CS203B: Final Examination Solution

September 18, 2015

Grading Policy: For each question, 20% marks are for making an intelligent statement about the problem, 20% for attempting solution in the right direction, 20% for making progress towards to solution, 20% for reaching close to solution, and 20% for getting the correct solution.

Question 1. (5 + 5 marks) For a ring R, let $\mathcal{U}_R$ be the set of units in R. Prove that $\mathcal{U}_R$ is a group.

Ring R is called a *local ring* if $\mathcal{I}_R = R \backslash \mathcal{U}_R$ is an ideal of R. Prove that every non-trivial ideal of R is a subset of $\mathcal{I}_R$. It follows immediately that $\mathcal{I}_R$ is the unique maximal ideal of R.

Answer 1. Let $a \in \mathcal{U}_R$. By definition of unit, there exists $b \in R$ such that $ab = 1$. To prove that $\mathcal{U}_R$ is a group under multiplication, one needs to show closure and inverse, as other properties already hold because R is a ring. Any $a \in \mathcal{U}_R$ has b as inverse where $ab = 1$. Consider $a_1, a_2 \in \mathcal{U}_R$. Then we have $a_1 b_1 = 1 = a_2 b_2$. So $a_1 a_2 b_1 b_2 = 1$ showing that $a_1 a_2 \in \mathcal{U}_R$.

Let I be any ideal of R not contained in $\mathcal{I}_R$. Then there exists $a \in I \backslash \mathcal{I}_R$. Therefore, $a \in \mathcal{U}_R$ which implies that $1 \in I$ making $I = R$. Hence, any non-trivial ideal of R is contained in $\mathcal{I}_R$.

Question 2. (10 marks) For any curve $C(x, y) = 0$ in $\mathbb{R}^2$, let $\Gamma(C) = \mathbb{R}[x, y]/(C(x, y))$. For any point $P \in \mathbb{R}^2$ on curve C, i.e., $C(P) = 0$, define $\Gamma_P(C)$ as:

$$\Gamma_P(C) = \left\{ \frac{f}{g} \mid f, g \in \Gamma(C) \text{ and } g(P) \neq 0 \right\}.$$

Prove that $\Gamma_P(C)$ is a local ring with

$$\mathcal{I}_{\Gamma_P(C)} = \left\{ \frac{f}{g} \mid \frac{f}{g} \in \Gamma_P(C) \text{ and } f(P) = 0 \right\}.$$

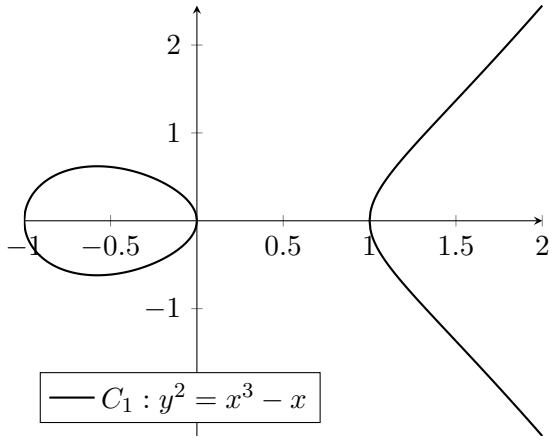
Answer 2. Consider $\frac{f_1}{g_1}, \frac{f_2}{g_2} \in \Gamma_P(C)$. We have $g_1(P), g_2(P) \neq 0$. Now

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2} \text{ and } \frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2},$$

and $g_1 g_2(P) = g_1(P) \cdot g_2(P) \neq 0$. Hence $\Gamma_P(C)$ is a ring. Units in $\Gamma_P(C)$ are elements $\frac{f}{g}$ such that $f(P) \neq 0$ and $g(P) \neq 0$ since their inverses $\frac{g}{f}$ are in $\Gamma_P(C)$. On the other hand, if $f(P) = 0$, then the inverse $\frac{g}{f}$ does not belong to $\Gamma_P(C)$. So $\mathcal{I}_{\Gamma_P(C)}$ is the set of all non-units of $\Gamma_P(C)$. We now prove that it is an ideal. Consider $\frac{f_1}{g_1}, \frac{f_2}{g_2} \in \mathcal{I}_{\Gamma_P(C)}$. Their sum has numerator $f_1 g_2 + f_2 g_1$ and $(f_1 g_2 + f_2 g_1)(P) = f_1(P) g_2(P) + f_2(P) g_2(P) = 0$. Hence

$\mathcal{I}_{\Gamma_P(C)}$ is closed under addition. The remaining group properies follow from the fact that $\Gamma_P(C)$ is a ring. For any $\frac{f}{g} \in \Gamma_P(C)$, $\frac{ff_1}{gg_1}(P) = \frac{f(P)f_1(P)}{g(P)g_1(P)} = 0$. Hence $\mathcal{I}_{\Gamma_P(C)}$ is an ideal of $\Gamma_P(C)$.

