SAMPLE MIDTERM I

MATH 4140

DATE

Name | _____

Please answer the all of the questions, and show your work.

Date: October 8, 2012.

1
10 points

1 . Let R be a ring (commutative with unity $1 \neq 0$) and let S be any subset of R. Show that the subset

$$A := \{r \in R : rs = 0 \text{ for all } s \in S\}$$

is an ideal.

SOLUTION:

We will show that A is a subgroup of R, and that it is closed under multiplication by elements of R. To show that A is a subgroup, it suffices to check that if $a_1, a_2 \in A$, then $a_1 - a_2 \in A$. To check this, we observe that for any $s \in S$

$$(a_1 - a_2)s = a_1 s - a_2 s = 0 - 0 = 0,$$

and thus $a_1 - a_2 \in A$.

Now we will show that A is closed under multiplication by elements of R. Indeed, let $a \in A$ and $r \in R$. Then for any $s \in S$ we have

$$(ra)s = r(as) = 0,$$

proving the claim. Thus the set A is a subgroup of R closed under multiplication by elements of R, and so it is an ideal of R.

2
10 points

2 . Consider the number $\alpha := \sqrt{2 - \sqrt[3]{5}} \in \mathbb{R}$.

2 (a). Show that α is algebraic over $\mathbb{Q}$ by finding a polynomial $p(x) \in \mathbb{Q}[x]$ such that $p(\alpha) = 0$.

2 (b). Find the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

SOLUTION:

For part (a), we start with the observation that

$$\alpha = \sqrt{2 - \sqrt[3]{5}} \iff \alpha^2 = 2 - \sqrt[3]{5} \iff \ldots \iff \alpha^6 - 6\alpha^4 + 12\alpha^2 - 3 = 0.$$

Thus the $p(x) = x^6 - 6x^4 + 12x^2 - 3$ is a solution to part (a).

For part (b), we use Eisenstein's Criterion to determine that $p(x)$ is irreducible. Consequently, the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$.

3
10 points

3 . Show that the field $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$ is algebraic over $\mathbb{Q}$, but not finite.

SOLUTION:

To show that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$ is algebraic over $\mathbb{Q}$ we must show that each

$$x \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$$

is algebraic over $\mathbb{Q}$. Since $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots) = \bigcup_{n\in\mathbb{N}} \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \ldots, \sqrt[n]{2})$, we must have $x \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \ldots, \sqrt[n]{2})$ for some n, and it then suffices to show that $\sqrt[n]{2}$ is algebraic over $\mathbb{Q}$ for each n. This is clear since $\sqrt[n]{2}$ is a root of the polynomial $x^n - 2 \in \mathbb{Q}[x]$.

We now show that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$ is not finite over $\mathbb{Q}$. Pursuing a proof by contradiction, assume that $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots) : \mathbb{Q}] = m$ for some $m \in \mathbb{N}$. Then take a natural number $n > m$. By Eisenstein's Criterion, $x^n - 2 \in \mathbb{Q}[x]$ is irreducible, and so $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. On the other hand, since $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$, we have

$$n = [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] | [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots) : \mathbb{Q}] = m,$$

which is a contradiction since $n > m$ and so it can not divide m. Thus $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$ could not have been finite over $\mathbb{Q}$.

4
10 points

4 . Suppose that $p(x) \in F[x]$ is an irreducible polynomial and E is a finite extension field of F. If $\deg p(x)$ and $[E : F]$ are relatively prime, show that $p(x)$ is irreducible over E.

SOLUTION:

Let $\bar{E}$ be some algebraic closure of E, and let $\alpha \in \bar{E}$ be some root of the polynomial $p(x)$. Then we consider the extension $E(\alpha)$ over F. There are two subfields of $E(\alpha)$ of interest: $F(\alpha)$ and E. The first observation is that

$$[E(\alpha) : E] \leq [F(\alpha) : F]$$

since $p(x)$ is certainly a polynomial with coefficients in E of which α is a root. Then comparing extensions we have

$$[E(\alpha) : E][E : F] = [E(\alpha) : F(\alpha)][F(\alpha) : F].$$

But we are given that $[E : F]$ is relatively prime to $[F(\alpha) : F]$ and so it must then follow that $[E : F]|[E(\alpha) : F(\alpha)]$ and in particular that

$$[E : F] \leq [E(\alpha) : F(\alpha)].$$

The equality above is only possible if each of the inequalities above is an equality. In particular we must have $[E(\alpha) : E] = [F(\alpha) : F]$, and it follows that $p(x)$ is irreducible over E.

5
10 points

5 . Let E be an extension field of a field F. Let $\alpha \in E$ be an element with $\alpha \notin F$. Show that multiplication by α induces a linear automorphism of E as a vector space over F. I.e.

$$\phi : E \to E$$

by

$$x \mapsto \alpha x.$$

Show that this is *not* an automorphism of E as a field.

