**Shashank Singh**
**sss1@andrew.cmu.edu**
**21-373 Honors Algebraic Structures, Fall 2011**
**Assignment 9**
**Due: Wednesday, November 30**

**Exercise 57:** Let $K$ be a finite field, and let $\forall a, b \in K$, if $a^2 = b^2$, then $(a+b)(a-b)$, so that $a = -b$. Therefore, if $x$ is a square in $K$, then there are at most two distinct elements of which $x$ is a square. Thus, if $n = |K|$, for $S = \{x^2 : x \in K\}$, $|S| \geq \lceil \frac{n+1}{2} \rceil$. Let $T = \{k - x : x \in S\}$. Then, $f(x) = k - x$ is an injection from $S$ to $T$, so that $|T| \geq \lceil \frac{n+1}{2} \rceil$. Therefore, since $S, T \subseteq K$, $S \cap T \neq \emptyset$ (for, if $S$ and $T$ were disjoint, then $|K| \geq n+1$, contradicting the choice of $n$). Then, for $x \in S \cap T$, $x = a^2$ and $k - x = b^2$, for some $a, b \in K$, so that $k = a^2 + b^2$.

**Exercise 58:** Let $E$ be a field, and let $F = E(x)$. Let $P, Q \in E[x]$ such that $P$ and $Q$ are relatively prime.

**i.** Let $n$ be the degree of $P$, and let $m$ be the degree of $Q$. For $R = \frac{P}{Q}Q - P$, $R \in E[x]$, and $R(x) = 0$. Thus, $x$ is algebraic over $E(\frac{P}{Q})$. Furthermore, since $[F : E(\frac{P}{Q})]$ is the degree of which $x$ is algebraic over $E(\frac{P}{Q})$ (as shown on the previous assignment), $[F : E(\frac{P}{Q})] \leq degree(R) = \max\{degree(P), degree(Q)\}$. It remains to show that $\frac{P}{Q}Q - P$ is irreducible, so that, since there is a unique monic, irreducible polynomial such of which $x$ is a root (and $R$ can be made monic be dividing by the coefficient of the leading term), $[F : E(\frac{P}{Q})] \geq degree(R)$.

**ii** Note that, since $P, Q$ are relatively prime, at least one is non-constant. Suppose $\max\{degree(P), degree(Q)\} = 1$. Then $\frac{P}{Q} = \frac{ax+b}{cx+d}$, for some $a, b, c, d \in E$. Thus, for $\tau(x) = \frac{b-dx}{cx-a}$, $\tau = \sigma^{-1}$. Thus, $\sigma$ is bijective, so that, since $\sigma$ is an endomorphism, $\sigma$ is an automorphism.

Suppose, on the other hand, that $\sigma$ is an automorphism. Since $\sigma$ maps $F$ to $E(\frac{P}{Q})$ and is bijective, $|F| \leq |E(\frac{P}{Q})$, so that, since $E(\frac{P}{Q}) \subseteq |F|$, $E(\frac{P}{Q}) = F$. Therefore, $[F : E(\frac{P}{Q})] = 1$, so that, by the result of part i., $\max\{degree(P), degree(Q)\} = 1$.

**Exercise 59:** Note that, in the scope of this exercise, $p$ denotes a prime integer. Clearly, $\nexists x \in \mathbb{Z}$ such that $x^2 = -1$, $x^2 = 2$, $x^2 = -2$, or $x^4 = -1$. Thus, since, as shown below, all factorizations of $x^4 + 1$ require the existence of some such element, $x^4 + 1$ is irreducible in $\mathbb{Z}$.

**i.** If $p = 2$, then, since $1 = -1$, 1 is a root of $x^4 + 1$.

**ii.** $(x^2 + b)(x^2 - b) = x^4 - b^2$. Thus, $x^4 + 1$ factors as $(x^2 + b)(x^2 - b)$ in $\mathbb{Z}_p$ if and only if $(-1)$ is a quadratic residue for $p$. Indeed, as given, since $p = 8n + 5 = 4(2n+1) + 1$, $(-1)$ is a quadratic residue for $p$, so, assuming $p$ is not of the form $8n + 1$, $x^4 + 1$ factors as $(x^2 + b)(x^2 - b)$ in $\mathbb{Z}_p$ if and only if $p = 8n + 1$ for some $n \in \mathbb{N}$.

**iii.** $(x^2 + ax + 1)(x^2 - ax + 1) = x^4 + (2 - a^2)x^2 + 1$. Thus, $x^4 + 1$ factors as $(x^2 + ax + 1)(x^2 - ax + 1)$ in $\mathbb{Z}_p$ if and only if 2 is a quadratic residue for $p$. Indeed, as given, since $p = 8n + 7 = 8(n+1) - 1$, 2 is a quadratic residue for $p$, so, assuming $p$ is not of the form $8n+1$, $x^4+1$ factors as $(x^2+ax+1)(x^2-ax+1)$ if and only if $p = 8n + 7$.

