MATH 120B SAMPLE FINAL EXAM SOLUTIONS

SPRING 2015

Problem 1 (16 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.

T (F) "$\mathbb{Z}_2 \times \mathbb{Z}_{10} \cong \mathbb{Z}_{20}$." False: the former has four elements a such that $a + a = 0$, but the latter only has two.

(T) F "For any two positive integers a and b, if $\gcd(a, b) = 1$ then $\varphi(ab) = \varphi(a)\varphi(b)$, where φ denotes Euler's phi function." True: $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$, and (m, n) is a unit in the direct product if and only if m is a unit and n is a unit.

T (F) "If F_1 and F_2 are integral domains, then their direct product $F_1 \times F_2$ is an integral domain." False: it has zero divisors $(0, 1)$ and $(1, 0)$.

(T) F "If the fields F_1 and F_2 are isomorphic to each other, then their multiplicative groups F_1^* and F_2^* are isomorphic to each other." True. The proof is routine.

T (F) "There is a finite field of order 6." False: if $(F, +, \cdot)$ were a field of order 6 then $(F, +)$ would be an abelian group of order 6, and the only possibility (up to isomorphism) is $\mathbb{Z}_6$. So F would have characteristic 6. But the characteristic of any finite field is prime. (In fact, one can show that any finite field has prime power order, but this is harder.)

T (F) "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: if R has zero divisors, it is easy to find an example where $\deg f(x)g(x) < \deg f(x) + \deg g(x)$.

T (F) "If p is a prime number and $f(x) \in \mathbb{Z}_p[x]$ is nonzero, then $f(x)$ has a zero in $\mathbb{Z}_p$." False: consider $f(x) = x^p - x + 1$. (Or the easier counterexample $f(x) = 1$; to make the problem interesting I should have said "non-constant" rather than "nonzero".)

T (F) "Let K be a field and let $f(x) \in K[x]$. If $f(x)$ has no zeroes in K, then $f(x)$ is irreducible in $K[x]$." False: consider $f(x) = x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$ in $\mathbb{Q}(x)$.

Ⓣ F "If D is an integral domain then the polynomial ring $D[x]$ is an integral domain." True. We proved this in class.

T Ⓕ "Every proper ideal of an integral domain is prime." False: consider the ideal $k\mathbb{Z}$ of $\mathbb{Z}$ where k is a composite number.

Ⓣ F "Every ideal is the kernel of some homomorphism." True: if R is a ring and N is an ideal of R, then N is the kernel of the canonical homomorphism $R \to R/N$.

Ⓣ F "Let R and R' be rings and let $\phi : R \to R'$ be a homomorphism. Then $\ker \phi$ is an ideal of R." True. We proved this in class.

Ⓣ F "Let R and R' be commutative rings, let $\phi : R \to R'$ be a homomorphism, and let N' be a prime ideal of R'. Then $\varphi^{-1}[N']$ is either a prime ideal of R or the improper ideal of R." True: the inverse image of an ideal under a homomorphism is an ideal, and if $a, b \in R$ and $ab \in \varphi^{-1}[N']$, then $\phi(a)\phi(b) = \phi(ab) \in N'$, so $\phi(a) \in N'$ or $\phi(b) \in N'$, so $a \in \varphi^{-1}[N']$ or $b \in \varphi^{-1}[N']$. (In the original version of the practice exam, I did not ask the question that I meant to ask, and the answer was false.)

T Ⓕ "$\mathbb{Q}$ is an extension field of $\mathbb{Z}_2$." False: $\mathbb{Z}_2$ is not a subfield of $\mathbb{Q}$ because its operations are not induced by those of $\mathbb{Q}$. (Moreover, $\mathbb{Z}_2$ cannot even be *isomorphic* to a subfield of $\mathbb{Q}$ because the characteristics are different.)

Ⓣ F "$\mathbb{Z}_2$ has an extension field E of order 4 (meaning $|E| = 4$.)" True: take an irreducible polynomial $p(x)$ of degree 2 in $\mathbb{Z}_2[x]$, such as $x^2 + x + 1$, and consider $E = \mathbb{Z}_2[x]/\langle p(x) \rangle$.