Question 3. (10 marks) Ring $\Gamma_P(C)$ carries information about behaviour of curve C at point P. Consider the curve C_1:



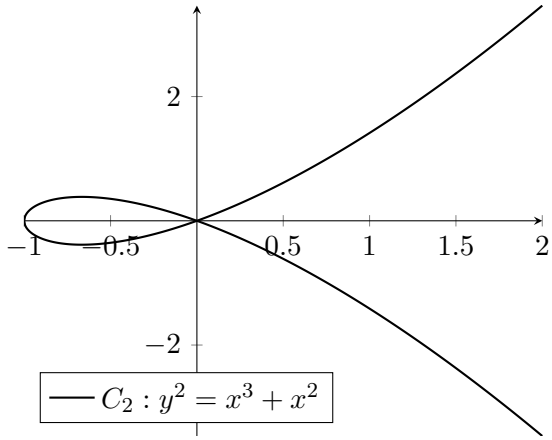
This is a simple curve with a tangent well-defined at every point on the curve. For such curves, the local ring at every point is principle. For point $P = (0, 0)$, prove that $\mathcal{I}_{\Gamma_P(C_1)}$ equals the principle ideal generated by $y \in \Gamma_P(C_1)$.

Answer 3. We need to prove that $\mathcal{I}_{\Gamma_P(C_1)}$ is principle. If $\frac{f}{g} \in \mathcal{I}_{\Gamma_P(C_1)}$, then $f(0, 0) = 0$ and $g(0, 0) \neq 0$. Hence, $f(x, y) = xf_1(x, y) + yf_2(x, y)$. So any element of $\mathcal{I}_{\Gamma_P(C_1)}$ can be written as $\frac{f_1}{g}x + \frac{f_2}{g}y$ and $\frac{f_1}{g}, \frac{f_2}{g} \in \Gamma_P(C_1)$. Therefore, $\mathcal{I}_{\Gamma_P(C_1)}$ is generated by elements x and y. Since x and y are elements of $\Gamma_P(C_1)$, $y^2 = x^3 - x = x(x^2 - 1)$. So we can write

$$x = \frac{y}{x^2 - 1}y,$$

and $\frac{y}{x^2-1} \in \Gamma_P(C_1)$. Hence ideal $\mathcal{I}_{\Gamma_P(C_1)}$ is generated by the element y and is therefore principle.

Question 4. (5 + 5 + 5 marks) On the other hand, consider the curve C_2:



This curve is *singular* at point $P = (0, 0)$, i.e., $\frac{\partial C_2}{\partial x} = 0 = \frac{\partial C_2}{\partial y}$ at P. This fact is captured in $\Gamma_P(C_2)$ by the property that $\mathcal{I}_{\Gamma_P(C_2)}$ is not principle. Let us prove it.

- Show that the ideal $\mathcal{I}_{\Gamma_P(C_2)}$ contains x and y and is generated by these two.
- For an ideal I of ring R, define

$$I^k = \{a_1 a_2 \cdots a_k \mid a_1, a_2, \ldots, a_k \in I\}.$$

  Prove that for every $k \geq 2$, I^k is an ideal of R and $I^k \subseteq I^{k-1}$.
- Prove that if I is a principle ideal, then so is I^k for every $k \geq 2$.

It can be shown, with some more work, that $\mathcal{I}^3_{\Gamma_P(C_2)}$ is not principle and has independent generators x^3 and x^2y showing that $\mathcal{I}_{\Gamma_P(C_2)}$ is not principle.

Thus, not only does every curve can be viewed as a ring, *every point on the curve can be viewed as a local ring*!!

