Subring Test

A nonempty subset S of a ring R is a subring of R iff for all $a, b \in S$ we have

$$a - b \in S \qquad ab \in S$$

Zero Divisors and Integral Domains

If $ab = 0$ with a, b nonzero, then a, b are called zero divisors. If a ring is commutative with unity, and has no zero divisors, the ring is an integral domain.

Subdomain Test

A nonempty subset S of an integral domain D is a subdomain of D iff S is a subring of D, and $1 \in S$ is also the unity in D.

Units and Fields

If an element in a ring with unity has a multiplicative inverse, it is called a unit. If on a commutative ring with one, all nonzero elements are units, then the ring is a field.

Note that being a unit implies it is not a zero divisor.

Units as a Cyclic Subgroup

The set of all units $R^\times$ over a ring R is a cyclic subgroup of R under multiplication.

Finite Integral Domains

Finite integral domains are fields. $\mathbb{Z}_p$ is a field iff p is prime.

Subfield Test

A nonempty subset S of a field F is a field under the same 2 operations as F iff for all $a, b \in S$ we have

$$a - b \in S \qquad ab^{-1} \in S \quad \forall b \neq 0$$

Characteristics

The characteristic of R, denoted $\operatorname{ch} R$, is the least positive integer n s.t. $n \cdot a = 0$ for all $a \in \mathbb{R}$. If no such n exists, we say $\operatorname{ch} R = 0$.

Note $\operatorname{ch} \mathbb{Z}_n = n$. If D an integral domain, then $\operatorname{ch} D$ either 0 or a p prime.

Ring Homomorphisms and Kernels

A map $\phi : R \to R'$ is a ring hom if $\forall a, b \in R$ we have

$$\phi(a+b) = \phi(a) + \phi(b) \qquad \phi(ab) = \phi(a)\phi(b)$$

the kernel of a ring hom ϕ is the set of element that gets mapped to 0 under ϕ. It has following properties

- $\phi(0) = 0$
- $\phi(-a) = -\phi(a)$
- $\phi(n \cdot a) = n \cdot \phi(a)$ where $\cdot$ is the scalar multiple by an integer
- ϕ is one to one iff $\ker \phi = \{0\}$
- $\phi(a^n) = \phi(a)^n$ where the power is a scalar multiple of products
- if A a subring of R, then $\phi(A)$ is a subring of $\phi(R)$
- $\phi(1)$ is the unity in $\phi(R)$
- R commutative implies $\phi(R)$ commutative

Ring Isomorphisms

If ring hom one to one and onto, then it is ring iso. Commutative rings, integral domains and fields transfer under a ring iso.

Ideals

I is an ideal in R if I is a subring of R, and $xr, rx \in I$ for all $r \in R$, $x \in I$. The kernel of any ring hom is an ideal in its domain.

Ideals and Fields

Let R comm ring with identity. Then R a field iff the only ideals in R are $\{0\}$, the trivial ideal, and R, the improper ideal.

Ideals and Cosets

Let I subring of R. Then I an ideal in R iff $(a+I)(b+I) = (ab+I)$ is a well-defined operations on the cosets of I in R.

Quotient Rings and Operations on Cosets

R/I, the quotient ring, is a ring under the operations defined by

$$(a+I)+(b+I)=(a+b)+I \qquad (a+I)(b+I)=ab+I$$

for all $a+I, b+I \in R/I$.

First Isomorphism Theorem

Let ϕ a ring hom. Then $R/\ker\phi \cong \phi(R)$. For any ideal I in R, there is an onto ring hom $\phi : R \to R/I$ with $\ker\phi = I$. Read 7.2.19, 7.2.20.

Prime Ideals

A nontrivial proper ideal $I \neq R$ in a commutative ring R is called a prime ideal if $ab \in I$ implies $a \in I$ or $b \in I$ for all $a, b \in R$.

Maximal Ideals

A nontrivial proper ideal $I \neq R$ in a ring R is called a maximal ideal if there are no other ideals between I and R.

Ideals and Types of Rings

- I is a prime ideal in R iff R/I an integral domain.
- I is a maximal ideal in R iff R/I a field.

Consequently, maximal ideal implies prime ideal.

Field of Quotients / Field of Fractions

Let D be an integral domain. Then there exists a field F consisting of quotients a/b, where $a, b \in D$ and $b \neq 0$. F is called the field of fractions of D.

The field of fractions F of an integral domain D is the smallest field containing D. Any two fields of fractions of an integral domain D are isomorphic.

Subdomains and Isomorphism with Old Friends

Let D be an integral domain. Then there exists a subdomain $D' \subseteq D$ s.t.