T Ⓕ "$\mathbb{Z}_2$ has an extension field E of order 5 (meaning $|E| = 5$.)" False: the two fields would need to have the same characteristic, but the characteristic of a finite field divides its order, and 2 does not divide 5. (In fact, one can show that any extension field of $\mathbb{Z}_p$, where p is a prime, has order p^n for some $n \in \mathbb{Z}^+$, but this is harder.)

Problem 2 (4 points). For each part, answer yes or no, and *justify your answer.*

(a) Does $\mathbb{Z}_8$ have a subring that is isomorphic to $\mathbb{Z}_2$?

No. Each of these rings has a unique nonzero element a such that $a + a = 0$, namely 1 in $\mathbb{Z}_2$ and 4 in $\mathbb{Z}_8$. So any isomorphism $\phi : \mathbb{Z}_2 \to \mathbb{Z}_8$ would need to satisfy $\phi(1) = 4$. But then $\phi(1 \cdot 1) = \phi(1) = 4$ and $\phi(1) \cdot \phi(1) = 4 \cdot 4 = 0 \neq 4$, contradicting the assumption that ϕ preserves multiplication.

(b) Does $\mathbb{Z}_6$ have a subring that is isomorphic to $\mathbb{Z}_2$?

Yes, $\{0, 3\}$ is a subring of $\mathbb{Z}_6$ that is isomorphic to $\mathbb{Z}_2$. We just have to check that $3 + 3 = 0$ and $3 \cdot 3 = 3$ in $\mathbb{Z}_6$.

Alternatively, note that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ because 2 and 3 are relatively prime, and $\mathbb{Z}_2 \times \mathbb{Z}_3$ has a subring isomorphic to $\mathbb{Z}_2$, namely $\mathbb{Z}_2 \times \{0\}$.

Problem 3 (4 points). Compute 3^{70} mod 23. Show your work, along with appropriate explanation and justification.

23 is prime and $3 \not\equiv 0 \pmod{23}$, so by Fermat's little theorem we have

$3^{70} \equiv 3^{70 \bmod 22} = 3^4 = 81 \equiv 12 \pmod{23}$.

Problem 4 (4 points). Find the quotient and remainder when the polynomial x^4+3x^2+2x+1 in $\mathbb{Z}_5[x]$ is divided by the polynomial x^2+2x+3 in $\mathbb{Z}_5[x]$.

$$
\begin{array}{r|l}
 & x^2 \quad +3x \quad +4 \\
\hline
x^2+2x+3 & x^4 \quad +3x^2 \quad +2x \quad +1 \\
 & x^4 \quad +2x^3 \quad +3x^2 \\
\cline{2-2}
 & 3x^3 \quad +2x \\
 & 3x^3 \quad +x^2 \quad +4x \\
\cline{2-2}
 & 4x^2 \quad +3x \quad +1 \\
 & 4x^2 \quad +3x \quad +2 \\
\hline
 & 4
\end{array}
$$

The quotient is x^2+3x+4 and the remainder is 4.

Problem 5 (6 points). Give the requested definitions.

(a) Let R be a ring. What is a *subring of* R?

A subring of R is a subset of R that forms a ring under the induced operations from R.

Alternatively, a subring of R is a subset of R that is closed under addition and multiplication, contains 0, and is closed under taking negatives (additive inverses.)

(b) Let F be a field, let E be an extension field of F, and let $\alpha \in E$.
What does it mean for α to be *algebraic* over F?

It means that there is a nonzero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$.

(c) Let R and R' be rings and let $\phi : R \to R'$ be a homomorphism.
What is the *kernel* of ϕ?

$\ker(\phi) = \{x \in R : \phi(x) = 0_{R'}\}$.

Alternatively, $\ker(\phi) = \phi^{-1}[\{0_{R'}\}]$.