Answer 4. The proof that ideal $\mathcal{I}_{\Gamma_P(C_2)}$ is generated by x and y is identical to the proof that the ideal $\mathcal{I}_{\Gamma_P(C_1)}$ is generated by x and y above.

There is an error in the second question statement. It should have been: *Prove that for every $k \geq 2$, if I is a finitely generated ideal of R then I^k is an ideal of R and $I^k \subseteq I^{k-1}$.* Due to this error, any attempt will get full marks.

Here we prove the correct version. Let I be generated by elements $c_1, c_2, \ldots, c_t$. Then every k products of these elements belongs to I^k and these products ($\binom{k+t-1}{k}$ many) together generate I^k as every element of I^k can be written as a combination of these.

Consider $a_1 a_2 \cdots a_k \in I^k$. Then, $a_1 a_2 \cdots a_k = a_1 \cdot (a_2 \cdots a_k)$ and $a_2 \cdots a_k \in I^{k-1}$. Hence $a_1 \cdot (a_2 \cdots a_k) \in I^{k-1}$. This proves that $I^k \subseteq I^{k-1}$.

Finally, assume I is a principle ideal. Let c generate I. Let $a_1, a_2, \ldots, a_k \in I$ with $a_i = b_i c$, $b_i \in R$. Then $a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_k c^k$ with $b_1 b_2 \cdots b_k \in R$. Hence, c^k generates the ideal I^k.

Question 5. (5 + 5 marks) Consider the following set of numbers:

$$Z_p = \left\{ \frac{a}{b} \mid \ \gcd(b, p) = 1 \right\},$$

for prime number p.

- Prove that Z_p is a local ring.
- Prove that $Z_p/\mathcal{I}_{Z_p}$ is isomorphic to field F_p.

Answer 5. Let $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in Z_p$. Then,

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \text{ and } \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2},$$

and $\gcd(b_1 b_2, p) = 1$. Hence, Z_p is closed under addition and multiplication. It follows that Z_p is a ring (remaining properties follow as Z_p is a subset of $\mathbb{Q}$). The units of Z_p are numbers $\frac{a}{b}$ such that $\gcd(a, p) = 1 = \gcd(b, p)$. The set of non-units, $\mathcal{I}_{Z_p}$ is an ideal because if $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathcal{I}_{Z_p}$ and $\frac{a}{b} \in Z_p$, then p divides both $a_1 b_2 + b_1 a_2$ and $a a_1$ since it divides both a_1 and a_2.

Elements of quotient ring $Z_p/\mathcal{I}_{Z_p}$ are $\frac{a}{b} + \mathcal{I}_{Z_p}$ and elements of $\mathbb{Z}/(p)$ are $a + (p)$. Define mapping $\phi : Z_p/\mathcal{I}_{Z_p} \mapsto \mathbb{Z}/(p)$ as:

$$\phi(\frac{a}{b} + \mathcal{I}_{Z_p}) = ab^{-1} + (p),$$

where $b^{-1}b = 1 \pmod{p}$. Since p does not divide b, $b^{-1} \pmod{p}$ exists. It is a ring homomorphism since:

$$\phi(\frac{a_1}{b_1} + \frac{a_2}{b_2} + \mathcal{I}_{Z_p}) = (a_1b_2 + b_1a_2)b_1^{-1}b_2^{-1} + (p) = a_1b_1^{-1} + a_2b_2^{-1} + (p) = \phi(\frac{a_1}{b_1}) + \phi(\frac{a_2}{b_2}),$$

and

$$\phi((\frac{a_1}{b_1} + \mathcal{I}_{Z_p}) \cdot (\frac{a_2}{b_2} + \mathcal{I}_{Z_p})) = a_1a_2b_1^{-1}b_2^{-1} + (p) = (a_1b_1^{-1} + (p)) \cdot (a_2b_2^{-1} + (p)) = \phi(\frac{a_1}{b_1}) \cdot \phi(\frac{a_2}{b_2}).$$

Suppose $\phi(\frac{a}{b} + \mathcal{I}_{Z_p}) = 0$. Then $ab^{-1} \in (p)$ which implies that p divides a. Hence, $\frac{a}{b} \in \mathcal{I}_{Z_p}$. Therefore, kernel of ϕ is $\{0\}$, making it one-to-one. It is straightforward to see that ϕ is also onto, and hence an isomorphism.