MA362
Sathaye

Final Take home exam **Fall 2019**

- This exam is due on Monday December 16. You may bring it to my office or drop it in my mailbox. Since our final exam is scheduled for 1 PM, I would expect your exam no later than 3 PM on that day.
- I would recommend that you start work on these problems right away. You may ask me for clarification and small amount of help. Other than that, I expect that you work on your own and not make it a group project(:-))
- Please write clearly and arrange all answers in order. Be sure to start new problems on new pages.
- **Notation** In the following F shall be a base field. It will have characteristic p where p is allowed to be zero. L will generally be an extension field of F. We set

$$g(x) = x^2 + ax + b$$

to be a quadratic polynomial in $F[x]$, where a, b are unspecified elements of F to be determined later.

Q.1. Preliminary set up.

1. The polynomial $g(x)$ in $F[x]$ is irreducible iff $g(x)$ has no root in F.
2. If the characteristic p is not 2, then this (irreducibility) is equivalent to $a^2 - 4b$ not having a square root in F.
3. If $p \neq 2$ then the roots of $g(x)$ are given by the usual quadratic formula. State and prove the formula.
4. If $p = 2$, then given one root to be u, the other can be written as $(u + a)$. Prove this.
   there is no known **formula** for u itself. Think about why this should be so and comment.

From now on, assume that F is Z_p the prime field of characteristic p with $p \neq 2$.

Q.2. Finite fields properties.

1. Suppose that $[L : F] = n$ where $n \geq 1$. Prove that the number of elements of L is exactly p^n. Prove that $x^{p^n} = x$ for all $x \in L$.
2. Deduce that the map $\sigma(u) = u^p$ is an isomorphism of L into itself. Moreover the field F is exactly those elements of L which are fixed by σ.

   Hint It will be helpful to use that $L^\times = L \setminus 0$ is a cyclic group under multiplication.
3. Recall that any element of F satisfies the equation $X^p = X$. Deduce that any element of L satisfying this equation must be in F.
4. Prove that if u is any root of (the above defined polynomial) $g(x)$, then so is u^p. Deduce that $g(x) = (x-u)(x-u^p)$.
5. Assume that $g(x)$ is irreducible in $F[x]$ and let u be any root of $g(x)$ in L. Consider the set $E = \{au + b \mid a, b \in F\}$ contained in L. Prove that E is a field. **Hint: Think of** $F[x]/(g(x))$**.**
6. Prove that every element of E satisfies the equation $X^{p^2} = X$.
7. Prove that every element of L satisfying the equation $X^{p^2} = X$ must be in E.
8. Deduce that if $\alpha \in L$ is a root of any irreducible quadratic polynomial over F, then α is in E. Thus, if you adjoin the roots of one irreducible quadratic equation, then you suddenly have roots for all quadratic equations!

   Do you recall another field (of characteristic zero, this time) which has such a property?
9. Prove that the field of rational numbers Q does not have this property.

Q.3. Quadratic extensions.

1. Returning to the field $F = Z_p$ with $p \neq 2$, suppose that we have a polynomial $h(x)$ over F such that $h(x)$ factors completely into a product of irreducible quadratic or linear polynomials over F.

   Use the above to deduce that $x^{p^2} - x$ is divisible by every irreducible factor of $h(x)$. In particular, if $h(x)$ has no repeated factors, then $x^{p^2} - x \equiv 0 \bmod h(x)$.

2. Now prove the converse that if the polynomial $h(x)$ divides $x^{p^2} - x$ then $h(x)$ is a product of linear polynomials or irreducible quadratics.

3. Prove that the polynomial $x^4 + 1$ divides $x^{p^2} - x$ for all choices of the characteristic p. **Hint: Calculate $x^{p^2} - x$ modulo $x^4 + 1$ by replacing x^4 by -1 repeatedly as needed! Try small values of p before attempting the full proof. Your argument in the general case will depend of whether $p = 4k + 1$ or $p = 4k + 3$ or $p = 2$.**

4. Conclude that the polynomial $x^4 + 1$ is reducible modulo every prime p (including $p = 2$) but it is irreducible over Q. This shows that the idea of reduction mod p does not always help to prove irreducibility!

Q.4. Extension to the cubic case.

1. Prove that a cubic polynomial in $F[x]$ either has a root in F or it is irreducible.

2. Using the facts deduced above, prove that $x^{p^3} - x$ is a product of linear, and cubic irreducible polynomials. Deduce that there must be irreducible polynomials of degree 3 in $F[x]$.

3. Generalize to argue that $F[x]$ contains irreducible polynomials of any desired degree n. Moreover, the polynomial $x^{p^n} - x$ is a product of all irreducible polynomials whose degree divides n.