
(1) [5] Find the centre of the ring of real quaternions $\mathbb{H}$.

**Answer:** $\mathbb{R} = \{a + 0i + 0j + 0k \mid a \in \mathbb{R}\}$. It is clear that all real elements commute with everything. To prove that no other elements are in the centre, consider $x = a + bi + cj + dk$. Since $xi = ix$, we get (by definition of the multiplication in $\mathbb{H}$)

$$ai - b - ck - dj = ai - b + cj + dk,$$

so $c = d = 0$. Similarly, since $x$ commutes with $j$, we get $b = 0$.

(2) [5] Let $R$ be a commutative ring with 1. Prove that if there exists a prime ideal $P$ of $R$ that contains no zero divisors, then $R$ is an integral domain.

**Solution:** Suppose $R$ had zero divisors, say $ab = 0$ with $a, b \neq 0$. Then consider $R/P$. We should have $\overline{a}\overline{b} = \overline{0}$ in $R/P$, but since $P$ is prime, $R/P$ is an integral domain, and thus $\overline{a}$ or $\overline{b} = 0$, which implies $a$ or $b$ is contained in $P$ – a contradiction with the assumption that $P$ contains no zero divisors.

(3) Let $R$ be a commutative ring with 1, and $I, J$ – ideals in $R$.

(a) [2] Give a sufficient condition for the equality $IJ = I \cap J$ to hold (just a statement, no proof required).

**Answer:** $I$ and $J$ are comaximal.

(b) [3] Give an example of two ideals $I$ and $J$ in a commutative ring $R$, such that $IJ \neq I \cap J$.

**Example:** $R = \mathbb{Z}$, $I = J = 2\mathbb{Z}$.

(c) [6] Prove that if $R$ is a UFD, and $I = (a)$, $J = (b)$ are two principal ideals, then $IJ = I \cap J$ if and only if $a$ and $b$ have no common irreducible factors.

**Proof:** Suppose $IJ = I \cap J$. Let us prove that then $a$ and $b$ have no common factors. Suppose they had a common irreducible factor $r$, say $a = ra'$, $b = rb'$. Then the element $ra'b'$ would be in $I \cap J$ but not in $IJ$.

Conversely, suppose $a$ and $b$ have no common factors. Then we want to show that $I \cap J \subseteq IJ$ (the reverse inclusion always holds). Let $x \in I \cap J$. Then $x = ax' = by'$ for some $x', y' \in R$. Since $R$ is a UFD and $a$ and $b$ have no common factors, $x'$ has to be divisible by all the irreducible factors of $b$, and $y'$ has to be divisible by all the irreducible factors of $a$. But then $x'$ is divisible by $b$, and so $x = ax' = abx''$ for some $x''$, i.e., $x \in IJ$.

(4) [5] Is 7 prime in $\mathbb{Z}[\frac{1 + \sqrt{-3}}{2}]$? If not, factor it as a product of primes, with proof that the factors are prime.

**Solution:** The ring $\mathbb{Z}[\frac{1 + \sqrt{-3}}{2}]$ is Euclidean, and hence for its elements prime is equivalent to irreducible. The element 7 is not irreducible: $7 = (2 + \sqrt{-3})(2 - \sqrt{-3}) = 4 + 3$, hence it is not prime. The norm of each of the elements $2 \pm \sqrt{-3}$ is $|2 + \sqrt{-3}|^2 = 7$, which is a prime in $\mathbb{Z}$. Hence, these elements are irreducible (their norms cannot be factored, hence they cannot be factored). Then this is a factorization into prime factors.
(5) [5] Find an example of an element of $\mathbb{Z}[\sqrt{-3}]$ that is irreducible but not prime (and give a complete proof that it has this property).

Answer: For example, $2$. It is irreducible because its norm is 4, and so if it factors, it factors as a product of elements of norm 2, but an element of $\mathbb{Z}[\sqrt{-3}]$ cannot have norm 2. On the other hand, it is not prime, since $(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4 \in (2)$, but neither element $1 \pm \sqrt{-3}$ lies in the ideal $(2)$.

(6) [6] Let $F$ be a field that has infinite cardinality. Let $n$ be an arbitrary integer. Prove that for any collection of distinct elements $a_1, \ldots, a_n \in F$, and any collection of values $c_1, \ldots, c_n \in F$ there exists unique polynomial $f \in F[x]$ of degree at most $n - 1$ such that $f(a_i) = c_i$ for $1 \leq i \leq n$.

Solution sketch: This is known as Lagrange interpolation; but here we obtain it as an easy corollary of Chinese Remainder Theorem. Consider the ideals $(x - a_i)$ in $F[x]$. These are pairwise comaximal. Note that the condition $f(a_i) = c_i$ is equivalent to $f \equiv c_i \mod (x - a_i)$. This pretty much completes the proof: use Chinese Remainder Theorem for this collection of ideals. Note that the least common multiple of $(x - a_i)$ is their product, which is a polynomial of degree $n$.

(7) Describe the quotient ring (i.e. find a simpler-looking ring isomorphic to it). Is the ideal $(x^2 + 1)$ maximal in either of these rings?

(a) $[4] \mathbb{F}_5[x]/(x^2 + 1)$

Solution: Note that $x^2 + 1 = (x - 2)(x + 2)$ in $\mathbb{F}_5[x]$; hence, by Chinese Remainder Theorem,

$$\mathbb{F}_5[x]/(x^2 + 1) \cong \mathbb{F}_5[x]/(x - 2) \times \mathbb{F}_5[x]/(x + 2) \cong \mathbb{F}_5 \times \mathbb{F}_5.$$ 

The ideal is not maximal, since the quotient is not a field.

(b) $[4] \mathbb{F}_7[x]/(x^2 + 1)$. Here the polynomial $x^2 + 1$ is irreducible, and hence generates a maximal ideal (remember that $\mathbb{F}_7[x]$ is a PID). The quotient is the field of 49 elements.

(8) [5] Let $F$ be a field, and let $I = (x, y^2 + x^2)$ be the ideal in $F[x, y]$ generated by the polynomials $x$ and $y^2 + x^2$. Describe the quotient ring $F[x, y]/I$ (i.e. find a simpler-looking ring isomorphic to it). (Hint: think of $F[x, y]/(x)$ first.)

Solution: Here we use the third Isomorphism Theorem: let $\pi : F[x, y] \to F[x, y]/(x)$ be the projection onto the quotient. Let $J = \pi(I)$ be the image of the ideal $I$ in the quotient ring $F[x, y]/(x)$. Then by the third Isomorphism Theorem, we have

$$F[x, y]/I \cong (F[x, y]/(x))/J.$$ 

Now note that $F[x, y]/(x) \cong F[y]$, and $J = (y^2) \subset F[y]$. Thus, the answer is $F[y]/(y^2)$.

(9)* (extra credit, 3 pts) Suppose we tried to construct a quaternion ring over $\mathbb{F}_p$ by considering expressions $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{F}_p$, and the operations as in the usual quaternion ring (except all the operations with the coefficients are modulo $p$). Prove that this ring has to contain zero divisors. (Hint: you can quote any theorems proved or even barely mentioned in the course.)
There are several solutions; I meant just a reference to Wedderburn’s Theorem (any finite division ring is a field), which was mentioned in Dummit and Foote but I cannot seem to find it right now).