M3P8 DISCUSSION PROBLEMS 2

These problems are for discussion in lecture and will NOT be assessed. They are somewhat more difficult than typical assessed coursework problems; do not get discouraged if it is not immediately clear how to approach them. Working on these in groups with your fellow students and trading ideas and approaches is HIGHLY encouraged!

If you have difficulty getting complete solutions to any particular problem it might be helpful to: work out some examples, try to find partial results in special cases, identify related, easier questions, etc. If all else fails, I am happy to give hints in office hours!

1. Let K be a field, and $f(X) \in K[X]$ an irreducible polynomial of degree n. Let $g(X)$ be any polynomial in $K[X]$. Show that every irreducible factor of the polynomial $f(g(X))$ has degree divisible by n.

2. Find the minimal polynomials of $\sqrt{2} + \sqrt{3}$ and $1 + 2^{\frac{1}{3}} + 4^{\frac{1}{3}}$ over $\mathbb{Q}$.

3a. Let q be a prime power, and let $P(X)$ be an irreducible polynomial of degree d in $\mathbb{F}_q[X]$. Show that $P(X)$ divides $X^{q^d} - X$ in $\mathbb{F}_q[X]$.

3b. Show conversely that if $P(X)$ is an irreducible factor of $X^{q^d} - X$, then the degree of $P(X)$ divides d.

3c. Show that $X^{q^d} - X$ has no repeated factors in $\mathbb{F}_q[X]$. Conclude that $X^{q^d} - X$ is the product of all the irreducible monic polynomials in $\mathbb{F}_q[X]$ of degree dividing d.

3d. You can use this to factor polynomials easily over finite fields: given a polnyomial $P(X)$ in $\mathbb{F}_q[X]$, you can take its GCD with $X^{q^r} - X$, for varying r. This is fast to compute via Euclid's algorithm. This lets you find factors of $P(X)$ quickly. Use this technique to factor the polnyomial:

$$X^7 + X^5 + X^4 + X^2 + 1$$

in $\mathbb{F}_2[X]$.

4. An element e of a ring R is *idempotent* if $e^2 = e$. A nonzero idempotent e is *primitive* if for any other idempotent e', one has $ee' = 0$ or $ee' = e$. We will call a ring R with no idempotents other than 0 and 1 *indecomposable*.

4a. Let e be an idempotent element of R, not equal to 0 or 1. Show that we have isomorphisms: $R/\langle 1-e \rangle \cong eR$ and $R/\langle e \rangle \cong (1-e)R$. Show further that the map:

$$R \to eR \times (1-e)R$$

defined by $x \mapsto (ex, (1-e)x)$ is an isomorphism of rings.

4b. Show that an idempotent e is primitive if, and only if, eR is indecomposable.

4c. Show that an idempotent e is primitive if, and only if, e cannot be expressed as a sum $e_1 + e_2$, where e_1, e_2 are nonzero idempotents and $e_1 e_2 = 0$.

4d. How many idempotents are there in $\mathbb{Z}/n\mathbb{Z}$? How many are primitive?

5a. Let $P(X)$ be an irreducible polynomial in $\mathbb{F}_q[X]$ of degree d. Let α be a root of $P(X)$ in some extension L of $\mathbb{F}_q$. Show that $P(X)$ factors in L as $(X-\alpha)(X-\alpha^q)\dots(X-\alpha^{q^{d-1}})$.

5b. Let $P(X)$ be as in part a, and let r be a positive integer. Let e be the greatest common divisor of d and r. Show that in $\mathbb{F}_{q^r}[X]$, the polynomial $P(X)$ factors into e irreducible factors, each of degree $\frac{d}{e}$.

5c. Show that for any $a \in \mathbb{F}_q$, the polynomial $X^q - X - a$ either factors into linear factors, or as a product of irreducible factors of degree p, where p is the characteristic of $\mathbb{F}_q$.