AM 106/206: Applied Algebra **Prof. Salil Vadhan**

Problem Set 9

Assigned: Mon. Nov. 22, 2010 Due: Fri. Dec. 3, 2010 (2:10 PM sharp)

- You may submit your problem sets in the AM106 in the Maxwell–Dworkin basement, or electronically by email to `am106-hw@seas.harvard.edu`. If you use LaTeX, please submit both the source (`.tex`) and the compiled file (`.pdf`). Name your files `PS9-yourlastname`.
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.
- Problems marked [AM106] or [AM106-X] are for AM106 students (though AM206 students should confirm that they know how to do them), and those marked [AM206-X] are for AM206 students. However, AM106 students can do a problem marked [AM206-X] instead of one marked [AM106-X] (for the same value of X) if they wish (out of interest, or for a challenge). If you wish to keep the option of staying in either AM106 or AM206 open until add/drop date, then you should do all problems marked [AM106] and all problems marked [AM206-X].

Problem 1. (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 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. (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 4. (Bivariate Interpolation) Let F be a field and $F[x,y]^{m,n}$ denote the set of bivariate polynomials over $\mathbb{F}$ whose degree in x is at most m and whose degree in y is at most n.

1. What is the dimension of $F[x,y]^{m,n}$ as a vector space over F? Exhibit a basis for $F[x,y]^{m,n}$ over F.

2. Suppose $S \subseteq F^2$ is a set of fewer than $(m+1)(n+1)$ points in F^2. Show that there is a *nonzero* polynomial $p(x,y) \in F[x,y]^{m,n}$ such that $p(a,b) = 0$ for all $(a,b) \in S$. Explain how, given S, we could compute such a polynomial $p(x,y)$ using $\text{poly}(n+m)$ operations over F.