CS21001 Discrete Structures, Autumn 2005

Exercise set 5

---

1. Let R be a ring. Prove that:

(a) $0 \cdot x = 0$ for all $x \in R$.

(b) $x(-y) = (-x)y = -(xy)$ and $(-x)(-y) = xy$ for all $x, y \in R$.

(c) R is commutative if and only if $(x+y)^2 = x^2 + 2xy + y^2$ for all $x, y \in R$.

(d) R is commutative if and only if $(x+y)(x-y) = x^2 - y^2$ for all $x, y \in R$.

2. Let R be a commutative ring. An element $a \in R$ is said to be *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$. Prove that if a and b are nilpotent, then so also is $a + b$. Conclude that the set of all nilpotent elements of R is an ideal of R. This ideal is called the *nilradical* of R.

3. The *characteristic* of a ring R is defined to be the smallest positive integer n for which $1 + 1 + \cdots + 1$ (n times) $= 0$. In this case we say $\operatorname{char} R = n$. If no such n exists, we say that $\operatorname{char} R = 0$.

(a) What are the characteristics of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$?

(b) Prove that $\operatorname{char} R = \operatorname{char} R[x]$.

(c) Let R be an integral domain of positive characteristic n. Prove that n is a prime.

4. Let R be an integral domain of prime characteristic p and let $a, b \in R$. Prove that:

(a) The binomial coefficient $\binom{p}{r}$ is divisible by p for $1 \leqslant r \leqslant p-1$.

(b) $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ for all $n \in \mathbb{N}_0$.

5. Let $f(x) = x^4 + 3x^3 + x + 3$ and $g(x) = x^3 + 2x^2 + 2x + 1$.

(a) Compute $\gcd(f, g)$ in $\mathbb{Z}[x]$.

(b) Compute $\gcd(f, g)$ in $\mathbb{Z}_7[x]$.

(c) Compute the extended gcd of f, g in $\mathbb{Z}[x]$.

(d) Compute the extended gcd of f, g in $\mathbb{Z}_7[x]$.

6. Find the complete factorization of the following polynomials:

(a) $x^4 + x^2 + 1$ in $\mathbb{Z}[x]$.

(b) $x^4 + x^2 + 1$ in $\mathbb{C}[x]$.

(c) $x^4 + 3x^3 + 2x + 4$ in $\mathbb{Z}_5[x]$.

(d) $x^4 + 16$ in $\mathbb{Z}_{17}[x]$.

* **(e)** $x^{22} + 22$ in $\mathbb{Z}_{23}[x]$.

7. Let F be an infinite field and $f(x), g(x) \in F[x]$. If $f(a) = g(a)$ for infinitely many elements $a \in F$, prove that $f(x) = g(x)$.

8. **(a)** Let R be an integral domain. Define a relation $\sim$ on $R \times (R \setminus \{0\})$ as $(a, b) \sim (c, d)$ if and only if $ad = bc$. Prove that $\sim$ is an equivalence relation.

(b) The equivalence class of (a, b) is denoted by a/b and the set of all equivalence classes by $\mathrm{Q}(R)$. Define addition and multiplication in $\mathrm{Q}(R)$ as $(a/b) + (c/d) = (ad + bc)/(bd)$ and $(a/b)(c/d) = (ac)/(bd)$. Prove that these operations are well-defined, i.e., independent of the choice of the representatives of the classes.

(c) Prove that $\mathrm{Q}(R)$ is a field under these operations. We call $\mathrm{Q}(R)$ the *quotient field* of R. We have $\mathrm{Q}(\mathbb{Z}) = \mathbb{Q}$ and $\mathrm{Q}(F[x]) = F(x)$, where F is a field and $F(x)$ is the set of all *rational functions* over F.

9. Let $R = \{a + \mathrm{i}b \mid a, b \in \mathbb{Z}\}$ be the ring of Gaussian integers. Take $a + \mathrm{i}b, c + \mathrm{i}d \in R$ with $c + \mathrm{i}d \neq 0$.

* **(a)** Prove that there exist $p + \mathrm{i}q, r + \mathrm{i}s \in R$ such that $a + \mathrm{i}b = (p + \mathrm{i}q)(c + \mathrm{i}d) + (r + \mathrm{i}s)$ with $0 \leqslant |r + \mathrm{i}s| \leqslant \frac{1}{\sqrt{2}}|c + \mathrm{i}d|$. (Hint: First express $\frac{a+\mathrm{i}b}{c+\mathrm{i}d} = x + \mathrm{i}y$, where x, y are rationals.)

(b) Conclude that R is a Euclidean domain. Demonstrate how you can compute the gcd of two elements (not both zero) in R.

