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

1. Answer the following questions and briefly justify your answers.
   (a) (2 point) Find all primes p such that $x-1$ is a factor of $x^5-2x^4+3x^3+5x^2+6$ in $\mathbb{Z}_p$.

   By the factor theorem, $x-1$ is a factor of $f(x)$ if and only if $f(1)=0$. Hence $x-1$ is a factor of $x^5-2x^4+3x^3+5x^2+6$ in $\mathbb{Z}_p[x]$ if and only if p divides $1-2+3+5+6=13$. Hence the only possible p is 13.

   (b) (3 points) True or false. $\mathbb{Z}[x]$ is a PID.

   No, it is not a PID as $\langle 2, x\rangle$ is not principal. Suppose to the contrary that it is a principal ideal, and it is generated by $f(x)$. Then there is $p(x) \in \mathbb{Z}[x]$ such that $2 = f(x)p(x)$. Comparing the degrees, we deduce that $f(x) = c \in \mathbb{Z}$ is a constant. Since $x \in \langle f(x)\rangle$, there is $q(x) \in \mathbb{Z}[x]$, such that $x = f(x)q(x) = cq(x)$. Comparing the leading coefficients we obtain that $c = \pm 1$. This means that $\langle 2, x\rangle = \langle \pm 1\rangle = \mathbb{Z}[x]$. Hence there are $r(x), s(x) \in \mathbb{Z}[x]$ such that $1 = 2r(x) + xs(x)$. Evaluating both sides at 0, we deduce that $1 = 2r(0)$ which is a contradiction as 1 is not even.

2. (5 points) Determine whether $f(x) := x^5-2x^4+5x^3-x+1$ has a zero in $\mathbb{Q}$. Justify your answer.

   Suppose $\frac{a}{b}$ is a zero of f and $\gcd(a,b)=1$. By the rational root criterion, a divides the constant term of f and b divides the leading coefficient of f. Therefore a and b divide 1. Hence $\frac{a}{b}=\pm 1$. We evaluate f at 1 and -1, and check whether or not we get zero. We have $f(1)=1-2+5-1+1=4\neq 0$ and $f(-1)=-1-2-5+1+1=-6\neq 0$. Therefore f does not have a rational zero.

3. Recall that $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$.
   (a) (4 points) Prove that $5+2i$ is irreducible in $\mathbb{Z}[i]$.
   (Hint: Think about $N(a+bi)=|a+bi|^2=a^2+b^2$.)

   Notice that for $z\in\mathbb{Z}[i]^\times$ if and only if there is $z'\in\mathbb{Z}[i]$ such that $zz'=1$. In this case, we have $N(z)N(z')=1$. As $N(z)$ and $N(z')$ are non-negative integers, we obtain that $N(z)=1$. The only points of $\mathbb{Z}[i]$ that have complex norm 1 are ± 1 and $\pm i$. Notice that these are units in $\mathbb{Z}[i]$. In particular, $5+2i$ is not a unit. Now suppose $5+2i=z_1z_2$. Comparing the norm of both sides we deduce that $29=N(z_1)N(z_2)$. As $N(z_i)$'s are non-negative integers, we deduce that either $N(z_1)=1$ or $N(z_2)=1$. This means either z_1 or z_2 is a unit in $\mathbb{Z}[i]$. Therefore $5+2i$ is irreducible in $\mathbb{Z}[i]$.

   (b) (4 points) Prove that $\mathbb{Z}[i]/\langle 5+2i\rangle$ is a field.

   We have proved that $\mathbb{Z}[i]$ is a PID. In a PID the ideal generated by an irreducible element is maximal. Hence $\langle 5+2i\rangle$ is a maximal ideal. The quotient ring by a maximal ideal of a unital commutative ring is a field. Hence $\mathbb{Z}[i]/\langle 5+2i\rangle$ is a field.

   (c) (2 points) Prove that the characteristic of $\mathbb{Z}[i]/\langle 5+2i\rangle$ is 29.

   Notice that $29=(5+21)(5-2i)\in\langle 5+2i\rangle$. Hence $29(1+\langle 5+2i\rangle)=0$. Since the additive order of 1 in the quotient ring is 29. This implies that the characteristic of the quotient ring is 29.

4. Suppose E is a field extension of $\mathbb{Z}_3$, and $\alpha \in E$ is a zero of $x^3 - x + 2$.
   (a) (6 points) Prove that $\mathbb{Z}_3[\alpha]$ is a field of order 27.

   By Fermat's little theorem, for every $i \in \mathbb{Z}_3$, we have that $i^3 - i + 2 = 2 \neq 0$. Hence $x^3 - x + 2$ does not have a zero in $\mathbb{Z}_3$. By the degree 2 or 3 irreducibility criterion, we have that $x^3 - x + 2$ is irreducible in $\mathbb{Z}_3[x]$. Since $x^3 - x + 2$ is monic and irreducible, and α is a zero of $x^3 - x + 2$, we deduce that $m_{\alpha,\mathbb{Z}_3}(x) = x^3 - x + 2$. Using the map of evaluation at α and the first isomorphism theorem, we have
   $$\mathbb{Z}_3[\alpha] \simeq \mathbb{Z}_3[x]/\langle x^3 - x + 2\rangle.$$
   Every element of $\mathbb{Z}_3[x]/\langle x^3 - x + 2\rangle$ can be uniquely written as $(a_0 + a_1 x + a_2 x^2) + \langle x^3 - x + 2\rangle$ for some $a_i \in \mathbb{Z}_3$. For each a_0, a_1, and a_2 we have 3 possibilities, and so we get $3^3 = 27$ elements in $\mathbb{Z}_3[\alpha]$.
   We know that if E is a field extension of F and $\alpha \in E$ is algebraic over F, then $F[\alpha]$ is a field. Hence $\mathbb{Z}_3[\alpha]$ is a field.

   (b) (2 points) Prove that $\alpha^{26} = 1$. (Hint: Think about $(\mathbb{Z}_3[\alpha])^{\times}$.)

   The group of units of $\mathbb{Z}_3[\alpha]$ has $27 - 1 = 26$ elements as $\mathbb{Z}_3[\alpha]$ is a field of order 27. Hence $\alpha^{26} = 1$. (Recall that if G is a finite group of order n, then for every $g \in G$ we have $g^n = 1$.)

   (c) (2 points) Prove that $x^3 - x + 2$ divides $x^{26} - 1$.

   α is a zero of $x^{26} - 1 \in \mathbb{Z}_3[x]$. Hence $m_{\alpha,\mathbb{Z}_3}(x) | x^{26} - 1$. As it is proved in part (a), the minimal polynomial $m_{\alpha,\mathbb{Z}_3}(x)$ of α over $\mathbb{Z}_3$ is $x^3 - x + 2$. Hence $x^3 - x + 2 | x^{26} - 1$.