1. if $\operatorname{ch} D = 0$, then $\mathbb{Z} \cong D' \subseteq D$
2. if $\operatorname{ch} D = p$, then $\mathbb{Z}_p \cong D' \subseteq D$

Sunfields and Isomorphism with Old Friends

Let F be a field. Then there exists a subfield $F' \subseteq F$ s.t.

1. if $\operatorname{ch} F = 0$, then $\mathbb{Q} \cong F' \subseteq F$
2. if $\operatorname{ch} F = p$, then $\mathbb{Z}_p \cong F' \subseteq F$

Rings and Polynomial Rings

A polynomial ring $R[x]$ of R is a ring containing R and all the finite degreed polynomials with coefficients in R. The following is true,

- $R[x]$ is a ring containing the ring R as a subring
- R commutative implies $R[x]$ commutative
- R shares unity 1 with $R[x]$
- R shares characteristic with $R[x]$
- D integral domain implies $D[x]$ integral domain. Moreover, the units in $D[x]$ are the same as the units in D, and any $f, g \in R[x]$ has $\deg fg = \deg f + \deg g$
- F a field, then $F[x]$ is an integral domain, but not a field

Division Algorithm on Polynomial Rings

Let F be a field, and $f, g \in F[x]$, with $g \neq 0$. Then there are unique $q, r \in F[x]$ s.t.

- $f = qg + r$
- $r = 0$ or $\deg r < \deg g$

if there is q s.t. $f = qg$, then $g \mid f$, read as g divides f, and f is a multiple of g.

Greatest Common Divisors of Two Polynomials

Let F a field, $f, g \in F[x]$ not both 0. Then there is a GCD d s.t. there is $u, v \in F[x]$ s.t.

$$d = uf + vg$$

The GCD we are interested in, denoted $\gcd(f, g)$, is the monic d.

Factor Theorem and Reminder Theorem

Let $f \in F[x]$ with F field. $f(a) = 0$ iff $(x - a)$ divides f. More generally, $f(a)$ is the remainder on dividing f by $(x - a)$.

Finite Roots of a Polynomial

Let $f \in F[x]$ where F a field. Then f has at most $\deg f$ number of roots in F.

Conjugates as Roots

Let $f \in \mathbb{Q}[x]$. If $a + b\sqrt{c}$ a root of f, where $a, b \in \mathbb{Q}$ and $\sqrt{c} \notin \mathbb{Q}$, then $a - b\sqrt{c}$ also a root of f.

Irreducible Polynomials

Let F be a field and f a nonconst poly in $F[x]$. We say f is irred over f if there are no $g, h \in F[x]$ with degree of both g, h lower than f.

If f irred and $f \mid gh$, then $f \mid g$ or $f \mid h$.

Unique Factorization Theorem

Let F be a field and f a nonconstant polynomial. Then we can write

$$f = up_1p_2 \cdots$$

where u nonzero and p_i irred polys. This is unique up to reordering.

Reducibility and Linear Factors

Let F a field and $f \in F[x]$. If f degree 2 or 3, then f reducible over F iff f has a root in F.

Rational Roots Theorem

Let $f \in \mathbb{Z}[x]$. Let $a = r/s$ a root of f in $\mathbb{Q}$, where r, s coprime. Then $r \mid a_0$ and $s \mid a_n$ in $\mathbb{Z}$.

Contents, Primitive Polynomials and Gauss' Lemma

In $\mathbb{Z}[x]$, the GCD of all coefficients of a polynomial is its content. If the GCD is one, the polynomial is primitive. The product of primitive polynomials is primitive. Moreover, it factors into two polys of degrees r, s in $\mathbb{Q}[x]$ iff it factors into polys of the same degrees in $\mathbb{Z}[x]$.

Eisenstein's Criterion

Let $f \in \mathbb{Z}[x]$. Then if there is prime p s.t.

- $p \nmid a_n$
- $p \mid a_i$ for all $i < n$

- $p^2 \nmid a_0$

then f irred over $\mathbb{Q}$.

Cyclotomic Polynomials

$x^n - 1$ is divisible by $x - 1$:

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

if p prime, then the cyclotomic polynomial for p is

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

which is always irred over $\mathbb{Q}$ by Eisenstein's.

Irreducibility in $\mathbb{Z}$ and $\mathbb{Z}_n$

Let $f \in \mathbb{Z}[x]$ of degree at least 1, let p prime, and let $\bar{f}$ be f mod p. Then if

- $\deg f = \deg \bar{f}$
- $\bar{f}$ irred over $\mathbb{Z}_p$

then f irred over $\mathbb{Q}$.

