SOLUTIONS OF QUIZ 1, VERSION A, MATH100B, WINTER 2021

1. Answer the following questions and briefly justify your answers.

   (a) (1 point) True or false. Every integral domain can be embedded into a field.

   By the universal property of field of fractions, every integral domain D can be embedded in its field of fractions $Q(D)$.

   (b) (2 point) Find $|(\mathbb{Z}[x])^\times|$.

   For every integral domain D, we have $D[x]^\times = D^\times$. Hence $\mathbb{Z}[x]^\times = \mathbb{Z}^\times = \{1, -1\}$. Therefore $|(\mathbb{Z}[x])^\times| = 2$.

   (c) (3 points) True or false. There is an integral domain D such that

   $$\underbrace{1_D + \cdots + 1_D}_{9 \text{ times}} = 0 \text{ and } 1_D + 1_D + 1_D \neq 0.$$

   It is false. The characteristic of an integral domain is prime, and it is equal to the additive order of 1_D. By the assumption, the additive order of 1_D is not 3 and it divides 9. Hence the additive order of 1_D is 9, which is not prime. Hence D is not an integral domain.

   (d) (4 points) Find $|(\mathbb{Z}_9 \times \mathbb{Z}_5)^\times|$.

   We know that $(A_1 \times A_2)^\times = A_1^\times \times A_2^\times$ and $\mathbb{Z}_n^\times = \{[a]_n \mid 1 \leq a \leq n, \gcd(a, n) = 1\}$. Therefore for every prime p and every positive integer n, we have

   $$|\mathbb{Z}_{p^n}^\times| = p^n - |\{a \mid 1 \leq a \leq p^n, p|a\}| = p^n - p^{n-1}.$$

   Hence

   $$|(\mathbb{Z}_9 \times \mathbb{Z}_5)^\times| = |\mathbb{Z}_9^\times||\mathbb{Z}_5^\times| = (9-3)(5-1) = (6)(4) = 24.$$

2. (5 points) Prove that $\mathbb{Q}[x]/\langle x^2 - 3\rangle \simeq \mathbb{Q}[\sqrt{3}]$ where $\mathbb{Q}[\sqrt{3}]$ is the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\sqrt{3}$.

   Let $\phi_{\sqrt{3}} : \mathbb{Q}[x] \to \mathbb{C}, \phi_{\sqrt{3}}(f(x)) := f(\sqrt{3})$ be the evaluation map. We know that $\phi_{\sqrt{3}}$ is a ring homomorphism, and its image is $\mathbb{Q}[\sqrt{3}]$. Therefore by the first isomorphism theorem we have that

   $$\mathbb{Q}[x]/\ker \phi_{\sqrt{3}} \simeq \mathbb{Q}[\sqrt{3}].$$

   As $\sqrt{3}$ is a zero of $x^2 - 3$, we have that $x^2 - 3 \in \ker \phi_{\sqrt{3}}$. Suppose $f(x) \in \ker \phi_{\sqrt{3}}$. By the long division, there are $q(x), r(x) \in \mathbb{Q}[x]$ such that

   $$f(x) = (x^2 - 3)q(x) + r(x) \quad \text{and} \quad \deg r < \deg(x^2 - 3).$$

   Thus $r(x) = a_0 + a_1 x$ for some $a_0, a_1 \in \mathbb{Q}$. Evaluating f at $\sqrt{3}$, we obtain that

   $$0 = r(\sqrt{3}) = a_0 + a_1\sqrt{3}.$$

   If $a_1 \neq 0$, then $\sqrt{3} = -\frac{a_0}{a_1}$. This is a contradiction as $\sqrt{3}$ is irrational. Therefore $a_1 = 0$, which implies that $a_0 = 0$. Hence $r(x) = 0$. This implies that $f(x) \in \langle x^2 - 3\rangle$. Altogether we deduce that $\ker \phi_{\sqrt{3}} = \langle x^2 - 3\rangle$. This finishes the proof.

3. (5 points) Suppose p is a prime number and $f(x) \in \mathbb{Z}_p[x]$ is a polynomial of degree 3. Use the long division for polynomials to prove that $|\mathbb{Z}_p[x]/\langle f(x)\rangle| = p^3$. For every $p(x)$ by the long division, there

are unique $q(x)$ and $r(x)$ in $\mathbb{Z}_p[x]$ such that

$$p(x) = f(x)q(x) + r(x) \quad \text{and} \quad \deg r < \deg f.$$

Notice that since p is prime, $\mathbb{Z}_p$ is a field, and so we are allowed to use the long division. Therefore

$$p(x) + \langle f(x)\rangle = r(x) + \langle f(x)\rangle$$

for some $r(x) \in \mathbb{Z}_p[x]$ that has degree at most 2.

Notice that if $r_1(x) + \langle f(x)\rangle = r_2(x) + \langle f(x)\rangle$ for some $r_1, r_2 \in \mathbb{Z}_p[x]$ with degree at most 2, then $r_1(x) - r_2(x) = f(x)g(x)$ for some $g(x)$. As $\deg f = 3$ and $\deg(r_1 - r_2) \geq 2$, we deduce that $r_1 - r_2 = 0$.

Overall we obtain that every element of $\mathbb{Z}_p[x]/\langle f(x)\rangle$ can be uniquely written as

$$(a_0 + a_1 x + a_2 x^2) + \langle f(x)\rangle$$

for some $a_0, a_1, a_2 \in \mathbb{Z}_p$. We have p choices for each one of the a_0, a_1, and a_2. Hence

$$|\mathbb{Z}_p[x]/\langle f(x)\rangle| = p^3.$$

4. Suppose m and n are positive integers and $\gcd(m, n) = 1$. Let $e : \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m$, $e(k) := k([1]_n, [1]_m)$. You can use without proof that e is a ring homomorphism.

(a) (3 points) Find the kernel of e.

$k \in \ker e$ if and only if $k[1]_n = [0]_n$ and $k[1]_m = [0]_m$. The latter holds if and only if $n|k$ and $m|k$. We know that $n|k$ and $m|k$ exactly when $\operatorname{lcm}(m, n)|k$. Since m and n are coprime, $\operatorname{lcm}(m, n) = mn$. Overall we deduce that $k \in \ker e$ if and only if $mn|k$. This means

$$\ker e = (mn)\mathbb{Z}.$$

(b) (4 points) Prove that e is surjective.

Notice that $e(n) = ([0]_n, [n]_m)$ and $e(m) = ([m]_n, [0]_m)$. Therefore the additive subgroup groups generated by $([0]_n, [n]_m)$ and $([m]_n, [0]_m)$ are subsets of the image of e. Since $\gcd(m, n) = 1$, $[n]_m$ is a unit in $\mathbb{Z}_m$, which implies that the group generated by $[n]_m$ is the entire $\mathbb{Z}_m$. Similarly the group generated by $[m]_n$ is the entire $\mathbb{Z}_n$. Therefore $\mathbb{Z}_n \times \{[0]_m\}$ and $\{0\} \times \mathbb{Z}_m$ are subsets of the image of e. Thus their sum is also a subset of the image of e, which implies that e is surjective.

(c) (3 points) Prove that $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}_n \times \mathbb{Z}_m$.

By the first isomorphism theorem, we have

$$\mathbb{Z}/\ker e \simeq \operatorname{Im} e.$$

Notice that $\ker e = (mn)\mathbb{Z}$ and $\operatorname{Im} e = \mathbb{Z}_n \times \mathbb{Z}_m$; and so the claim follows.