MATH 120B MIDTERM EXAM SOLUTIONS (YELLOW PAPER)

SPRING 2015

Problem 1 (12 points).

T (F) "There is a field of characteristic 4." False: the characteristic of any integral domain is prime, as we proved in class.

(T) F "If D is an integral domain, then there is a field F and an injective homomorphism from D to F." True: there is an injective homomorphism from any integral domain D to its field of quotients.

(T) F "If p is a prime number and $a \in \mathbb{Z}$ is not divisible by p, then $a^{\varphi(p)} \equiv 1 \pmod{p}$." True by Fermat's little theorem, because $\varphi(p) = p - 1$ when p is prime.

(T) F "If D and D' are integral domains and $\phi : D \to D'$ is a nontrivial homomorphism, then $\phi(1_D) = 1_{D'}$." True: Any homomorphism maps idempotent elements (such as 1_D) to idempotent elements, and the only idempotent elements of D' are $0_{D'}$ and $1_{D'}$ because D' is an integral domain. Therefore $\phi(1_D) = 1_{D'}$, because if $\phi(1_D) = 0_{D'}$ then ϕ would be trivial.

T (F) "Let S be a set and let f be a function from S to S. If f is injective, then it is surjective." False: the function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(n) = n + 1$ is injective but not surjective.

(T) F "If $(F, +, \cdot)$ is a field and F^* is the set of nonzero elements of F, then $(F^*, \cdot)$ is a group." True: the units of a ring always form a group under multiplication (the group of units) and the units of a field are precisely its nonzero elements.

(T) F "There is a surjective homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_6$." True: there is a canonical homomorphism defined by $\phi(a) = a \bmod 6$.

T (F) "Let K be a field and let $f(x) \in K[x]$. If $f(\alpha) = 0$ for all $\alpha \in K$, then $f(x)$ is the zero polynomial." False. For example, consider $x^p - x$ in $\mathbb{Z}_p[x]$ where p is a prime. More generally, for any finite field $F = \{a_1, \ldots, a_n\}$ consider the polynomial $(x - a_1) \cdots (x - a_n) \in F[x]$.

Ⓣ F "If K is a field and $f(x), g(x) \in K[x]$ are nonzero then the degree of $f(x)g(x)$ is $\deg f(x) + \deg g(x)$." True. We proved this in class more generally for integral domains. The point is that the leading coefficients are not zero divisors.

Ⓣ F "If D is an integral domain then the polynomial ring $D[x]$ is an integral domain." True. We proved this in class. Also, this follows from the answer to the previous question.

T Ⓕ "Let K be a field and let $f(x) \in K[x]$ be nonzero. The number of roots of $f(x)$ is equal to $\deg f(x)$." False: for example, consider $x^2 + 1$ or $x^2 - 2$ in $\mathbb{Q}[x]$.

Ⓣ F "Every finite integral domain is a field." True. We proved this in class using problem 4 from homework set 2.

Problem 2 (4 points). Give the requested definitions.

(a) What is a *field*?

A field is a commutative ring with unity $1 \neq 0$ in which every nonzero element is a unit.

Alternatively, a field is a commutative division ring. (Of course, you should still know the definition of a division ring.)

A remark: it is not necessary to add the property of having no zero divisors. In a ring with unity $1 \neq 0$, a unit cannot be a zero divisor.

(b) What is an *idempotent* element of a ring?

An idempotent element of a ring R is an element $a \in R$ such that $a^2 = a$.

Problem 3 (4 points). Let R and R' be rings with unity 1 and $1'$ respectively, let $\phi : R \to R'$ be a homomorphism, and let $a \in R$.

(a) Prove that if $\phi(1) = 1'$ and a is a unit, then $\phi(a)$ is a unit.

If a is a unit in R, then it has an inverse a^{-1} in R. We have

- $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1) = 1'$, and
- $\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(1) = 1'$,

so $\phi(a)$ is a unit in R'.

