Lior Silberman's Math 501: Problem Set 2 (due 25/9/2020)

Some polynomial algebra

1. Let R be a ring, $P \in R[x]$.
   (a) Show that $(x-y)$ divides $(x^n - y^n)$ in $\mathbb{Z}[x,y]$, and conclude that if $a \in R$ is such that $P(a) = 0$ then $(x-a)|P$ in $R[x]$.
   (b) Suppose now that R is an integral domain and that $\{a_i\}_{i=1}^k \subset R$ are *distinct* zeroes of P. Show that $\prod_{i=1}^k (x-a_i)|P$ in $R[x]$. Give a counterexample when R has zero-divisors.

2. (The Vandermonde determinant) Let $\mathcal{V}_n(x_1,\ldots,x_n) \in M_n(\mathbb{Z}[x_1,\ldots,x_n])$ be the $n \times n$ *Vandermonde matrix* $(\mathcal{V}_n)_{ij} = x_i^{j-1}$. Let $V_n(\underline{x}) = \det(\mathcal{V}_n(\underline{x})) \in \mathbb{Z}[x_1,\ldots,x_n]$ (in other words, the entries of $\mathcal{V}_n$ come from the ring of polynomials in n variables, and hence its determinant is also in this ring).
   (*a) Show that there exists $c_n \in \mathbb{Z}$ so that $V_n(\underline{x}) = c_n \prod_{i>j}(x_i - x_j)$.
   Hint: You know $n-1$ zeroes of V_n, thought of as an element of $(\mathbb{Z}[x_1,\ldots,x_{n-1}])[x_n]$.
   (b) Setting $x_n = 0$ show that $c_n = c_{n-1}$, hence that $c_n = 1$ for all n.
   SUPP (Lagrange interpolation) Let F be a field. Show that for any $\{(x_i,y_i)\}_{i=1}^n \subset F^2$ with the x_i distinct there is a unique polynomial $p \in F[x]$ of degree at most $n-1$ such that $p(x_i) = y_i$.

Irreducible polynomials and zeroes

3. Let $f \in \mathbb{Z}[x]$ be non-zero and let $\frac{a}{b} \in \mathbb{Q}$ be a zero of f with $(a,b) = 1$. Show that constant coefficient of f is divisible by a and that the leading coefficient is divisible by b. Conclude that if f is monic then any rational zero of f is in fact an integer.

4. Decide while the following polynomials are irreducible
   (a) $t^4 + 1$ over $\mathbb{R}$.
   (b) $t^4 + 1$ over $\mathbb{Q}$.
   (c) $t^3 - 7t^2 + 3t + 3$ over $\mathbb{Q}$.

5. Show that $t^4 + 15t^3 + 7$ is reducible in $\mathbb{Z}/3\mathbb{Z}$ but irreducible in $\mathbb{Z}/5\mathbb{Z}$. Conclude that it is irreducible in $\mathbb{Q}[x]$.

Derivations and differential rings

- Differential rings will be a source of some advanced examples in this course covered only in problem sets. It's ok to skip this material.
- In a ring R for any $n \in \mathbb{Z}_{\geq 0}$ we identify $n = \overbrace{1_R + \cdots + 1_R}^{n}$ (and similarly for $-n$).

6. Let R be a ring, and let S be an R-algebra (a ring with a compatible structure as an R-module). A *derivation* on S is an R-linear map $\partial\colon S \to S$ such that $\partial(fg) = \partial f \cdot g + f \cdot \partial g$ for all $f,g \in S$. A *differential R-algebra* is a pair (S,∂) with S,∂ as above.
   (a) Call $f \in S$ *constant* if $\partial f = 0$. Show that the set of constants is a subring containing the image of R in S.
   (b) Show that $\partial(f^n) = nf^{n-1}\partial f$ for positive n, and also for negative n if f is invertible (hint: apply ∂ to $f^n \cdot f^{-n} = 1$). Conclude that if S is a field then the set of constants is a subfield, the *field of constants.*
   (c) Show that for any open interval $I \subset \mathbb{R}$, $\frac{d}{dx}$ is a derivation on the $\mathbb{R}$-algebra $C^\infty(I)$.
   (d) Show that for any ring R, $\partial\left(\sum_{n=0}^\infty a_n x^n\right) \stackrel{\text{def}}{=} \sum_{n=1}^\infty n a_n x^{n-1}$ defines a derivation on $R[[x]]$, the *formal derivative*. Show that if R is an integral domain then the constants of ∂ are exactly the constant series $a_0 + \sum_{n=1}^\infty 0x^n$.
   SUPP Let ∂_1, ∂_2 be derivations on S and let $\alpha \in R$. Show that $f \mapsto \alpha\partial_1 f$ and $f \mapsto \partial_1\partial_2 f - \partial_2\partial_1 f$ are derivations. This makes the set of derivations into a *Lie algebra* over R.

Supplementary Problems I: Review of ideals

Fix a ring R.

A. (Working with ideals)
   (a) Let $\mathcal{I}$ be a set of ideals in R. Show that $\bigcap \mathcal{I}$ is an ideal.
   (b) Given a non-empty $S \subset R$ show that $(S) \stackrel{\text{def}}{=} \bigcap \{I \mid S \subset I \lhd R\}$ is the smallest ideal of R containing S.
   (c) Show that $(S) = \{\sum_{i=1}^{n} r_i s_i \mid n \geq 0,\, r_i \in R,\, s_i \in S\}$.
   (d) Let $a \in R^{\times}$. Show that a is not contained in any proper ideal.
   Hint: Show that $a \in I$ implies $1 \in I$.

B. (Prime and maximal ideals) Call $I \lhd R$ *prime* if whenever $a, b \in R$ satisfy $ab \in I$, we have $a \in I$ or $b \in I$. Call I *maximal* if it is not contained in any proper ideal of R.
   (a) Show that R is an integral domain iff $(0) = \{0\} \lhd R$ is prime.
   (b) Show that $I \lhd R$ is prime iff R/I is an integral domain.
   (c) Show that R is a field iff (0) is its unique ideal (equivalently, a maximal ideal).
   (d) Use the correspondence theorem to show that I is maximal iff R/I is a field.
   (e) Show that every maximal ideal is prime.
   Hint: Every field is an integral domain.