Kris Harper
MATH 25900
Quiz 2 April 14, 2010

Problem 1. *Prove no finite field is algebraically closed.*

Proof. Let F be a finite field with q elements $\{a_1, \ldots, a_q\}$. Let $n > 1$ and let $p(x) \in F[x]$ be a monic polynomial with degree n. For each $a_i \in F$ let $p_i(x) = p(x) + a_i$. Then we have a collection of q polynomials in $F[x]$ each identical except for a distinct constant term. If F is algebraically closed, then each of these polynomials has a root in F and for $i \neq j$, a root of $p_i(x)$ cannot be a root of $p_j(x)$ since they differ by $a_i - a_j$. Thus we have q distinct roots and q elements of F. The only way this can happen is if $p_i(x) = (x - a_j)^n$ where a_j is the root for $p_i(x)$. But this is impossible since n is greater than 1 and all the $p_i(x)$ are identical except for their constant terms. Thus, for example, the $n - 1$ term of each $p_i(x)$ is different in this case, contrary to our assumption. Therefore there must be at least one $p_i(x)$ which has no root in F. $\square$

Problem 2. *An algebraic number a is said to be an algebraic integer if it satisfies an equation of the form*

$$a^m + \alpha_1 a^{m-1} + \cdots + \alpha_m = 0$$

where $\alpha_1, \ldots, \alpha_m$ are integers.
(a) If a is any algebraic number, prove that there is a positive integer n such that na is an algebraic integer.
(b) If a is an algebraic integer and m is an ordinary integer, prove that $a + m$ is an algebraic integer.

Proof. (a) Since a is algebraic there exists some polynomial $p(x) \in \mathbb{Q}[x]$ such that $a^m + \alpha_1 a^{m-1} + \cdots + \alpha_m = 0$ and $\alpha_i \in \mathbb{Q}$. Now find the least common multiple of the α_i and call it n. Multiply our polynomial by n so we have $na^m + \beta_1 a^{m-1} + \cdots + \beta_m = 0$ where $\beta_i \in \mathbb{Z}$. Finally, multiply both sides by n^{m-1} so we have $n^m a^m + \beta_1 n^{m-1} a^{m-1} + \beta_2 n^{m-1} a^{m-2} + \cdots + \beta_m n^{m-1} = 0$. We can now pass the appropriate exponent of n inside each exponent of a for every term which results in the equation $(na)^m + \beta_1 (na)^{m-1} + \beta_2 n (na)^{m-2} + \cdots + \beta_{m-1} n^{m-2}(na) + \beta_m n^{m-1} = 0$. Since each $\beta_i n^{i-1}$ is an integer we see that na is an algebraic integer.

(b) Let a and b be any two algebraic integers. Then we can write $a^m = -\alpha_1 a^{m-1} - \cdots - \alpha_m$ and $a^{m+1} = -\alpha_1 a^m - \cdots - \alpha_m a$. Substituting the above equation in for a^m we see that a^{m+1} can be expressed as a polynomial with integer coefficients. Similarly, any power of a can be expressed as a linear combination of the elements $1, a, \ldots, a^{m-1}$. Likewise any power of b can be expressed as a linear combination of $1, b, \ldots, b^{n-1}$. Thus any polynomial in a and b can be expressed as a linear combination of the mn elements $a^i b^j$ for $0 \leq i \leq m-1$ and $0 \leq j \leq n-1$ with integer coefficients. Thus we can write $a + b = c_1 a^0 b^0 + c_2 a^1 b^0 + \cdots + c_{mn} a^{m-1} b^{m-1}$. We can now multiply both sides of this equation successively by $a^i b^j$ for $0 \leq i \leq m-1$, $0 \leq j \leq n-1$ and rewrite the righthand side as a linear combination of powers of a and b with integer coefficients. We then obtain mn equations

$$\begin{aligned}
(a+b)a^0b^0 &= c_1' a^0 b^0 + c_2' a^1 b^0 + \cdots + c_{mn}' a^{m-1} b^{n-1} \\
(a+b)a^1b^0 &= c_1'' a^0 b^0 + c_2'' a^1 b^0 + \cdots + c_{mn}'' a^{m-1} b^{n-1} \\
&\vdots \\
(a+b)a^{m-1}b^{n-1} &= c_1^{(mn)} a^0 b^0 + c_2^{(mn)} a^1 b^0 + \cdots + c_{mn}^{(mn)} a^{m-1} b^{n-1}.
\end{aligned}$$

Subtracting the left hand side we see that these have a nontrivial solution and so the corresponding matrix must have determinant zero. That is

$$\det \begin{pmatrix} c_1' - (a+b) & c_2' & \cdots & c_{mn}' \\ c_1'' & c_2'' - (a+b) & \cdots & c_{mn}'' \\ \vdots & \vdots & & \vdots \\ c_1^{(mn)} & c_2^{(mn)} & \cdots & c_{mn}^{(mn)} - (a+b) \end{pmatrix} = 0.$$

This determinant is a polynomial in $a + b$ with integer coefficients and leading coefficient ± 1 so $a + b$ must be an algebraic integer. But now it's easy to see that any integer b is an algebraic integer because it's the solution to $x - b$. $\square$