Principal Ideals and PIDs

An ideal is principal if it can be generated by a single element a. If so, it can be written as $\langle a \rangle$. An integral domain D is a principal ideal domain if every ideal in D is a principal ideal.

Any field F is a PID by the results from ideals.

Prime and Maximal Ideals in Polynomial Rings

Let F be a field. An ideal $I = \langle p(x) \rangle$ is a prime ideal in $F[x]$ iff $p(x)$ irred over F. I is an maximal ideal if it is nontrivial.

Divisions of Irreducible Polynomials

Let $f, g \in F[x]$ irred polys, s.t. $f \neq cg$ for any unit $c \in F[x]$. Then

- $\gcd(f, g) = 1$
- there are $u, v \in F[x]$ s.t. $1 = uf + vg$
- u is the multiplicative inverse of f in $F/\langle g \rangle$

Chinese Remainder Theorem

Let F be a field and let

$$I_i = \langle g_i(x) \rangle$$

with $i = \{1, \ldots, n\}$, be ideals in $F[x]$ s.t. all g_is are paiwise coprime. Let $f_1, \ldots, f_n$ be polys in $F[x]$, then

- there is $f \in F[x]$ s.t. $f - f_i \in I_i$ for all i
- f uniquely determined up to congruence modulo the ideal $J = \langle \prod g_i(x) \rangle$

Corollary to CRT, Polynomial Rings modulo Primal Ideals

Let F be a field and let $I_i = \langle g_i(x) \rangle$ be ideals and g_i pairwise coprime, and let $J = \langle \prod g_i(x) \rangle$. Then

$$F[x]/J \cong F[x]/I_1 \times \cdots \times F[x]/I_n$$

Euclidean Domains

An integral domain D is called a Euclidean Domain if there is a function $\nu : D \setminus \{0\} \to \mathbb{Z}^+ \cup \{0\}$ from the set of nonzero elements of D to the set of nonnegative integers s.t.

- for nonzero $x, y \in D$, $\nu(x) \leq \nu(xy)$
- given $a, b \in D$ with b nonzero, there are $q, r \in D$ s.t. $a = qb + r$ with either $r = 0$ or $\nu(r) < \nu(b)$

where q is called the quotient and r is called the remainder in the division.

The domain of Gaussian Integers $\mathbb{Z}[i]$ is a Euclidean domain.

Every ED is a PID.

GCDs on EDs

Let D be a ED and $a, b \in D$ two nonzero elements of D. Then there exists an element $d \in D$ s.t.

- d is a GCD of a and b
- there are $u, v \in D$ s.t. $d = ua + vb$

Associates

Let R be a commutative ring with unity. $a, b \in R$ are associates if $a = ub$ for some unit $u \in R$.

Properties of Euclidean Functions ν

Let D be a ED. Then

- $\nu(1) \leq \nu(a)$ for all nonzero $a \in D$
- $\nu(1) = \nu(a)$ iff a a unit in D

Irreducibility vs Primality

Let D be an integral domain and $a \in D$ nonzero nonunit. Then

- a irreducible if $a = xy$ implies x or y unit.
- a prime if $a \mid xy$ implies $a \mid x$ or $a \mid y$.

In an integral domain, every prime is irreducible.

In a principal ideal domain D, $p \in D$ irred iff $I = \langle p \rangle$ is a maximal ideal in D. Moreover, a nonzero p is prime iff it is irred.

Unique Factorization Domain

An integral domain D is said to be a unique factorization domain (UFD) if the following are satisfied

- every nonzero nonunit $a \in D$ can be written as the product of irreducibles $p_i \in D$:

$$a = p_1 p_2 \dots p_n$$

- if

$$a = p_1 \dots p_n = r_1 \dots r_s$$

  where p_i, r_j irred, then $r = s$ and q_j can be renumbered so that p_i and q_i are associates in D

in a UFD, a nonzero element is prime iff it is irred.

Every PID is a UFD.

Ascending Chain Condition

Let D be a PID, and let $I_1 \subseteq I_2 \subseteq I_3$ be an ascending chain of ideals. Then there exists a positive integer n s.t. $I_m = I_n$ for all $m \geq n$.

The Ascending Chain Condition (ACC) holds in an integral domain D if D contains nos trictly increasing infinite chain of ideals.

Existance of Irred Divisor

Let D be a PID and $a \in D$ nonzero nonunit. Then a has at least one irred divisor. Moreover, it is a product of irreds.

Generalized Gauss' Lemma

Let D be a UFD and let f, g primitive polys in $D[x]$. Then fg is primitive.

