NAME (print): KEY

Math 494 Spring 2007—Exam 1

Instructor: J. Shapiro

Please work neatly and write the problems in the space provided. Remember I cannot grade what I cannot read!

[30pts] 1. Define the following terms (in the first three questions R is an integral domain and $a, b \in R$):

See the text for the definitions

(a) a and b are associates.

(b) a is irreducible.

(c) a is prime.

(d) A perfect field.

(e) The splitting field of a polynomial.

[16pts] 2. Give examples of the following:

(a) Fields $F \subset E$ and $a \in E$, such that a is the root of an irreducible polynomial $f(x) \in F[x]$, yet $F(a)$ does not contain all the roots of $f(x)$.

Let $F = \mathbb{Q}$ and $E = \mathbb{C}$. Let $f(x) = x^3 - 2$ and $a = \sqrt[3]{2}$. Then the other two roots of $f(x)$ are imaginary and hence they are not in $\mathbb{Q}(\sqrt[3]{2})$.

(b) Fields $F \subset E$ and $a \in E$, such that a is the root of an irreducible polynomial $f(x) \in F[x]$, and $F(a)$ does contain all the roots of $f(x)$.

Let $f(x) = x^2 - 2$. Then the two roots of $f(x)$ are $\pm\sqrt{2}$. Clearly both roots are in $\mathbb{Q}(\sqrt{2})$.

[10pts] 3. Let $f(x) = x^2 + x + 2 \in \mathbb{Z}_3$ and let a be a root of $f(x)$ in some extension field of $\mathbb{Z}_3$. Find a^{-1} as a linear combination of x and 1 over $\mathbb{Z}_3$.

We know that a satisfies $a^2 = -a - 2 = 2a + 1$. We want an element of the from $xa + y$ such that $a(xa + y) = 1$. Thus $xa^2 + ay = 1$. But $xa^2 = x(2a + 1)$, so $xa^2 + ay = x(2a + 1) + ay = a(2x + y) + x = 1$. The coefficient of a must be zero. Hence $2x + y = 0$ and $x = 1$. Thus $y = 1$. Hence $a^{-1} = a + 1$.

[10pts] 4. Let E be an extension field of F. Let $a, b \in E$ and suppose that $[F(a) : F] = p$ and $[F(b) : F] = q$, where p and q are distinct prime numbers. What is $[F(a, b) : F]$? Justify your answer!

Everyone got this right.

[24pts] 5. Answer the following True or False and give either a brief proof or give a counterexample to show that it is false.

(a) A field with 3^5 elements contains only one subfield.

TRUE Subfields of a field of order p^n correspond to divisors of n. Since n is prime in this case, the only proper subfield corresponds to $n = 1$; the subfield is $\mathbb{Z}_p$.

(b) In an integral domain, the product of a unit and an irreducible is an irreducible

TRUE. Let a be an irreducible and let u be a unit. Suppose that ua factors, say $ua = bc$. Then $a = (u^{-1}b)c$. Since a is irreducible, either $u^{-1}b$ or c is a unit. If c is a unit, then bc is a trivial factorization of ua. If $u^{-1}b$ is a unit, then so is b (since b divides $u^{-1}b$). Again bc is a trivial factorization of ua. Thus ua is irreducible.

(c) The polynomial $f(x) = x^3 + x^2 + x + 3$ is irreducible over $\mathbb{Z}_7$.

FALSE. We just plug the elements of field into the polynomial $f(x)$. It is irreducible iff none of the elements are are root of $f(x)$. But

$$f(3) = 3^3 + 3^2 + 3 + 3 = 27 + 9 + 3 + 3 = 42 \equiv 0 \bmod 7$$

Thus $f(x)$ is reducible.

[10pts] 6. Let $f(x) \in F[x]$ with deg $f(x) = n$, show that the splitting field for $f(x)$ over F has degree at most $n!$.

We induct on n. Clearly its true if $n = 1$. Assume true if the degree of $f(x)$ is less than n. Let E be a splitting field of $f(x)$. Let $a \in E$ be a root of $f(x)$. Then $[F(a) : F] \leq n$ (if $f(x)$ is irreducible, then it is exactly n. Otherwise, a is a root of some factor of f, and so there is strict inequality). Thus over $F(a)$, $f(x) = (x - a)g(x)$, where deg $g(x) = n - 1$. Then E is a splitting field for $g(x)$ over $F(a)$. So by induction, $[E : F(a)] \leq (n-1)!$. Thus $[E : F] = [E : F(a)][F(a) : F] \leq (n-1)!n = n!$ - done.