TEST

DEFS

1. a proper ideal of a ring is an ideal $I \leq R$ so that I is not zero ideal and I is not R.
2. an integral domain is a commutatitve ring with idneity so that R has no nonzero zero divisors.
3. an ideal I of a ring R is a prime ideal iff $ab \in I$ implies $a \in I$ or $b \in I$.
4. let D be an integral domain. $p \in D$ is prime iff $p \mid ab \implies p \mid a \vee p \mid b$.
5. let D be an ID. then $p \in D$ irredubible iff $p = ab \implies$ a or b is a unit.
6. a principal ideal domain is an integral domain D so that every ideal in D is a principal ideal.
7. a unique factorization domain (UFD) is an integral domain so that (1): let $a \in D$ nonzero, nonunit. then we have that a can be written as a product of irreducibesl in D. (2): if $a = p_1, \dots p_n = q_1 \dots q_m$, then $n = m$ and there exists $\pi \in S_n$ so that $p_i, q_{\pi(j)}$ are associates.
8. An integral domain D is a euclidean domain with a fucntion $\nu : D \setminus \{0\} \to \mathbb{N}$ so that (1): if $a, b \in D$ nonzero, then $\nu(a) \leq \nu(ab)$. (2): if $a, b \in D$ and $b \neq 0$, then there exist $q, r \in D$ so that $a = bq + r$ with $r = 0$ or $\nu(r) < \nu(b)$.
9. let I, J be ideals. Then their product is $I \cdot J = \{\sum_{k=1}^{n} a_k b_k \mid a_k \in I, b_k \in J, n \in \mathbb{Z}_{>0}\}$.
10. let R be a ring. it is finitely generrated iff there exist $x_1, \dots, x_n \in R$ (for some $n \in \mathbb{Z}_{>0}$) so that $R = \langle x_1, \dots, x_n \rangle = \{a_1 x_1 + \dots + a_n x_n \mid a_i \in R \forall i\}$.
11. let R be a commutative ring with identity. then $x, y \in R$ are asssociates iff there exist $c \in U(R)$ so that $x = yc$.
12. a vector space is a set V so that
    (a) $(V, +)$ is an abelian group, with so that $+ : V \times V \to V$ so that $(u, v) \mapsto u + v$.
    (b) V closed under scalar multiplication, i.e. if $\lambda \in F$ and $v \in V$, then $\lambda \cdot v \in V$.
    (c) $(\alpha\beta)v = \alpha(\beta v)$.
    (d) $\alpha(u + v) = \alpha u + \alpha v$.
    (e) $(\alpha + \beta)v = \alpha v + \beta v$.
    (f) $1 \cdot v = v$.
13. a linear map from F-vector spaces V, W is a map $\phi : V \to W$ so that $\phi(v + w) = \phi(v) + \phi(w)$ and $\phi(cv) = c\phi(v)$.
14. let $E \geq F$ be fields with field extension. then $E \geq F$ is a simple algebraic field extension iff $E = F(\alpha_1)$ where $\alpha \in E$ and algebraic over F.
15. let E and F be fields. $E \geq F$ is a simple algebraic field extension iff $E \cong F[x]\langle p(x) \rangle$ for irreducible $p(x)$.
16. $F[p(x)] := F(\alpha_1, \dots, \alpha_n)$, where $\alpha_1, \dots, \alpha_n$ are all the roots of $p(x)$.
17. let F be a field and $p(x)$ be a nonconstant polynomial in $F[x]$. Then $E \geq F$ is a splitting field of the extension $E \geq F$ iff $E = F(\alpha_1, \dots, \alpha_n)$ for some $\alpha_i \in E (\forall i)$ and so that $p(x) = \prod(x - \alpha_i)$.
18. the degree of a splitting field extension is the dimension of the vector space it genrates.
19. let $E \geq F$ be a field extension. then an automorphism of E over F is a bijective ring homoomrphism $\phi : E \to E$ so that $\phi(f) = f \forall f \in F$.

