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

1. Answer the following questions and briefly justify your answers.
   (a) (1 points) True or false. Every integral domain is a field.

   No, for instance $\mathbb{Z}$ is an integral domain, but it is not a field.

   (b) (2 point) True or false. A field has exactly two ideals. This is true. We know that if an ideal contains a unit, it is the entire ring. In a field, every non-zero element is a unit. Hence there is only one non-zero ideal which is the entire ring. Since a field F is non-trivial, $F \neq \{0\}$. So F has exactly two ideals.

   (c) (3 points) Find the characteristic of $\mathbb{Z}_3 \times \mathbb{Z}_7$.

   In a finite unital ring, the characteristic is the additive order of the identity. So we need to find the smallest n such that $n([1]_3, [1]_7) = ([0]_3, [0]_7)$. We have

   $$n([1]_3, [1]_7) = ([0]_3, [0]_7) \Leftrightarrow ([n]_3 = [0]_3 \text{ and } [n]_7 = [n]_7) \Leftrightarrow (3|n \text{ and } 7|n) \Leftrightarrow 21|n.$$

   Hence the characteristic of this ring is 21.

   (d) (4 points) Find $|(\mathbb{Z}_{25} \times \mathbb{Z}_7)^\times|$.

   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

   $$|(\mathbb{Z}_{25} \times \mathbb{Z}_7)^\times| = |\mathbb{Z}_{25}^\times||\mathbb{Z}_7^\times| = (25-5)(7-1) = (20)(6) = 120.$$

2. Let's recall that $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{C}$.
   (a) (4 points) Prove that $\mathbb{Q}[x]/\langle x^2 + 1\rangle \simeq \mathbb{Q}[i]$.

   Let $\phi_i : \mathbb{Q}[x] \to \mathbb{C}, \phi_i(f(x)) := f(i)$ be the evaluation map. Then the image of ϕ_i is $\mathbb{Q}[i]$. Therefore by the first isomorphism theorem

   $$\mathbb{Q}[x]/\ker\phi_i \simeq \mathbb{Q}[i].$$

   Since i is a zero of $x^2 + 1$, $x^2 + 1$ is in the kernel of ϕ_i. We want to show that $\ker\phi_i = \langle x^2 + 1\rangle$. We have already showed that $\langle x^2 + 1\rangle \subseteq \ker\phi_i$. Now suppose that $f(x) \in \ker\phi_i$. By the long division, there are $q(x), r(x) \in \mathbb{Q}[x]$ such that

   $$f(x) = (x^2 + 1)q(x) + r(x) \quad \text{and} \quad \deg r < \deg(x^2 + 1).$$

   Hence $r(x) = a_0 + a_1 x$ for some $a_0, a_1 \in \mathbb{Q}$. Evaluating f at i, we deduce that $0 = r(i) = a_0 + a_1 i$. This implies that $a_0 = a_1 = 0$. Therefore $r(x) = 0$, and so $f(x) \in \langle x^2 + 1\rangle$. This completes the proof.

(b) (2 points) Prove that $\mathbb{Q}[x]/\langle x^2+1\rangle$ is a field.

By part (a) it is enough to show that $\mathbb{Q}[i]$ is a field. We already know that $\mathbb{Q}[i]$ is a subring of $\mathbb{C}$. So it is enough to show that every non-zero element of $\mathbb{Q}[i]$ is a unit. Suppose $a+bi$ is a non-zero element of $\mathbb{Q}[i]$ for some $a, b \in \mathbb{Q}$. Then

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

which is in $\mathbb{Q}[i]$. This completes the proof.

3. (4 points) Suppose p is prime. Prove that $x^{p^2} - x + 1$ has no zero in $\mathbb{Z}_p$.

By Fermat's little theorem, for every $a \in \mathbb{Z}_p$, we have $a^p = a$. Raising both side to power p, we get $a^{p^2} = (a^p)^p = a^p = a$. Therefore

$$a^{p^2} - a + 1 = a - a + 1 = 1 \neq 0$$

for every $a \in \mathbb{Z}_p$. The claim follows.

4. (4 points) Suppose $\alpha \in \mathbb{C}$ is a zero of a polynomial $p(x) \in \mathbb{Q}[x]$ of degree 3. Use the long division for polynomials to prove that $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 |\ a_0, a_1, a_2 \in \mathbb{Q}\}$.

By definition, $\mathbb{Q}[\alpha]$ is the image of the evaluation map $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{C}, \phi_\alpha(f(x)) := f(\alpha)$. Hence every element of $\mathbb{Q}[\alpha]$ is of the form $f(\alpha)$ for some $f(x) \in \mathbb{Q}[x]$. By the long division, there are $q(x), r(x) \in \mathbb{Q}[x]$ such that

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

Hence $r(x) = a_0 + a_1x + a_2x^2$ for some $a_0, a_1, a_2 \in \mathbb{Q}$. Evaluating f at α and using the assumption that $p(\alpha) = 0$, we obtain that

$$f(\alpha) = r(\alpha) = a_0 + a_1\alpha + a_2\alpha^2.$$

On the other hand, for every $a_i \in \mathbb{Q}$, we have that $a_0 + a_1\alpha + a_2\alpha^2 = \phi_\alpha(a_0 + a_1x + a_2x^2)$ is in the image of ϕ_α. The claim follows.

5. Let's recall that $\mathbb{Z}[i] := \{a+bi |\ a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.

(a) (2 points) Suppose p is a prime and there is a ring homomorphism $f : \mathbb{Z}[i] \to \mathbb{Z}_p$ such that $f(1) = 1$. Prove that there is $x \in \mathbb{Z}_p$ such that $x^2 = -1$.

Since f is a ring homomorphism,

$$f(i)^2 = f(i^2) = f(-1) = -f(1) = -1;$$

and so $f(i) \in \mathbb{Z}_p$ is a solution of $x^2 = -1$ in $\mathbb{Z}_p$.

(b) (4 points) Find a surjective ring homomorphism $f : \mathbb{Z}[i] \to \mathbb{Z}_{13}$ such that $3-2i \in \ker f$. (Notice that 8^2+1 is a multiple of 13.)

By part (a), we know that $f(i)$ is a zero of $x^2 = -1$. So we look for the solutions of this equation in $\mathbb{Z}_{13}$. We are given that 8 is a zero of $x^2 = -1$ in $\mathbb{Z}_3$, and so is -8. This means it might be legitimate to have either $f(i) = 8$ or $f(i) = -8$. In the first case, $f(3-2i) = 3 - 2 \times 8 = 0$. So that one should be a good choice for us, which means we let $f(a+bi) := a + 8b$. Let's check

why it is a ring homomorphism. For $a, b, c, d \in \mathbb{Z}$, we have

$$\begin{aligned} f((a+bi)+(c+di)) =& f((a+c)+(b+d)i) \\ =& (a+c)+8(b+d) = (a+8b)+(c+8d) \\ =& f(a+bi)+f(c+di). \end{aligned}$$

We also have

$$\begin{aligned} f((a+bi)(c+di)) =& f((ac-bd)+(ad+bc)i) \\ =& (ac-bd)+8(ad+bc), \end{aligned}$$

and

$$\begin{aligned} f(a+bi)f(c+di) =& (a+8b)(c+8d) \\ =& (ac-bd)+8(ad+bc); \end{aligned}$$

this implies that f is a ring homomorphism. We have already observed that $3-2i$ is in the kernel of f.