Final

May 9th

- To do a later question in a problem, you can always assume a previous question even if you have not answered it.
- I am aware that this is long. I don't expect you to do everything.
- There are 16 questions distributed among 4 problems.
- Remember that using a pen and writing clearly improves readability.

Problem 1 :

1. Let R be an integral domain. Show that prime elements are irreducible.

2. Let R be a PID. Show that any a, $b \in R$ have a greatest common divisor.

3. Let $F \leqslant K$ be a field extension, and $a \in K$ be algebraic over F. Show that there exists an irreducible $P \in F[X]$ such that $P(a) = 0$.

Problem 2 :
Let G be a finite group and H, K be two subgroups of G. For all $g \in G$, we define $gHg^{-1} := \{g \cdot h \cdot g^{-1} : h \in H\}$. Let $S = \{gHg^{-1} : g \in G\}$.

1. For all $g \in G$, show that gHg^{-1} is a subgroup of G and that $h \mapsto g \cdot h \cdot g^{-1}$ defines a group isomorphism between H and gHg^{-1}.

2. For all $k \in K$ and $L \in S$, define $k \star L := kLk^{-1} = \{k \cdot l \cdot k^{-1} : l \in L\}$. Show that this defines an action of K on S and that for all $L \in S$, $\mathrm{Stab}[K](L) = \mathrm{N}_G(L) \cap K$.

3. Show that $|S|$ divides $[G : H]$.

4. Assume that $|K| = p^n$ for some prime p and some $n \in \mathbb{Z}_{>0}$. Let $F := \{L \in S : \forall k \in K, k \star L = L\}$. Show that $|F| \equiv |S| \mod p$.

5. Assume that both $|K|$ and $|H|$ are powers of some prime p and that $\gcd(p, [G : H]) = 1$. Show that there exists $L \in S$ such that $K \leqslant \mathrm{N}_G(L)$.

6. With the same assumptions and notations as above (in particular, $K \leqslant \mathrm{N}_G(L)$), show that $[LK : L]$ is a power of p. Conclude that $K \leqslant L$.

Problem 3 :
Let R be a commutative ring and $I \subset R$ be a proper ideal. Recall that

$$\sqrt{I} := \bigcap_{I \subseteq \mathfrak{p} \text{ prime ideal}} \mathfrak{p}.$$

We also define

$$\mathcal{J}(I) := \bigcap_{I \subseteq \mathfrak{M} \text{ maximal ideal}} \mathfrak{M}.$$

1. Show that $\mathcal{J}(I) \subseteq R$ is an ideal and that $\sqrt{I} \subseteq \mathcal{J}(I)$.

2. Let R be a PID and $a \in R$. Assume that $a = \prod_{i=0}^{k} p_i^{\alpha_i}$ where the p_i are pairwise non associated irreducibles and $\alpha_i \in \mathbb{Z}_{>0}$. Show that $R/(a)$ is isomorphic to $\prod_k R/(p_i^{\alpha_i})$.

3. With the same notations and assumptions than in the previous question, show that $\sqrt{(a)} = \mathcal{J}((a)) = (\prod_{i=0}^{k} p_i)$.

Problem 4 :
Let F be a field of characteristic zero. For all $P = \sum_{i=0}^{k} a_i X^i \in F[X]$, we define $P' = \sum_{i=0}^{k-1}(i+1)a_{i+1}X^i$.

1. Show that $P \mapsto P'$ is a group homomorphism $(R[X], +) \to (R[X], +)$ whose kernel is the set of constant polynomials.

2. Show that, for all $P, Q \in F[X]$, $(PQ)' = P'Q + PQ'$ and that $(P^n)' = nP'P^{n-1}$.

3. Show that if a is a root of P of multiplicity $n \in \mathbb{Z}_{>0}$, then a is a root of P' of multiplicity $n-1$ (by convention, a is a root of P of multiplicity 0 if it is not a root of P).

4. Let $F \leqslant K$ be a field extension, $P \in F[X]$ an irreducible polynomial and $a \in K$ a root of P of multiplicity strictly greater than 1. Show that $P' = 0$.