcd(p(x), q(x))$ is unique.

5 Section 17.3 - Irreducible Polynomials

1. **Lemma 17.13.** Let $p(x) \in \mathbb{Q}[x]$. Then $p(x) = \frac{r}{s}(a_0 + \cdots + a_n x^n)$, where $r, s, a_0, \ldots, a_n \in \mathbb{Z}$, $a_i's$ are relatively prime, and r, s relatively prime.

2. **Theorem 17.14. (Gauss's Lemma).** Let $p(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $p(x)$ factors into a product of two polynomials $\alpha(x), \beta(x) \in \mathbb{Q}[x]$, where $\deg \alpha(x), \deg \beta(x) < \deg p(x)$. Then $p(x) = a(x)b(x)$, where $a(x), b(x)$ are monic polynomials in $\mathbb{Z}[x]$, with $\deg a(x) = \deg \alpha(x)$ and $\deg b(x) = \deg \beta(x)$.