Math 547, Exam 2, Spring , 2005 Solutions

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 Monday'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. **(8 points) Give an example of a ring R and an ideal I with I not a principal ideal. Explain.**

If $R = \mathbb{Q}[x, y]$ and $I = (x, y)$, then I is not a principal ideal. Indeed, if I were generated by f, then f would have to divide both x and y. One can calculate, using degree arguments, that this forces f to be a unit. However, $f \in (x, y)$; so f can't be a unit. Thus, no such polynomial f exists and I is not principal.

2. **(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 $g \in (f)$.

3. **(8 points) Is $\frac{\mathbb{Q}[x]}{(x^2-1)}$ a domain? Explain.**

No. The elements of $\frac{\mathbb{Q}[x]}{(x^2-1)}$ determined by $x - 1$ and $x + 1$ are not zero in $\frac{\mathbb{Q}[x]}{(x^2-1)}$; but the product $(x - 1)(x + 1)$ is zero in $\frac{\mathbb{Q}[x]}{(x^2-1)}$.

4. **(8 points) Let $\alpha = e^{\frac{2\pi i}{6}}$ 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.**

We know that $x^6 - 1 \in \ker \phi$. We also know that $x^6 - 1 = (x^3 - 1)(x^3 + 1)$. A moments thought shows that $x^3 - 1 \notin \ker \phi$ (since $\alpha^3 - 1 \neq 0$) and $x^3 + 1 \in \ker \phi$ since $\alpha^3 + 1 = -1 + 1 = 0$. Furthermore, $x^3 + 1 = (x + 1)(x^2 - x + 1)$. (If you don't remember how to factor the sum of perfect cubes, you can always do long division.) It is clear that α is not a root of $x + 1$ so α must be a root of $f(x) = x^2 - x + 1$. We see that $f(x)$ is irreducible in $\mathbb{Q}[x]$, because if f were to factor, then the factors would be linear, with rational coefficients and α would have to be a root of one of the factors; that is, α would have to be a rational number, which, of course, is not true since $\alpha = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$. At any rate, the irreducible polynomial $f(x)$ is in the kernel of ϕ. It follows that the entire ideal (f) in $\mathbb{Q}[x]$ is contained in $\ker\phi$. The polynomial f is irreducible; so, the ideal (f) is a maximal ideal in $\mathbb{Q}[x]$ with $(f) \subseteq \ker\phi \subsetneq \mathbb{Q}[x]$;and therefore, $(f) = \ker\phi$.

5. **(9 points) Let $\phi\colon R \to S$ be a ring homomorphism. Suppose that $\ker\phi = \{0\}$. Prove that ϕ is one-to-one.**

We assume $\ker\phi = \{0\}$. Suppose r_1 and r_2 are in R with $\phi(r_1) = \phi(r_2)$. We see that

$$\phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) = 0;$$

thus, $r_1 - r_2 \in \ker\phi = \{0\}$, and $r_1 = r_2$. We conclude that ϕ is one-to-one.

6. **(9 points) Let M be an ideal of the ring R. Suppose that $M \neq R$ and that R is the only ideal of R which properly contains M. 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 $\frac{R}{M}$.