MATH 120B SAMPLE MIDTERM EXAM SOLUTIONS

SPRING 2015

Problem 1 (12 points). Mark each statement 'T' for true (meaning always true) or 'F' for false (meaning sometimes false). You do NOT need to justify your answers to this problem.

Ⓣ F "If $n \geq 2$ is an integer and $a \in \mathbb{Z}_n$ is a unit, then $a^{\varphi(n)} = 1$ in $\mathbb{Z}_n$." True. This is a way of stating Euler's theorem.

T Ⓕ "If R is a ring with unity and S is a subring of R, then S has unity." False: consider $R = \mathbb{Z}$ and $S = 2\mathbb{Z}$.

Ⓣ F "$\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$." True: this follows from the Chinese remainder theorem because 3 and 4 are relatively prime.

T Ⓕ "If p is prime and $a \in \mathbb{Z}$ is not divisible by p, then $a^p \equiv 1 \pmod{p}$." False: $a^p \equiv a \pmod{p}$ by Fermat's theorem, so any prime $p > 2$ and any $a \not\equiv 1 \pmod{p}$ gives a counterexample.

T Ⓕ "If F_1 and F_2 are fields, then their direct product $F_1 \times F_2$ is a field." False: $(0, 1)$ is a zero divisor (for example.)

Ⓣ F "Let K be a field and let $f(x) \in K[x]$ be nonzero. The number of roots of $f(x)$ is less than or equal to $\deg f(x)$." True. This can be proved from the factor theorem.

Ⓣ F "If F is a field and K is a subfield of F, then the characteristic of K equals the characteristic of F." True. (To see this, first note that every subfield of a field F contains 1_F.)

Ⓣ F "If the rings R_1 and R_2 are isomorphic to each other, then their groups of units $U(R_1)$ and $U(R_2)$ are isomorphic to each other." True. (You should be able to recognize such statements as following routinely from the existence of an isomorphism, even though it may be tedious to write out the details.)

T Ⓕ "If $(R, +, \cdot)$ is a ring and R^* is the set of nonzero elements of R, then $(R^*, \cdot)$ is a group." False: if R has zero divisors then R^* is not closed under multiplication.

T Ⓕ "If R is a ring and $f(x), g(x) \in R[x]$ are nonzero then $\deg f(x)g(x) = \deg f(x) + \deg g(x)$." False. You can get counterexamples where the leading coefficients are zero divisors.

Ⓣ F "Let R_1 and R_2 be rings and define the direct product ring $R_1 \times R_2$. If $R_1 \times R_2$ has unity, then R_1 and R_2 both have unity." True: if (a_1, a_2) is a unity for $R_1 \times R_2$, then a_1 is a unity for R_1 and a_2 is a unity for R_2. Note for instance that for all $b_1 \in R_1$ we have $(a_1, a_2) \cdot (b_1, 0) = (b_1, 0)$, so $a_1 \cdot b_1 = b_1$.

Ⓣ F "If D is an integral domain and R is a subring of D containing 1_D, then R is an integral domain." True: if $1_D \in R$ then 1_D is a unity for R. It follows that R has unity $1 \neq 0$. Moreover, R is commutative because D is commutative, and R has no zero divisors because D has no zero divisors.

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

(a) Let R be a commutative ring and let $a \in R$.
What does it mean for a to be a *zero divisor*?

It means that a is nonzero and $ab = 0$ for some nonzero $b \in R$.

(b) What is the *degree* of a polynomial $f(x)$?

It is the largest integer n such that the coefficient of x^n in $f(x)$ is nonzero, if such an n exists; otherwise it is $-\infty$.

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

(a) Prove that if R' is an integral domain and $a, b \notin \ker(\phi)$, then $ab \notin \ker(\phi)$.

Because $a, b \notin \ker(\phi)$ we have $\phi(a), \phi(b) \neq 0$. Therefore $\phi(ab) = \phi(a)\phi(b) \neq 0$ because ϕ is a homomorphism and R' is an integral domain. This means $ab \notin \ker(\phi)$.

(b) Give an example where R' is not an integral domain, $a, b \notin \ker(\phi)$, and $ab \in \ker(\phi)$.

Define $R = \mathbb{Z}$ and $R' = \mathbb{Z}_6$, and define the function $\phi : \mathbb{Z} \to \mathbb{Z}_6$ by $\phi(k) = k \mod 6$. This is a homomorphism and $2, 3 \notin \ker(\phi)$, but $2 \cdot 3 = 6 \in \ker(\phi)$.

Problem 4 (4 points). Compute $4^{444} \bmod 25$ and $5^{444} \bmod 25$. Show your work and say what theorems you are applying, if any.

- First note that $25 = 5^2$ and 5 is prime, so $\varphi(25) = 5^2 - 5 = 20$ by a homework problem. (Or you could find it by counting.)
- 4 is relatively prime to 25, so by Euler's theorem we have
  $4^{444} \equiv 4^{444 \bmod 20} = 4^4 = 256 \equiv 6 \pmod{25}$.
- 5 is not relatively prime to 25, so Euler's theorem doesn't apply. But instead we have
  $5^{444} = (5^2)^{222} = 25^{222} \equiv 0^{222} = 0 \pmod{25}$.
  (Euler's theorem happens to give the right answer for $5^{444} \bmod 25$ also, but it is only an accident.)

Problem 5 (4 points). Let K be a field and let $f(x), g(x) \in K[x]$.

(a) Prove that if K is infinite and $f(x), g(x) \in K[x]$ are polynomials such that $f(\alpha) = g(\alpha)$ for all $\alpha \in K$, then $f(x) = g(x)$.

If $f(\alpha) = g(\alpha)$ for all $\alpha \in K$, then $f(\alpha) - g(\alpha) = 0$ for all $\alpha \in K$. So every $\alpha \in K$ is a zero of the polynomial $f(x) - g(x)$. Because K is infinite, this means that $f(x) - g(x)$ has infinitely many zeroes.

If the polynomial $f(x) - g(x)$ is nonzero then the number of its zeroes is at most its degree, so it has only finitely many zeroes, a contradiction. Therefore $f(x) - g(x)$ is the zero polynomial, so $f(x) = g(x)$.

(b) Give an example where K is finite and there are polynomials $f(x), g(x) \in K[x]$ such that $f(\alpha) = g(\alpha)$ for all $\alpha \in K$, but $f(x) \neq g(x)$.

Let $K = \mathbb{Z}_p$ where p is a prime. Define $f(x) = x$ and $g(x) = x^p$. Then $f(x) \neq g(x)$ but $f(\alpha) = g(\alpha)$ for all $\alpha \in K$ by Fermat's little theorem. (There are many other examples, but this one is convenient.)