1. if T is a field, then its only ideals are the zero one and T itself.
2. R/I is a field iff I is maximal in R.
3. for a given ring, the set of zero divisors is disjoint from the set of units.
4. R/I is an integral domain iff I is a prime ideal in R.
5. div alg. Let $a, b \in Z$ so that $b \neq 0$. Then there exist unique $q, r \in Z$ so that $a = bq + r$ with $0 \leq r < b$.
6. let $a, b \in Z$ nonzero. then there exist integers $p, q \in Z$ so that $\gcd(a, b) = pa + qb$, where $\gcd(a, b)$ is unique.

7. fundamental theorem of arithemetic. let $n \in \mathbb{Z}_{>0}$. then n can be factored uniquely into product of primes.
8. if $a(x), b(x) \in F[x]$, then there exist unique $q(x), r(x) \in F[x]$ so that
   (a) $a(x) = q(x)b(x) + r(x$.
   (b) $\deg(r(x)) < \deg(b(x))$.
9. if F is a field, then $\alpha \in F$ so that α is a root of $p(x) \in F[x]$ iff $(x - \alpha) \mid p(x)$.
10. if F is any field and $f(x) \in F[x]$ has degree n, then $f(x)$ has at most n roots.
11. $Z[i]$ is a commutative ring with identity but not a field.
12. units in $Z[i]$ are ± 1 and is an integral domain.
13. $N(xy) = N(x)N(y)$ for all x, y in the gaussian integers.
14. div. alg. for guasssian integers. let $\alpha, \beta \in Z[i]$, and also let $\beta \neq 0$. then there exist $q, r \in Z[i]$ so that $\alpha = q\beta + r$ where $r = 0$ or $N(r) < N(b)$.
15. $Z[sqrt - 5]$ is an integral domain, commutative ring with 1, but not a field.
16. the units in z sqrt -5 are ± 1 and is an integral domain.
17. norm is multiplicative on z sqrt -5
18. let R be an integral domain. then every prime is irreducible.
19. 3 is irreducible in z sqrt -5 but not prime
20. let R be a integral domain. then $\langle u \rangle = R$ iff u is a unit in R.
21. let R be an integral and $r \in R$ a nonunit. then $\langle r \rangle$ is prime iff r is prime.
22. if $I =< a >$ and $J =< b >$, then $I \cdot J =< ab >$, where I and J are (principal) ideals in R.
23. if $R = Z$ and $x_1, \ldots, x_n \in Z$ then $\langle x_1, \ldots, x_n \rangle = \{a_1 x_1 + \cdots + a_n x_n, \mid a_i \in R \forall i\} =< \gcd(x_i s >$.
24. z sqrt -5 is not a principal ideal domain.
25. let R be z sqrt -5. for norm we have that $N(A) = 0$ iff $A = 0$, α is a unit iff $N(\alpha) = \pm 1$, and if $N(\alpha)$ is prime, then α is irreducible.
26. every maximal ideal of a commutativie ring with identiy is a prime ideal .
27. fundamental theorem of ideal theory. let R be a commutative ring with identity. and I be a nonzero proper ideal of R. then there exists a unique (up to order) factorization $I = P_1 \cdots P_k$ (for some k) so that each P_i is a prime ideal.
28. let α be a nonzero nonunit element of z sqrt -5. then α is irreducible iff $< \alpha >$ is prime, or iff $< \alpha >= P_1 \cdot P_2$, where P_i are nonprincipal prime ideals.
29. if α is a nonzero elemtn of z sqrt -5, and $\beta_1, \ldots, \beta_n$ and $\gamma_1, \ldots, \gamma_m$ are irreducbible, with the products both equal to α, then $s = t$.
30. if F is a field then $F[x]$ is a PID.
31. let $p(x) \in F[x]$. then $\langle p(x) \rangle$ is maximal iff $p(x)$ is irreducible.
32. in $F[x]$, prime ideals = maximal ideals.
33. if $E \geq F$ is a field extension, then E is an F-vector spcae.
34. splitting field algorithm. let F be a field and $p(x) \in F[x]$ irred. then to find the splitting field of $F[p(x)]$, we have that put $F_1 := F[x] < p(x) >$, and write $p(x) = (x - a_1)q(x)$, put F_2 and so on....
35. let $F = K(a_1, a_2)$ be a field extension. then the degree $[F : K] = [F : K(a_1)] \cdot [K(a_1) : K]$.
36. $\{\mathrm{id}, \}$ are all the automorphisms of C over R.