A remark. It really is necessary in the definition of "unit" to multiply on both sides, as the following example shows. Let $M_\infty(\mathbb{Z})$ denote the set of infinite matrices with entries in $\mathbb{Z}$, meaning matrices A that have entries $a_{i,j}$ for all $i, j \in \mathbb{N}$. This is a ring under the usual operations of matrix addition and multiplication. Define the matrices $A, B \in M_\infty(\mathbb{Z})$ by

$$A = \begin{pmatrix} 0 & 1 & & & & \\ & 0 & 1 & & & \\ & & 0 & 1 & & \\ & & & 0 & \ddots & \\ & & & & \ddots & \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & & & & & \\ 1 & 0 & & & & \\ & 1 & 0 & & & \\ & & 1 & 0 & & \\ & & & \ddots & \ddots & \end{pmatrix},$$

where the diagonals that are not shown consist entirely of zeroes. Let I denote the multiplicative identity element, which has ones on the main diagnonal and zeroes elsewhere, as usual. Then $AB = I$ but $BA \neq I$, and in fact neither A nor B is a unit of $M_\infty(\mathbb{Z})$.

(b) Give an example where $\phi(1) \neq 1'$ and a is a unit, but $\phi(a)$ is not a unit.

Consider $R = \mathbb{Z}$ and $R' = \mathbb{Z} \times \mathbb{Z}$ with the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by $\phi(a) = (a, 0)$. Then $\phi(1) = (1, 0) \neq (1, 1) = 1_{\mathbb{Z}\times\mathbb{Z}}$, and 1 is a unit in $\mathbb{Z}$, but $\phi(1)$ is not a unit in $\mathbb{Z} \times \mathbb{Z}$.

Alternatively, consider any two rings R and R' with unity $1 \neq 0$ and $1' \neq 0'$ respectively, and consider the trivial homomorphism $\phi : R \to R'$ that sends every element of R to $0'$. Then $\phi(1) = 0' \neq 1'$ and 1 is a unit in R, but $\phi(1)$ is not a unit in R'.
(Beware that if instead we allow R' to be trivial, then it doesn't work: we get $\phi(1) = 0' = 1'$ and $0'$ is a unit in R'.)

A remark: in both examples above we used 1 as our unit in R. This is not necessary; we could use some other unit.

Problem 4 (4 points). Compute $2^{41} \bmod 27$. Show your work. Say what theorems you are applying, if any.

Because 2 is relatively prime to 27 we have $2^{41} \equiv 2^{41 \bmod \varphi(27)} \pmod{27}$ by Euler's theorem. We have $\varphi(27) = 18$ because 9 of the 27 elements of the set $\{0, 1, \ldots, 26\}$ are *not* relatively prime to 27 (namely the multiples of 3, which are $0, 3, \ldots, 24$.) Therefore $2^{41} \equiv 2^{41 \bmod 18} = 2^5 = 32 \equiv 5 \pmod{27}$.

Problem 5 (4 points). This problem asks you to verify one of the steps in the construction of a field of quotients.

Let D be an integral domain and let D^* denote the set of nonzero elements of D. Recall that the relation $\sim$ on $D \times D^*$ defined by $(a, b) \sim (a', b') \iff ab' = ba'$ is an equivalence relation, and let $\frac{a}{b}$ denote the equivalence class of (a, b).

Define the set

$$F = \left\{ \frac{a}{b} : (a, b) \in D \times D^* \right\}.$$

(a) Prove that there is a (well-defined) operation $\cdot$ on F given by $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

Let $\frac{a}{b}, \frac{c}{d} \in F$. First, note that $bd \in D^*$ because $b, d \in D^*$ and D has no zero divisors, so $\frac{ac}{bd}$ is defined and is in F.
Next, we show that $\frac{ac}{bd}$ only depends on a, b, c, and d insofar as it depends on the equivalence classes $\frac{a}{b}$ and $\frac{c}{d}$ of the pairs (a, b) and (c, d) respectively:
Let $\frac{a'}{b'}, \frac{c'}{d'} \in F$ also.
If $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$, then $ab' = ba'$ and $cd' = dc'$; multiplying these equations gives $ab'cd' = ba'dc'$, so $(ac)(b'd') = (bd)(a'c')$, and therefore $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ as desired.

(b) Give at least one reason why this operation $\cdot$ on F could not be defined if D had zero divisors.

We could have $b, d \neq 0$ but $bd = 0$, in which case $\frac{ac}{bd}$ would not be defined.

Alternatively, recall from a homework problem (problem 4 on homework set 3) that if D has zero divisors then the relation $\sim$ defined above is not transitive, so it is not an equivalence relation, and the defintion of the set F itself (as a set of equivalence classes) does not work.