Math 547, Exam 3, Spring , 2005

The exam is worth 50 points.

Write your answers as legibly as you can on the blank sheets of paper provided. Use only **one side** of each sheet. Take enough space for each problem. Turn in your solutions in the order: problem 1, problem 2, ... ; although, by using enough paper, you can do the problems in any order that suits you.

I will e-mail your grade to you as soon as I finish grading the exams.

If you want me to leave your exam outside my door (so that you can pick it up before Wednesday's class), then **TELL ME** and I will do it. The exam will be there as soon as I e-mail your grade to you.

I will post the solutions on my website later today.

1. **(6 points) Define** *maximal ideal***.**

The ideal I of the ring R is a *maximal ideal* if $I \subsetneq R$ and whenever J is an ideal of R with $I \subsetneq J$, then $J = R$.

2. **(6 points) Define** *Principal Ideal Domain***.**

The domain R is a *Principal Ideal Domain* if every ideal of R has is equal to $\{ar \mid r \in R\}$ for some $a \in R$.

3. **(6 points) Define** *irreducible element***.**

Let R be a domain. The non-zero, non-unit element r of R is an *irreducible element* if whenever $r = ab$ for some a and b in R, then either a is a unit or b is a unit.

4. **(8 points) Prove that $\mathbb{Q}[x]$ is a Principal Ideal Domain.**

Let I be a non-zero ideal in $\mathbb{Q}[x]$. Let f be a non-zero polynomial in I of least degree. We show that $I = (f)$. It is clear that $(f) \subseteq I$. We show that $I \subseteq (f)$. Let g be an arbitrary element of I. Divide f into g and get $g = hf + r$ for polynomials h and r of $\mathbb{Q}[x]$ where either r is the zero polynomial or r has degree less than the degree of f. We see that $r = g - hf \in I$. We chose f to be a non-zero polynomial in I of least degree. It follows that r is the zero polynomial and $g \in (f)$.

5. **(8 points) Let $\alpha = e^{\frac{2\pi i}{9}}$ and let $\phi\colon \mathbb{Q}[x] \to \mathbb{C}$ be the function which is given by $\phi(f(x)) = f(\alpha)$. All of us know that this function is a ring homomorphism; you do not have to show me a proof. What is the kernel of ϕ? Prove your answer.**

The kernel of ϕ is generated by an irreducible polynomial $g(x) \in \mathbb{Q}[x]$ with $g(\alpha) = 0$. The polynomial $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$ is in the kernel of ϕ and $x^3 - 1$ is not in the kernel of ϕ (which is a prime ideal). So, $g(x) = x^6 + x^3 + 1$

is in the kernel of ϕ. We complete the proof by showing that $g(x)$ is irreducible. We give a tricky argument here. Observe that

$$g(x) = g((x-1)+1) = ((x-1)+1)^6 + ((x-1)+1)^3 + 1$$

$$= \left\{ \begin{array}{r} (x-1)^6 + 6(x-1)^5 + 15(x-1)^4 + 20(x-1)^3 + 15(x-1)^2 + 6(x-1) + 1 \\ + \quad (x-1)^3 + \;\; 3(x-1)^2 + 3(x-1) + 1 \\ +1 \end{array} \right.$$

$$= (x-1)^6 + 6(x-1)^5 + 15(x-1)^4 + 21(x-1)^3 + 18(x-1)^{18} + 9(x-1) + 3.$$

So, $g(x) = f(x-1)$, where

$$f(y) = y^6 + 6(x-1)^5 + 15y^4 + 21(x-1)^3 + 18y^{18} + 9y + 3.$$

We apply Eisenstein's Criteria to see that $f(y)$ is irreducible. (The prime 3 divides every coefficient of $f(y)$ except the leading coefficient, and 3^2 does not divide the constant term.) It follows that $g(x)$ is irreducible and the proof is complete.

6. **(8 points) Let M be a maximal ideal of the ring R. Prove that $\frac{R}{M}$ is a field.**

We need only show that each non-zero element of $\frac{R}{M}$ has a multiplicative inverse in $\frac{R}{M}$. Pick a non-zero element of $\frac{R}{M}$. This element has the form $\bar{a}$ where a is an element of R which is not an element of M. We must show that the element $\bar{a}$ of $\frac{R}{M}$ has an inverse in $\frac{R}{M}$.

Let (M, a) denote the smallest ideal of R which contains M and a. Observe that $(M,a) = \{m + ra \mid m \in M \text{ and } r \in R\}$. The hypothesis ensures us that $(M,a) = R$. In other words, there exist elements $m \in M$ and $r \in R$ with $1 = m + ra$. We conclude that $\bar{r}$ is the inverse of $\bar{a}$ in $\frac{R}{M}$.

7. **(8 points) Suppose $K \subseteq F \subseteq E$ are fields with α_1, α_2 a basis of F over K and β_1, β_2 a basis of E over F.**
   (a) What is a basis for E over K?
   (b) Prove your answer to (a).

The elements $\alpha_1\beta_1, \alpha_2\beta_1, \alpha_1\beta_2, \alpha_2\beta_2$ are a basis of E over K.

Span: Take $e \in E$. The elements β_1, β_2 are a basis of E over F; so there exist f_1 and $f_2 \in F$ with $e = f_1\beta_1 + f_2\beta_2$. The elements α_1, α_2 are a basis of F over K, so, there exist $k_{1,1}$, $k_{1,2}$, $k_{2,1}$, $k_{2,2}$ in K, with $f_1 = k_{1,1}\alpha_1 + k_{1,2}\alpha_2$ and $f_2 = k_{2,1}\alpha_1 + k_{2,2}\alpha_2$. We now see that

$$e = f_1\beta_1 + f_2\beta_2 = (k_{1,1}\alpha_1 + k_{1,2}\alpha_2)\beta_1 + (k_{2,1}\alpha_1 + k_{2,2}\alpha_2)\beta_2.$$

Thus,

$$e = k_{1,1}\alpha_1\beta_1 + k_{1,2}\alpha_2\beta_1 + k_{2,1}\alpha_1\beta_2 + k_{2,2}\alpha_2\beta_2.$$

We have expressed the arbitrary element e of E as a linear combination of the proposed basis with coefficients from K. In other words, we have shown that $\alpha_1\beta_1, \alpha_2\beta_1, \alpha_1\beta_2, \alpha_2\beta_2$ spans E over K.

Linear Independence: Suppose A, B, C, D are elements of K with

$$0 = A\alpha_1\beta_1 + B\alpha_2\beta_1 + C\alpha_1\beta_2 + D\alpha_2\beta_2.$$

It follows that

$$0 = (A\alpha_1 + B\alpha_2)\beta_1 + (C\alpha_1 + D\alpha_2)\beta_2.$$

Notice that $(A\alpha_1 + B\alpha_2)$ and $(C\alpha_1 + D\alpha_2)$ are in F and β_1, β_2 are linearly independent over F. It follows that $A\alpha_1 + B\alpha_2 = 0$ and $C\alpha_1 + D\alpha_2 = 0$. However A, B, C, and D are in K and α_1, α_2 are linearly independent over K. It follows that A, B, C, and D are all zero. Thus, $\alpha_1\beta_1, \alpha_2\beta_1, \alpha_1\beta_2, \alpha_2\beta_2$ are linearly independent over K.