10. Let R be a ED, $a, b \in R$ (not both zero), and d a gcd of a and b. Prove that $\langle a \rangle + \langle b \rangle = \langle d \rangle$.

11. Let R be a commutative ring. A non-zero non-unit $p \in R$ is called *prime* if $p \mid (ab)$ in R (with $a, b \in R$) implies $p \mid a$ or $p \mid b$. A non-zero non-unit $x \in R$ is called *irreducible* if $x = uv$ with $u, v \in R$ implies either u or v is a unit. Prove that every prime element is irreducible.

12. Let $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Prove that R is a commutative ring under complex addition and multiplication. Prove that the elements $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are all irreducible in R. Use the fact $2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ to conclude that every irreducible element is not necessarily prime. (Note: R is an example of a ring in which unique factorization does not hold.)

13. Let R be a ring and $\mathfrak{a}, \mathfrak{b}$ ideals of R.

(a) Prove that $\mathfrak{a} \cap \mathfrak{b}$ is an ideal of R.

(b) Prove that $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ is an ideal of R.

(c) Demonstrate by an example that $\mathfrak{a} \cup \mathfrak{b}$ is not necessarily an ideal of R.

* **(d)** Demonstrate by an example that $\mathfrak{a}\mathfrak{b} = \{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ is not necessarily an ideal of R.

14. Let R be a commutative ring. An ideal $\mathfrak{m}$ of R is called *maximal* if $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R$ with $\mathfrak{a}$ an ideal implies $\mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = R$. In other words, there does not exist a proper ideal strictly containing a maximal ideal.

(a) Let $n \in \mathbb{N}$. Prove that the ideal $\langle n \rangle$ is maximal in $\mathbb{Z}$ if and only if n is a prime.

(b) Let F be a field and $f(x) \in F[x]$ a non-constant polynomial. Prove that the ideal $\langle f(x) \rangle$ is maximal in $F[x]$ if and only if $f(x)$ is irreducible in $F[x]$.

* **(c)** Let $\mathfrak{a}$ be an ideal of R. Prove that $\mathfrak{a}$ is maximal in R if and only if $R/\mathfrak{a}$ is a field.

15. Let R, S be rings. A function $f : R \to S$ is called a *homomorphism of rings* if $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$ and if $f(1_R) = 1_S$. A ring homomorphism is called an *isomorphism* if f has an inverse $g : S \to R$ such that g is also a ring homomorphism.

(a) Prove that f is an isomorphism if and only if f is bijective as a function.

(b) Let $n \in \mathbb{N}$. Demonstrate that the function $\mathbb{Z} \to \mathbb{Z}_n$ that maps a to $a \operatorname{rem} n$ is a ring homomorphism.

(c) Prove that the only homomorphism $\mathbb{Z} \to \mathbb{Z}$ is the identity map.

* **(d)** Let F, K be fields and $f : F \to K$ a homomorphism. Prove that f is injective.

* **(e)** [*Isomorphism theorem*] Let $f : R \to S$ be a ring homomorphism. The *kernel* of f is defined as $\operatorname{Ker} f = \{a \in R \mid f(a) = 0_S\}$. The *image* of f is defined as $\operatorname{Im} f = \{f(a) \mid a \in R\}$. Prove that $\operatorname{Ker} f$ is an ideal in R, $\operatorname{Im} f$ is a subring of S, and $R/\operatorname{Ker} f$ is isomorphic to $\operatorname{Im} f$.

* **16.** Prove that every element in $\mathbb{Z}_p$, p prime, has a p-th root in $\mathbb{Z}_p$, i.e., for every $a \in \mathbb{Z}_p$ there exists $x \in \mathbb{Z}_p$ such that $x^p = a$. (Hint: Fermat's little theorem.)

17. Let F be a field. We can identify every integer n with an element of F in the following way. The integer 0 is identified with the additive identity of F. For $n > 0$ we identify the integer n with $1+1+\cdots+1$ (n times), where 1 is the multiplicative identity of F. Finally, if $n = -m < 0$, we identify the integer n with the additive inverse of m in F.

Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ be a polynomial in $F[x]$. The *formal derivative* of $f(x)$ is defined to be the polynomial $f'(x) = d a_d x^{d-1} + (d-1)a_{d-1}x^{d-2} + \cdots + a_1 \in F[x]$.

(a) Prove that $(f + g)' = f' + g'$ and $(fg)' = f'g + fg'$ for all $f, g \in F[x]$.

(b) Let $\operatorname{char} F = 0$. Show that $f'(x) = 0$ if and only if $f(x)$ is a constant polynomial.

** **(c)** Let $F = \mathbb{Z}_p$ with p prime. Prove that $f'(x) = 0$ if and only if $f(x) = g(x)^p$ for some $g(x) \in \mathbb{Z}_p[x]$.