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 $\deg b(x) = \deg \beta(x)$.

3. **Cor. 17.15.** Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with coefficients in $\mathbb{Z}$ and $a_0 \neq 0$. If $p(x)$ has a zero in $\mathbb{Q}$, then $p(x)$ also has a zero α in $\mathbb{Z}$. Furthermore, $\alpha \mid a_0$.

4. **Theorem 17.17. (Eisenstein's Criterion).** Let p be prime and let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. If $p \mid a_i$ for $i = 0, 1, \ldots, n-1$ but $p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

6 Section 3.1 - Integer Equivalence Classes & Symmetries

N/A.

7 Section 3.2 - Definitions & Examples

1. **Prop. 3.17.** The identity element in a group G is unique; that is, there exists only one element $e \in G$ such that $eg = ge = g$ for all $g \in G$.

2. **Prop. 3.18.** If $g \in G$, where G is a group, then g^{-1} (the inverse of g) is unique.

3. **Prop. 3.19.** Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

4. **Prop. 3.20.** Let G be a group. For any $a \in G$, $(a^{-1})^{-1} = a$.

5. **Prop. 3.21.** Let G be a group and $a, b \in G$. Then, the equation $ax = b$ and $xa = b$ have unique solutions in G.

6. **Prop. 3.22. (Right & Left Cancellation Laws).** If G is a group and $a, b, c \in G$, then $ba = ca$ implies and $b = c$ and $ab = ac$ implies $b = c$.

7. **Theorem 3.23.** In a group, the usual laws of exponents hold; that is, for all $g, h \in G$, we have:

   (a) $g^m g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$.

   (b) $(g^m)^n = g^{mn}$ for all $m, n \in \mathbb{Z}$.

   (c) $(gh)^n = (h^{-1}g^{-1})^{-n}$ for all $n \in \mathbb{Z}$. Furthermore, if G abelian, then $(gh)^n = g^n h^n$.

8. **Cor. 3.23.** Let the group be $\mathbb{Z}$ or $\mathbb{Z}_n$. Then, suppose we write the group operation additively and the exponential operation multiplicatively; that is, write ng instead of g^n. The laws of exponents (as in Theorem 3.23) now become:

   (a) $mg + ng = (m+n)g$ for all $m, n \in \mathbb{Z}$.

   (b) $n(mg) = (mn)g$ for all $m, n \in \mathbb{Z}$.

   (c) $m(g+h) = mg + mh$ for all $m \in \mathbb{Z}$.

8 Section 3.3 - Subgroups

1. **Prop. 3.30.** A subset H of G is a subgroup iff it satisfies the following conditions:

   (a) The identity e of G is in H.

   (b) If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.

   (c) If $h \in H$, then $h^{-1} \in H$.

2. Let H be a subset of a group G. Then H is a subgroup of G iff $H \neq \emptyset$ and $g, h \in H$ implies $gh^{-1} \in H$.

9 Section 4.1 - Cyclic Subgroups

1. **Theorem 4.3.** Let G be a group and $a \in G$. Then, the set $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G that contains a.

2. **Theorem 4.9.** Every cyclic group is abelian.

3. **Cor. 4.11.** The subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.

4. **Prop. 4.12.** Let G be a cyclic group of order n and suppose a is a generator for G. Then $a^k = e$ iff $n \mid k$.

5. **Theorem 4.13.** Let G be a cyclic group of order n and suppose $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is n/d, where $d = \gcd(k, n)$.

6. **Cor. 4.14.** The generators of $\mathbb{Z}_n$ are the integers r such that $1 \leq r < n$ and $\gcd(r, n) = 1$.

10 Section 4.2 - Multiplicative Group of Complex Numbers

1. **Prop. 4.24.** The circle group is a subgroup of $\mathbb{C}^\star$.

2. **Theorem 4.25.** The n^{th} roots of unity form a cyclic subgroup of $\mathbb{T}$.

11 Section 5.1 - Definitions & Notation (Permutation Groups)

1. **Theorem 5.1.** The symmetric group on n letters, S_n, is a group with $n!$ elements, where the binary operations is the composition of maps.