UFD through Polynomial Rings

If D a UFD then $D[x]$ a UFD.

Primes over Gaussian Integers

Let $z = a + bi \in \mathbb{Z}[i]$ be s.t. $\nu(z) = a^2 + b^2$ is prime in $\mathbb{Z}$, then $z = a + bi$ is prime in $\mathbb{Z}[i]$.

Consequently, if p can be written as a sum of squares, i.e. $p = a^2 + b^2$, then $a + bi$ is prime in $\mathbb{Z}[i]$.

Fermat's Theorem on Sums of Squares

Let p be an odd prime. Then

$$p = a^2 + b^2 \qquad \iff \qquad p \equiv 1 \mod 4$$

Primes in Gaussian Integers

If $a + bi$ a prime in $\mathbb{Z}[i]$, then so is $a - bi$.

If a, b nonzero and $a + bi$ prime in $\mathbb{Z}[i]$, then $a^2 + b^2$ prime in $\mathbb{Z}$.

All the primes in $\mathbb{Z}[i]$ are exactly the following elements and their associates:

- $1 + i$ and $1 - i$
- p prime with $p \equiv 3 \mod 4$
- $a + bi$ and $a - bi$, where $a^2 + b^2 = p$ a prime with $p \equiv 1 \mod 4$

Vector Spaces

A set V equipped with two operations (addition and multiplication) is a vector space over F if V is an Abelian group under addition, and the following holds for all $a, b \in F$, $u, v \in V$:

- $av \in V$ is defined

- $a(v+w) = av + aw$
- $a(bv) = (ab)v$
- $1v = v$

$v \in V$ is called a vector. The additive identity on V is the zero vector 0. An element $a \in F$ is a scalar, and the operation of forming av is called scalar multiplication.

Properties of Scalar Multiplication

Let V be a vector space over a field F. Then for any scalar $c \in F$ and any vector $v \in V$

- $cv = 0$ iff $c = 0 \in F$ or $v = 0 \in V$
- $(-c)v = -(cv) = c(-v)$

Subspace Test

A nonempty subset U of a vector space V over a field F is a subspace of V iff for all $c \in F$ and $u, w \in U$ we have

- $u - w \in U$
- $cu \in U$

which is very similar to a subring test.

Any ideal in $F[x]$ where F a field is a subspace of $F[x]$.

Linear Independence, Bases and Dimensions

The set $\{v_i\}$ with $v_i \in V$ where V VS over F is linearly independent over F if

$$c_1 v_1 + c_2 v_2 + \cdots + c_n v_n = 0$$

implies that $c_i = 0$ for all i. In other words, the only linear combination of the vectors which leads to zero is trivial.

Such set of vectors is called a basis for V over F if the span of this set is V.

Any two basis of V over F have the same cardinality.

The cardinality of a basis of such vector spaces is called the dimension of V over F. If there exists no finite basis for V, then V is infinite dimensional over F.

Extendability of Base

Let V be a vector space over a field F with $\dim_F V = n$, and let $\{u_1, \ldots, u_r\}$ be a linearly independent set of vectors in V. Then

- $r \leq n$
- if $r < n$ then we can add $n - r$ vectors to the set to form a basis for V

Let U, the spans of $\{u_1, \ldots, u_r\}$ be a subspace of V. Then

- $\dim_F U \leq \dim_F V$
- $\dim_F U = \dim_F V$ iff $U = V$

Extension Fields

Let E a field and $F \subseteq E$ a subfield of E. Let $\alpha \in E$. Let

$$F[\alpha] = \{f(\alpha) : f(x) \in F[x]\} \qquad F(\alpha) = \{f(\alpha)/g(\alpha) : f(x), g(x) \in F[x], g(\alpha) \neq 0\}$$

then

- $F[\alpha]$ is the smallest subring of E containing F and α
- $F(\alpha)$ is the smallest subfield of E containing F and α

specifically, $F(\alpha)$ is an extension field of F, and is read F adjoining α.

Kronecker's Theorem

Let F be a field and $p(x)$ a nonconst polynomial in $F[x]$. Then there is an extension field of F, E, s.t. $\alpha \in E$ is a root of $p(x)$.

Algebraic and Transcendental Numbers

Let F be a field and E an extension field, $F \subseteq E$. Then an element $\alpha \in E$ is said to be algebraic over F if there exists a nonzero polynomial $f \in F[x]$ s.t. $f(\alpha) = 0$. Otherwise, α is transcendental over F.

Minimal Polynomials and Degrees of Algebraic Numbers

Let $F \subseteq E$ fields and $\alpha \in E$ algebraic over F. Then there is a unique monic polynomial $p(x) \in F[x]$ s.t.

