1. Define what it means to say that a ring is an integral domain.

Let R be an integral domain.

(a) Define what is meant by a unit of R.

Prove that u is a unit of R if and only if $uR = R$.

(b) Define what is meant by an irreducible element of R.

Find the units of $\mathbb{Z}[i]$.

For each of the elements $1 + 3i$ and $2 + 3i$ of $\mathbb{Z}[i]$, determine whether or not the element is irreducible.

(c) Define what is meant by a unique factorization domain.

Prove that $\mathbb{Z}[\sqrt{-11}]$ is *not* a unique factorization domain.

2. Say what is meant by an ideal of a commutative ring. Define what is meant by a principal ideal domain.

(a) Let $R = \mathbb{Q}[x]$. Prove that the ideal $(x^2 - 4)R + (x^3 - x^2 - x - 2)R$ of R is a principal ideal. (*If you use the fact that R is a Euclidean domain, then you must provide a full proof of this fact.*)

(b) Let $R = \mathbb{Z}[x]$. Prove that the ideal $2R + xR$ of R is *not* a principal ideal.

(c) Prove that if R is a principal ideal domain and

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

are ideals of R, then for some n we have

$$I_n = I_{n+1} = I_{n+2} = \ldots .$$

(d) Give an example of a principal ideal domain R and ideals $I_1, I_2, I_3, \ldots$ of R such that

$$I_1 \supset I_2 \supset I_3 \supset \ldots .$$

3. Suppose that R is a principal ideal domain and that $a, b, p \in R$, with p irreducible. Prove that if p divides ab, then p divides a or p divides b.

Now let p be an odd prime number.

Prove that if p divides $x^2 + 2$ for some integer x then p may be written in the form $p = u^2 + 2v^2$ for some integers u and v. (*You may assume that $\mathbb{Z}[\sqrt{-2}]$ is a principal ideal domain.*)

Conversely, prove that if p may be written in the form $p = u^2 + 2v^2$ for some integers u and v then p divides $x^2 + 2$ for some integer x.

4. Suppose that $f(x)$ is a non-constant polynomial with integer coefficients. Prove that if $f(x)$ is irreducible in $\mathbb{Z}[x]$ then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

State Eisenstein's Irreducibility Criterion.

For each of the following polynomials, determine whether or not the polynomial is irreducible over $\mathbb{Q}$.

(a) $x^3 - 9$

(b) $x^4 + x^2 + 1$

(c) $x^4 - 255x + 2004$.

5. Suppose that F and K are fields with $F \subseteq K$. Define what is meant by the degree $|K : F|$ of K over F.

Assume that F, K and E are fields with $F \subseteq K \subseteq E$, and that $|K : F|$ and $|E : K|$ are finite. State and prove a relation connecting $|E : F|$ to $|K : F|$ and $|E : K|$.

Suppose that m is a positive integer and let $\alpha = \cos(\frac{\pi}{2m})$.

Prove that the degree of the minimal polynomial of α over $\mathbb{Q}$ is at most m.

Prove that in the case where m is a power of 2, the degree of the minimal polynomial of α over $\mathbb{Q}$ is also a power of 2.

(You may quote any general results on minimal polynomials which you need.)