SOLUTION:

To show that ϕ is a linear automorphism we must show that it is a linear map, with an inverse.

To show that it is a linear map, we must show that $\phi(x+y) = \phi(x)+\phi(y)$ for all $x, y \in E$, and that $\phi(\lambda x) = \lambda\phi(x)$ for all $x \in E$ and all $\lambda \in F$.

Let us check this now. Let $x, y \in E$. Then

$$\phi(x + y) = \alpha(x + y) = \alpha x + \alpha y = \phi(x) + \phi(y).$$

Similarly, let $x \in E$ and $\lambda \in F$. Then

$$\phi(\lambda x) = \alpha(\lambda x) = \lambda(\alpha x) = \lambda\phi(x).$$

The inverse of ϕ is given by the map $x \mapsto \alpha^{-1}x$ ($\alpha \notin F$ implies in particular that $\alpha \neq 0$). One can check in the same way that this is a linear map. Thus we have checked that ϕ is a linear automorphism of E.

This is not a ring homomorphism. Indeed, we have $\phi(1) = \alpha \neq 1$ since α is not in F. (You can also check that $\phi(xy) \neq \phi(x)\phi(y)$.)

6
10 points

6 . Show that $x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{Z}_p[x]$ of a degree d dividing n.

SOLUTION:

Fix an algebraic closure $\bar{\mathbb{Z}}_p$ of $\mathbb{Z}_p$. Let $\mathbb{F}_{p^n}$ be the subfield with p^n elements; we have proven a theorem that these are exactly the roots in $\bar{\mathbb{Z}}_p$ of the polynomial $x^{p^n} - x$. We will also want to use the following claim: $d|n$ if and only if $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$. We will give a proof of the claim at the end. For now we will use the claim to give a solution to the problem.

Step 1: If $f(x)$ is a monic irreducible polynomial of degree d dividing n, then $f(x)$ divides $x^{p^n} - x$.

To prove this, let $f(x)$ be a monic irreducible polynomial of degree d dividing n, and let $\alpha \in \bar{\mathbb{Z}}_p$ be a root. We have $|\mathbb{Z}_p(\alpha)| = p^d$; thus $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^d}$, and so $\mathbb{Z}_p(\alpha) \subseteq \mathbb{F}_{p^n}$ (since $d|n$). In particular, α is also a root of $x^{p^n} - x$, and so by definition of the irreducible polynomial, $f(x)$ divides $x^{p^n} - x$, proving Step 1.

Step 2: If $f(x)$ is a monic irreducible polynomial dividing $x^{p^n} - x$ then $d|n$.

Indeed, suppose that $f(x)$ is a monic irreducible polynomial dividing $x^{p^n} - x$. Say the degree of $f(x)$ is equal to d. We have seen that $f(x)$ defines a degree d extension $\mathbb{F}(\alpha)$ of $\mathbb{Z}_p$, for some $\alpha \in \bar{\mathbb{Z}}_p$. The order of $\mathbb{F}(\alpha)$ is p^d, and thus the extension is equal to $\mathbb{F}_{p^d}$. Now α is a root of $f(x)$, which divides $x^{p^n} - x$, and thus α is a root of $x^{p^n} - x$. Thus $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$, and so $d|n$.

Step 3: Finishing the proof.

From Steps 1 and 2 it follows that the irreducible monic polynomials dividing $x^{p^n} - x$ are exactly the irreducible monic polynomials of degree $d|n$. Let $f_1, \ldots, f_N$ be these irreducible monic polynomials of degree $d|n$. Since $\mathbb{Z}_p[x]$ is a UFD, it follows that

$$x^{p^n} - x = \prod_{i=1}^{N} f_i^{a_i}$$

for some natural numbers $a_1, \ldots, a_N$. In fact, the a_i are all equal to 1, since we have proven a theorem that the polynomial $x^{p^n} - x$ has no multiple roots. This completes the proof, up to the claim we made at the beginning.

Step 4: The proof of the Claim.

Recall that we used the claim: $d|n$ if and only if $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$. We prove this now. We start by proving the "if" implication ($\Longrightarrow$). So assume $d|n$. We observe that the elements of $\mathbb{F}_{p^d}$ are exactly the roots of $x^{p^d} - x$. Now let $\alpha \in \mathbb{F}_{p^d}$. We will show that $\alpha \in \mathbb{F}_{p^n}$. Indeed,

$$\alpha^{p^n} - \alpha = \underbrace{\left((\alpha^{p^d})^{p^d} \ldots\right)^{p^d}}_{n/d \text{ times}} - \alpha = \alpha - \alpha = 0,$$

proving that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$.

For the proof of the other direction of the claim ($\Longleftarrow$), we start by assuming $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$. Now, since $n = [\mathbb{F}_{p^n} : \mathbb{Z}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}][\mathbb{F}_{p^d} : \mathbb{Z}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}]d$ it follows that $d|n$.