- $p(\alpha) = 0$
- $p(x)$ irred over F

- if $f \in F[x]$ s.t. $f(\alpha) = 0$, then $p(x) \mid f(x)$

such $p(x)$ is called the minimal polynomial of α over F. The degree of α over F is

$$\deg_F(\alpha) = \deg p(x)$$

Priperties of Minimal Polynomials

Let $F \subseteq E$ be fields, $\alpha \in E$ algebraic over F with $\deg_F(\alpha) = n$, and let $p(x)$ be the minimal polynomial of α. Then

- $F(\alpha) \cong F[x]/\langle p(x)\rangle$
- $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for the vector space $F(\alpha)$ over F
- $\dim_F F(\alpha) = \deg_F(\alpha) = \deg p(x)$

Algebraic and Finite Extensions

Let E be an extension field of a field F. Then E is

- an algebraic extension of F if every element $\alpha \in E$ is algebraic over F
- a finite extension of F if E is a finite-dimensional vector space over F. In this case, the dimension n of E over F by $[E : F] = n$, and we call n the degree of E over F

If E is a finite extension of F, then it is an algebraic extension of F. Moreover,

$$\deg_F(\alpha) \leq [E : F]$$

for every $\alpha \in E$.

Degrees of Extensions and Elements Within

Let E be a finite extension field of a field F and K a finite extension field of E. Then K is a finite extension field of F and

$$[K : F] = [K : E][E : F]$$

Moreover, let $\alpha, \beta \in E$, with $\deg_F(\alpha) = n, \deg_F(\beta) = m$. Then $n, m \mid [E : F]$, and $[F(\alpha, \beta) : F] \leq nm$.

Algebraic Numbers

Let $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ algebraic over } \mathbb{Q}\}$. Then $\bar{\mathbb{Q}}$ is called the field of algebraic numbers.

Splitting Fields

Let $f \in F[x]$ nonconst, and E extension field of F. f splits over E if in $E[x]$, f can be written as a unit times monic linear factors:

$$f(x) = u(x - \alpha_1)(x - \alpha_n)$$

note $u \in F$. A subfield K of E containing F is called the splotting field in E of f over F if

- f splits over K
- K is the smallest subfield of E containing F over which $f(x)$ splits

More precisely, the splitting field in this case is $K = F(\alpha_1, \ldots, \alpha_n)$.

For any nonconstant $f \in F[x]$, it has a splitting field E that is a finite extension field of F. Moreover,

$$[E : F] \leq n!$$

any two splitting fields of f are isomorphic to each other.

10.3.20

This is too long. Don't wanna write it down.

Algebraic Closure

A field F is algebraically closed if every nonconst $f \in F[x]$ has a root in F. Moreover, it is equivalent to the following:

- $f \in F[x]$ irred iff $\deg f = 1$
- every nonconst poly in $F[x]$ splits over F
- if E is an algebraic extension of F, then $E = F$

The *Fundamental Theorem of Algebra* states that $\mathbb{C}$ is algebraically closed.

List of Facts

For any nonconst $f \in Q[x]$, there is a splitting field $K \subseteq \mathbb{C}$.

If E is an extension field of $\mathbb{C}$ and $[E : \mathbb{C}] > 1$, then E is not an algebraic extension of $\mathbb{C}$ and $[E : \mathbb{C}]$ is infinite.

Let $f \in \mathbb{R}[x]$ nonconst, then if f irred, it has degree 1 or 2.

Finite Fields

Let F be a finite field, then

- the order of F is a prime power: $|F| = p^n$, where $p = \operatorname{ch} F$.
- F is an algebraic extension $\mathbb{Z}_p(\alpha)$, where α is the root of an irred monic poly $q(x) \in \mathbb{Z}_p[x]$ of degree n

Moreover, $|F| = p^n$ iff F is a splitting field of $f(x) = x^{p^n} - x$ over $f \in \mathbb{Z}_p[x]$

Multiplicity and Roots

Let F be a field, $f(x) \in F[x]$ a poly, and $f(\alpha) = 0$ for an α in some extension field of F. Then α has multiplicity > 1 iff $f'(\alpha) = 0$.

More Results on Finite Fields

Given any prime p and any positive integer n,

- there exists a finite field F of order p^n
- any two fields of order p^n are isomorphic

Constructible Numbers

The set of constructible real numbers C is an extension field of $\mathbb{Q}$ and a subfield of $\mathbb{R}$. Specifically, let α be a constructible real number with $\sqrt{\alpha} > 0$, then $\sqrt{\alpha}$ is constructible.