**iv.** $(x^2+ax-1)(x^2-ax-1) = x^4-(2+a^2)x^2+1$. Thus, $x^4+1$ factors as $(x^2+ax-1)(x^2-ax-1)$ if and only if $(-2)$ is a quadratic residue for $p$. The Legendre symbol of $(-2)$ shows that, since $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$, $-2$ is a quadratic residue of $p$ if and only if either both or neither of 2 and $(-1)$ are quadratic residues for $p$. Since $p$ is prime, for some $n \in \mathbb{N}$, $p = 8n+1$, $p = 8n+3$, $p = 8n+5$, or $p = 8n+7$. In the latter two cases, as shown above, one, but not both, of 2 and $(-1)$ is a quadratic residue for $p$. Thus, assuming $p$ is not of the form $8n + 1$, $x^2 + 1$ factors as $(x^2 + ax - 1)(x^2 - ax - 1)$ if and only if $p = 8n + 3$.

**Exercise 60:** **i.** Let $E$ be a field of characteristic 0, and suppose $P \in E[x]$ is such that $P(x^2 + 1) = (P(x))^2 + 1$ and $P(0) = 0$. Let $S = |\{x \in \mathbb{N} : P(x) = x\}|$. Suppose, for sake of contradiction, that, for some $n \in \mathbb{N}$, $|S| = n$. Let $k = \max S$. Then, $P(k^2 + 1) = P(k)^2 + 1 = k^2 + 1 \notin S$, contradicting the choice of $k$. Thus, there are infinitely many solutions $x$ to $P(x) = x$, so that $(P - x)$ has infinitely many roots. Since the number of roots of a non-zero polynomial is bounded by the degree of the polynomial, then, $(P - x) = 0$, so that $P - x$.

**ii.** Let $E$ be a field of characteristic $p$. Clearly, for $P = x$ (the "trivial solution"), $P \in E[x]$ satisfies $P(x^2+1) = (P(x))^2+1$ and $P(0) = 0$. Suppose that, for some $P \in E[x]$, $P$ satisfies $P(x^2+1) = (P(x))^2+1$ and $P(0) = 0$. As shown in class, since $E$ is a finite field (as it is of positive characteristic), the Frobenius homomorphism on $E$ is an automorphism on $E$, so that it is bijective. Thus, if $f$ is the Frobenius homomorphism on $E$, $P(f(x)) = P(x^p)$ satisfies $P(x^2+1) = (P(x))^2+1$ and $P(0) = 0$. Furthermore, $P(f(f(x))), P(f(f(f(x)))), \ldots, P(f^i(x)), \ldots$ all satisfy the constraint, so that there are an infinite number of solutions $P \in E[x]$ to the constraint.

**Exercise 61:** Let $n \in \mathbb{N}$ with $n \geq 2$. It is easily shown by induction on $n$ that $(x + x^{n+2})(1 - x^{n+1} + x^{2(n+1)} - \ldots + (-1)^n (x^{n+1})^{n-2}) + (-1)^{n+1}(x^{n^2})$. Thus, for $P(x,y,z) = z(1 - y + y^2 - \ldots + (-1)^n y^{n-2}) + (-1)^{n+1}x^2$, $x \equiv P(x^n, x^{n+1}, x + x^{n+2})$.

**Exercise 62:** Let $n, m \in \mathbb{N}$ with $n = 2m$ and $m > 1$ is odd, and let $\theta = e^{2\pi i/n}$. Then, $\theta^m + 1 = e^{\pi i} + 1 = 0$. It is easily shown by induction that, $\forall x \in \mathbb{C}$, $\forall k \in \mathbb{N}$, if $k$ is odd, then $x^k = (x+1)\left(\sum_{i=1}^{k}(-1)^{i+1}x^{k-i}\right)$. Thus, $\theta^m = (\theta+1)\left(\sum_{i=1}^{m}(-1)^{i+1}\theta^{m-i}\right)$. Since $\theta \neq -1$ (as $m > 1$), $0 = \sum_{i=1}^{m}(-1)^{i+1}\theta^{m-i}$ and thus $1 = \sum_{i=1}^{m-1}(-1)^{i}\theta^{m-i}$. $1 = \sum_{i=1}^{m-1}(-1)^{i}\theta^{m-i}$.

Separating even and odd terms gives $1 = (1-\theta)(\sum_{i=0}^{\frac{m-3}{2}} \theta^{2i+1})$. Thus, $(1-\theta)^{-1} = (\sum_{i=0}^{\frac{m-3}{2}} \theta^{2i+1})$.