MA362
Sathaye Homework 3 Due 10/28/19

This is a mixture of homework and exam practice. Only the problems marked with a * are to be submitted as homework. Others will be discussed in class.

1. * **5 pts.** For each of the following field extensions, determine a basis and hence its dimension.
   - $Q(\sqrt{2})$ over Q.
   - $Q(\sqrt{2})$ over $\Re$
   - $\boldsymbol{Q(\sqrt[4]{2})}$ over $\boldsymbol{Q}$.
2. * **8 pts.** Let $h : \boldsymbol{Z}_2[X] \to \boldsymbol{Z}[2_2[X]]/(X^2 + X + 1)$ be the canonical homomorphism and let $h(X) = \alpha$. Find the following minimum polynomials.
   - $Irr(\alpha, \boldsymbol{Z}_2)$.
   - $Irr(\alpha + 1, \boldsymbol{Z}_2)$.
   - $Irr(\alpha^2, \boldsymbol{Z}_2)$.
   - $Irr(5, \boldsymbol{Z}_2)$.
3. * **6 pts.** Let $F = Q(\pi)$.
   - Explain why $\zeta = \pi^2 + \pi + 1$ is algebraic over F. Determine $Irr(\zeta, F)$.
   - Determine $Irr(\pi, Q(\pi^5))$
   - Determine $Irr(\pi, Q(1 + \pi^5))$
4. * **6 pts.** Answer the following.
   - Prove or disprove that $I = (X + Y + Y^2)$ is a prime ideal in $Q[X, Y]$.
   - Prove or disprove that $J = (X^2 - Y^4)$ is a prime ideal in $Q[X, Y]$.
5. * **5pts** Answer the following.
   - Determine the quotient ring $Q[X, Y]/(X - 1, Y - 2)$. Is it a field?
   - Determine the quotient ring $Q[X, Y]/(X^2 - 1, Y - 2)$. Is it a field?

For practice, may be expanded.

1. Let $F = X^5 - YX^2 + Y$ and $R = Q[Y][X]$.

   Prove that $F \in R$ is irreducible.

   Hint: First prove that $(Y) \in Q[Y]$ is a prime ideal. Then an Eisenstein type criterion exists for (Y). Use it.
2. Let α be a root of F in some extension field of $qt(R)$ the quotient field of R. Prove that $[qt(R)(\alpha) : qt(R)] = 5$.

   Determine a basis for $qt(R)(\alpha)$ over $qt(R)$.

   Hint: Observe that F is a polynomial satisfied by α over $qt(R)$. Argue that F is irreducible and hence is $Irr(\alpha, qt(R))$
3. Let α be a root of a polynomial $f(X) = \sum_0^m a_i X^i$ where all a_i are in $K = GF(27)$.

   Answer the following:

   (a) Let σ denote the Frobenius automorphism $\sigma(z) = z^3$. Let $K = GF(3)$.
   Explain why $\sigma(z) = z$ if $z \in GF(3) \subset K$.

   (b) Explain why $\sigma(z) \neq z$ if $z \notin GF(3)$.

   (c) Prove that $\sigma^3(z) = z$ for all $z \in K$.

(d) **Idea of argument:** Note that $K^\times = K - 0$ is a cyclic group of order $3^3 - 1 = 26$.
Hence $z^{26} = 1$ or $z^{27} - z = 0$ for all $z \in K$.
Argue that the elements of $GF(p^n)$ are exactly all possible roots of $X^{p^n} - X$. This should answer all remaining questions.

4. Suppose that $I \subset Q[X, Y]$ is the ideal $I = (X - a, Y - b)$, where $a, b \in Q$. Explain why $f(X, Y) \in I$ if and only if $f(a, b) = 0$.

   Prove that I is maximal thus: Let $f \notin I$. Then $f(a, b) = t \neq 0$. Show that $g = f - t$ is in I and hence f is a unit modulo I. **Hint:** Let $s \in Q$ where $st = 1$. Let $g(X, Y) = s$. Prove that $fg = 1 \pmod{I}$.

   How does this finish the proof?

5. Construct a polynomial f of degree 23 in $Q[X]$ such that f is irreducible and has at least four different terms.

   Answer the same question where $f = f_1 f_2$ where each f_1, f_2 are irreducible with four different terms.

6. Answer if the statements are true or false. If they are false, then you must give an example.

   - A finite extension of any field is finite.
   - $C(x)$ is algebraically closed for any x in an extension field of C provided $x \notin C$.
   - Let $F \subset G$ be finite fields. Then F, G have the same characteristic, p. Moreover, if $p > 0$ then $\log_p(|F|)$ divides $\log_p(|G|)$.
   - Suppose that F is a finite field and u, v are two elements in an extension field E of F. Suppose that $[F(u) : F] = [F(v) : F] = n$ where $n \geq 1$ is an integer. Then $[F(u, v) : F] = n^2$.

Last edited November 10, 2019