SOLUTION OF QUIZ 2, VERSION B, MATH100B, WINTER 2021

1. (3 points) Suppose I is an ideal of a unital commutative ring A and A/I is a finite integral domain. Show that I is a maximal ideal.

   A/I is a finite integral domain. Every finite integral domain is a field. Hence A/I is a field. A/I is a field if and only if I is maximal.

2. (5 points) Suppose D is an integral domain, $f, g \in D[x]$ are polynomials of degree at most n, and $a_1, \ldots, a_{n+1}$ are distinct elements of D. Prove that if $f(a_i) = g(a_i)$ for every i, then $f(x) = g(x)$.

   Let $h(x) := f(x) - g(x)$. Then $a_1, \ldots, a_{n+1}$ are distinct zeros of h. Hence by the generalized factor theorem, there is $r(x) \in D[x]$ such that

   $$h(x) = (x - a_1) \cdots (x - a_{n+1}) r(x). \tag{1}$$

   Notice that since D is an integral domain, we are allowed to use the generalized factor theorem. By (1), comparing the degrees of both sides of (1) we obtain that $\deg h = n + 1 + \deg r$. Since $\deg f, \deg g \leq n$, $\deg h \leq n$. From these we deduce that $\deg r < -1$. Hence $r(x) = 0$, which in turn implies that $h(x) = 0$; and so $f(x) = g(x)$.

3. (5 points) Determine whether $f(x) := x^{3^{2021}} - x + 100$ has a zero in $\mathbb{Q}$. Justify your answer.

   Notice that by Fermat's little theorem for every $a \in \mathbb{Z}_3$, we have $a^3 = a$. And so $a^{3^n} = a$ for every positive integer n. Hence for every $a \in \mathbb{Z}_3$, we have that $f(a) = a^{3^{2021}} - a + 100 = 1 \neq 0$. This means that the monic polynomial $f(x)$ does not have a zero in $\mathbb{Z}_3$. Hence by the mod-n criterion, we deduce that $f(x)$ does not have a rational zero.

4. Suppose $\alpha \in \mathbb{C}$ is a zero of $x^3 - x + 1$.
   (a) (3 points) Find the minimal polynomial of α over $\mathbb{Q}$.

   By Fermat's little theorem, for every $i \in \mathbb{Z}_3$, we have $i^3 - i + 1 = 1 \neq 0$. Hence the monic polynomial $x^3 - x + 1$ does not have a zero in $\mathbb{Z}_3$. Hence by the mod-n criterion, $x^3 - x + 1$ does not have a rational zero. Therefore by the degree 2 or 3 irreducibility criterion, we obtain that $x^3 - x + 1$ is irreducible in $\mathbb{Q}[x]$. Since α is the zero of the monic irreducible polynomial $x^3 - x + 1$, we have that $m_{\alpha,\mathbb{Q}}(x) = x^3 - x + 1$.

   (b) (4 points) Argue why $(\alpha^2 + 1)^{-1}$ can be written as $a_0 + a_1\alpha + a_2\alpha^2$ for some $a_i \in \mathbb{Q}$. (You are allowed to use all the results proved in the lectures after carefully stating them.)

   We know that if E is a field extension of F and $\alpha \in E$ is algebraic over F, then
   (a) $F[\alpha]$ is a field.
   (b) If $\deg m_{\alpha,F}(x) = n$, then every element of $F[\alpha]$ can be uniquely written as

   $$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

   for some a_i's in F.

   Hence $\mathbb{Q}[\alpha]$ is a field and every element of $\mathbb{Q}[\alpha]$ can be written as $a_0 + a_1\alpha + a_2\alpha^2$ for some a_i's in $\mathbb{Q}$. Since the minimal polynomial of α over $\mathbb{Q}$ is of degree 3, $\alpha^2 + 1 \neq 0$. Hence $(\alpha^2+1)^{-1} \in \mathbb{Q}[\alpha]$, and the claim follows.

5. Suppose D is an integral domain which is not a field and $a \in D$.

(a) (4 points) Prove that $x - a$ is irreducible in $D[x]$.

Since D is an integral domain, $D[x]^\times = D^\times$. Hence $x-a$ is not a unit. Suppose $x-a = f(x)g(x)$ for some $f, g \in D[x]$. Comparing the degrees we deduce that either $\deg f = 0$ or $\deg g = 0$. Without loss of generality, we can and will assume that $f(x) = c$ is a constant. Comparing the leading coefficients of $x - a$ and $cg(x)$, we obtain that c is a unit. This means $f(x)$ is a unit in $D[x]$.

(b) (4 points) Prove that $D[x]/\langle x - a\rangle \simeq D$.

Let $\phi_a : D[x] \to D$ be the map oof evaluation at a. For every $c \in D$, $\phi_a(c) = c$. Hence ϕ_a is surjective. Notice that $f \in \ker \phi_a$ if and only if a is a zero of $f(x)$. By the factor theorem, we have that a is a zero of f if and only if $f(x) = (x - a)g(x)$ for some $g \in D[x]$. Altogether, we obtain that $\ker \phi_a = \langle x - a\rangle$. Thus by the first isomorphism theorem, we have that

$$D[x]/\langle x - a\rangle \simeq D.$$

(c) (2 points) Prove that $D[x]$ is not a PID.

Suppose to the contrary that $D[x]$ is a PID. Then the ideal generated by an irreducible element of $D[x]$ is a maximal ideal. Hence by part (a), $\langle x - a\rangle$ is maximal. Therefore $D[x]/\langle x - a\rangle$ is a field. By part (b), we deduce that D is a field, which is a contradiction.