AM 106: Applied Algebra **Prof. Madhu Sudan**

Problem Set 9

Assigned: Wed. Nov. 15, 2017 Due: Wed. Nov. 29, 2017 (8:00 AM)

- You may submit your solutions via assignment page on the canvas website of the course.
- For collaboration and late days policy, see course website at `http://madhu.seas.harvard.edu/courses/Fall2017`
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.

Problem 1. (Abstract Extension Fields [AM106]) Write out complete addition and multiplication tables for $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$. (Due to commutativity, you only need to write the upper-triangular portion of these tables, including the main diagonal.)

Problem 2. (Splitting Fields) Determine a splitting field $F \subseteq \mathbb{C}$ for the polynomial $x^3 - 2$ over $\mathbb{Q}$. Compute $[F : \mathbb{Q}]$ and describe a basis for F over $\mathbb{Q}$.

Problem 3. (Adjoining Two Square Roots) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is defined to be the smallest field containing $\mathbb{Q}$ and the elements $\sqrt{2}$ and $\sqrt{3}$. That is, it consists of all real numbers of the form $p(\sqrt{2}, \sqrt{3})/q(\sqrt{2}, \sqrt{3})$ where $p(x, y), q(x, y) \in \mathbb{Q}[x, y]$ are bivariate polynomials and $q(\sqrt{2}, \sqrt{3}) \neq 0$.

1. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
2. Determine $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$, and give a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. (Hint: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.)
3. Find the minimal polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. (Hint: write powers of $\sqrt{2} + \sqrt{3}$ in the basis you found above, and find a linear dependency.)
4. Find 3 distinct fields F such that $\mathbb{Q} \subsetneq F \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Problem 4. (Density of Irreducible Polynomials) Let $F = \mathbb{F}_q$, and $E = \mathbb{F}_{q^n}$ for some prime power q.

1. Show that every element $a \in E$ is the zero of an irreducible polynomial in $F[x]$ of degree dividing n.
2. Deduce that the number of monic irreducible polynomials in $F[x]$ of degree at most n is at least q^n/n, and the number of monic irreducible polynomials of degree exactly n is at least $q^n/n - q^{n/2}$.