## Lior Silberman's Math 501: Problem Set 9 (due 20/11/2020)

### Solubility by radicals

1. Solve the equation $t^6 + 2t^5 - 5t^4 + 9t^3 - 5t^2 + 2t + 1 = 0$ by radicals.
   Hint: Let $u = t + \frac{1}{t}$.

2. Let $K$ be a field of characteristic zero and consider the system of equations over the field $K(t)$:

$$\begin{cases} x^2 = y + t \\ y^2 = z + t \\ z^2 = x + t \end{cases} .$$

   (a) Let $(x, y, z)$ be a solution in a field extension of $K(t)$. Show that $x$ satisfies either $x^2 = x + t$ or a certain sextic equation over $K(t)$.
   OPT Use a computer algebra system to verify that the sextic is relatively prime both to $x^2 - x - t$ and to its own formal derivative.
   (b) Show that the Galois group of the splitting field of the sextic preserves an equivalence relation among its six roots.
   Hint: Find an permutation of order 3 acting on the roots. This is visible in the original system.
   (c) Let $\{\alpha, \beta, \gamma\}$ be an equivalence class of roots, and let $s(a, b, c)$ be a symmetric polynomial in three variables. Show that $s(\alpha, \beta, \gamma)$ belongs to an extension of $K(t)$ of degree 2 at most.
   Hint: If $s(\alpha, \beta, \gamma)$ is a root of a quadratic, what should the other root be? Show that the coe cients of the putative quadratic are indeed invariant by the Galois group.
   (d) Show that the system of equations can be solved by radicals.
   Hint: For each equivalence class construct a cubic whose roots are the equivalence class and whose coe cients lie in a radical extension.
   OPT Show that knowing $[K(t, x + y + z) : K(t)] = 2$ where $x, y, z$ are roots of the original system would have been enough.

### Zorn's lemma

This is set-theroetic preparation ahead of working with infinite extensions.
The powerset of a set $X$ is the set $\mathcal{P}(X) = \{A \mid A \subset X\}$ of subsets of $X$. $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.
A chain in $\mathcal{P}(X)$ is a subset $\mathcal{C} \subset \mathcal{P}(X)$ which is totally ordered by inclusion: for any $A, B \in \mathcal{C}$ we either have $A \subset B$ or $B \subset A$ (or both if $A = B$). If $\mathcal{F} \subset \mathcal{P}(X)$ we call $M \in \mathcal{F}$ maximal if it's maximal for inclusion: there is no $A \in \mathcal{F}$ so that $M \subsetneq A$.

THEOREM (Zorn's Lemma; equivalent to the Axiom of Choice). Let $X$ be a set, and let $\mathcal{F} \subset P(X)$ be a non-empty family of subsets of $X$. Suppose that $F$ is "closed under unions of chains": for any non-empty chain $\mathcal{C} \subset \mathcal{F}$ we have $\bigcup \mathcal{C} \in \mathcal{F}$. Then $\mathcal{F}$ has maximal elements.

3. Let $R$ be a ring, and let $\mathcal{F} \subset \mathcal{P}(R)$ be the set of proper ideals (together with the empty set).
   (a) Let $\mathcal{C} \subset \mathcal{F}$ be a chain of proper ideals and let $a, b \in \bigcup \mathcal{C}$. Show that there is $I \in \mathcal{C}$ so that $a, b \in I$.
   (b) Show that $\bigcup \mathcal{C}$ is an ideal.
   (c) Using the fact that an ideal is proper i it does not contain $1_R$, show that $\bigcup \mathcal{C}$ is a proper ideal.
   (d) Invoke Zorn's Lemma to show that every ring has maximal ideals.

4. Let $K$ be a field, and let $V$ be a $K$-vectorspace. Let $\mathcal{F} \subset \mathcal{P}(V)$ be the family of linearly independent subsets of $V$.
   (a) Let $\mathcal{C} \subset \mathcal{F}$ be a chain. Show that $\bigcup \mathcal{C}$ is linearly independent.
   (b) Invoke Zorn's Lemma to show that $V$ contains a maximal linearly independent set $B$.
   (c) Let $v \in V$. Show that $v \in \mathrm{Span}_K(B)$, in other words that $B$ is a basis (hint: the alternative contradicts the maximality of $B$).