Problem 6 (4 points). Let R be a commutative ring and define

$$N = \{a \in R : a^n = 0 \text{ for some } n \in \mathbb{Z}^+\}.$$

Prove that N is an ideal of R.

- Let $a, b \in N$, say $a^m = 0$ and $b^n = 0$. Then $(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i} = \sum_{i=0}^{n+m} 0 = 0$, so $a+b \in N$. (In each term, we have $i \geq m$ or $n+m-i \geq n$, so one of the factors is zero.)
- $0^1 = 0$, so $0 \in N$.
- Let $a \in N$, say $a^m = 0$. Then $(-a)^m$ is a^m if m is even and $-a^m$ if m is odd (this can be proved by induction on m) so in either case it is zero, and $-a \in N$. (If R had unity, we could say $(-a)^m = (-1)^m a^m = 0$.)
- Let $a \in N$ and $b \in R$. Say $a^m = 0$. Then $(ab)^m = a^m b^m = 0$ because R is commutative, so $ab \in N$.

Problem 7 (4 points). For each part, make sure to justify your answer.

(a) Give an example of a commutative ring R with unity such that the trivial ideal $\{0\}$ of R is prime but not maximal.

In $\mathbb{Z}$, the trivial ideal is prime because $\mathbb{Z}$ is an integral domain, but it is not maximal because $\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$. (Any integral domain that is not a field would work here in place of $\mathbb{Z}$.)

(b) If R is a commutative ring with unity and N is a nontrivial prime ideal of R, must N be maximal? Prove it or give a counterexample.

In $\mathbb{Z} \times \mathbb{Z}$, the ideal $\mathbb{Z} \times \{0\}$ is prime (using the fact that the second copy of $\mathbb{Z}$ is an integral domain) but it is not maximal because $\mathbb{Z} \times \{0\} \subsetneq \mathbb{Z} \times 2\mathbb{Z} \subsetneq \mathbb{Z} \times \mathbb{Z}$.

Alternatively, in $\mathbb{Z}[x]$ the ideal $\langle x \rangle$ is prime but not maximal because $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ (apply the fundamental homomorphism theorem to the evaluation homomorphism $\phi_0 : \mathbb{Z}[x] \to \mathbb{Z}$) and $\mathbb{Z}$ is an integral domain but not a field.

Problem 8 (4 points). Define the real number $\alpha = 2^{2/3} - 1$.

(a) Prove that α is algebraic (over $\mathbb{Q}$).

We have $\alpha+1 = 2^{2/3}$, so $(\alpha+1)^3 = 2^2 = 4$. So $0 = (\alpha+1)^3-4 = \alpha^3+3\alpha^2+3\alpha-3$, and α is a zero of the nonzero polynomial $p(x) = x^3 + 3x^2 + 3x - 3 \in \mathbb{Q}[x]$.

(b) Find $\deg(\alpha, \mathbb{Q})$, meaning the degree of α over $\mathbb{Q}$, and $\operatorname{irr}(\alpha, \mathbb{Q})$, meaning the irreducible polynomial of α over $\mathbb{Q}$. Justify your answer.

We claim that $\operatorname{irr}(\alpha, \mathbb{Q})$ is the polynomial $p(x)$ from part a. Because $p(x)$ is in $\mathbb{Q}[x]$ and is monic, it will suffice to show that $p(x)$ is irreducible in $\mathbb{Q}[x]$. Because $\deg p(x) \leq 3$, it will suffice to show that $p(x)$ does not have a zero in $\mathbb{Q}$. By the rational root theorem, if a/b is a rational zero of $p(x)$ in lowest terms, then $b \mid 1$ and $a \mid -3$, so a/b is ± 1 or ± 3. But none of these four possibilities works.[1]

It follows that $\deg(\alpha, \mathbb{Q}) = \deg p(x) = 3$.

[1]Here is one way to see this: $p(\pm 1) \equiv (\pm 1)^3 \equiv \pm 1 \not\equiv 0 \pmod 3$, and $p(\pm 3) \equiv -3 \not\equiv 0 \pmod 9$.