Math 103B - HW-2 (solution)

TA : Shubham Sinha

February 24, 2020

All problems are from **A first course in Abstract Algebra** by John B. Fraleigh.

Problem set

1 Show that $x^p - x = x(x-1)\dots(x-(p-1))$ in $\mathbb{Z}_p[x]$. Use this to prove that $(p-1)! = -1$ in $\mathbb{Z}_p$.

Proof. We know (by Fermat's theorem) that for any $a \in \mathbb{Z}_p$, $a^p - a = 0$. Since $\mathbb{Z}_p$ is a field, by factor theorem, $x^p - x = x(x-1)\dots(x-(p-1))g(x)$. Thus by looking at degree and leading coefficient, we see that $g(x) = 1$.

Take $x = p$ in the identity (obtained by canceling x) $x^{p-1} - 1 = (x-1)\dots(x-(p-1)$. We thus obtain obtain $-1 = p^{p-1} - 1 = (p-1)!$ in $\mathbb{Z}_p$. □

2 Let $w = \frac{-1+\sqrt{-3}}{2}$ be third root of unity. Show that $\mathbb{Z}[w]$ is a subring of $\mathbb{C}$. Show that the field of fraction of $\mathbb{Z}[w]$ is $\mathbb{Q}[w]$.

Proof. Let $a + bw$ and $c + dw$ be elements in $\mathbb{Z}[w]$, we need to show that their sum and product is also in $\mathbb{Z}[w]$. Note that $w^3 = 1$ and $w^2 + w + 1 = 0$. Thus $(a + bw) + (c + dw) = (a + b) + (c + d)w \in \mathbb{Z}[w]$ and $(a + bw)(c + dw) = ac + (ad + bc)w + bdw^2 = ac + (ad + bc)w + bd(-1 - w) = (ac - bd) + (ad + bc - bd)w \in \mathbb{Z}[w]$.

Note that any element$(a+bw) \in \mathbb{Q}[w]$ can be written as $(r+sw)/n$ where $(r+sw) \in \mathbb{Z}[w]$ and $n \in \mathbb{Z}$. Thus it suffices to show that $\mathbb{Q}[w]$ is a field. It is clearly a ring (by argument above), we need to show that $(a + bw)^{-1}$ is an element in $\mathbb{Q}[w]$. It follows from noting that the complex conjugate $\bar{w} = w^2$ in $\mathbb{C}$ and the following calculation :

$$\frac{1}{a + bw} = \frac{(a + bw^2)}{(a + bw)(a + bw^2)} = \frac{(a - b) - bw}{a^2 + b^2 - ab} \in \mathbb{Q}[z].$$

Moreover note that $a^2 + b^2 - ab \neq 0$ whenever $(a + bw) \neq 0$. □

3 Find all primes p such that $x + 2$ is a factor of $f(x) = x^6 - x^4 + x^3 - x + 1$ in $\mathbb{Z}_p[x]$.

Answer. By factor theorem, $x+2$ is a factor of $f(x)$ (where $f(x)$ is a polynomial over a field) if and only if $f(-2) = 0$. Note that $f(-2) = 43$ which is prime. So $f(x) = 43 = 0$ in $\mathbb{Z}_p$ only when $p = 43$. $\square$

4 Factor $f(x) = x^3 - 2x + 1$ in $\mathbb{Z}_5[x]$ as a degree 1 and degree two polynomials.

Answer. Note that $f(1) = 0$, thus $x - 1$ is a factor. We have $f(x) = (x-1)(x^2 + x - 1)$ in $\mathbb{Z}_5[x]$. $\square$

5 How many degree 2 and degree 3 polynomials with no zeros are there in $\mathbb{Z}_2[x]$?

Answer. Note that in $\mathbb{Z}_2$, we have $y \neq 0 \implies y = 1$. Let $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ be a degree three polynomial in $\mathbb{Z}_2[x]$. The given conditions implies : $a_3 \neq 0$ (since $f(x)$ has degree 3), $f(0) = a_0 \neq 0$ and $f(1) = a_3 + a_2 + a_1 + a_0 \neq 0$. Thus in $\mathbb{Z}_2$, these conditions imply $a_0 = 1$, $a_3 = 1$ and $a_1 + a_2 = 1$. Thus all possible solutions of (a_1, a_2) are {(1,0),(0,1)}. Thus there are **two** such degree 3 polynomial.

Similar argument can be used to show that a degree two polynomial $f(x) = a_2x^2 + a_1x + a_0$ has no zeros if and only if $a_2 = a_1 = a_0 = 1$. Thus there is only **one** such polynomial. $\square$

6 Prove that the following polynomials are irreducible in $\mathbb{Q}[x]$:
(a) $f(x) = x^3 - 3x^2 + 3x + 4$

Proof. Note that since it is a degree 3 polynomial, it is irreducible if and only if $f(x)$ has no zeros. Using Gauss' lemma we need to show irreducibility in $\mathbb{Z}[x]$. Note that any integer root a of $f(x)$ must satisfy $a|4$. Checking all (positive and negative) factors of 4 we conclude that $f(x)$ has no integer root, hence it is irreducible. $\square$

(b) $f(x) = x^n + 12$

Proof. Use Eisenstein's criterion with $p = 3$. The conditions are satisfied since $f(x)$ is , $3|12$,, $3^2 \not| 12$ an rest of the coefficients are 0. $\square$

(c) $f(x) = x^5 - 10x^3 + 25x^2 - 51x + 2017$

Proof. Reducing $f(x)$ modulo $p = 5$, we get $\bar{f}(x) = x^5 - x + 2$ which is known to be irreducible. Hence $f(x)$ is irreducible in $\mathbb{Z}[x]$. $\square$

7 (a) Prove that $f(x) = x^5 - 3x^3 + 6x^2 + 9x - 21$ is irreducible in $\mathbb{Q}[x]$.

Proof. It follows from Eisenstein's criterion for prime $p = 3$, since 3 divides all the coefficients other that that of x^5, and $3^2 \not| 21$. $\square$

(b) Let α be a real root of $f(x)$ in $\mathbb{R}$. Suppose $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{R}$ be the evaluation homomorphism. Prove that $\ker(\phi_\alpha) = \langle f(x) \rangle$.

Proof. We know that ker of a ring homomorphism is always an ideal.Moreover, we know that all ideal in $\mathbb{Q}[x]$ are principle (i.e it is of the form $\langle g(x) \rangle$). Thus $\ker(\phi_\alpha) = \langle g(x) \rangle$ for some polynomial g.

Since $\phi_\alpha(f(x)) = f(\alpha) = 0$, we see that $f \in \ker = \langle g(x) \rangle$. We conclude that $f(x) = g(x)h(x)$ for some polynomial $h(x)$. Since f is irreducible and $g(x)$ is not constant (since $g(\alpha) = 0$), we conclude that $h(x)$ is constant. Thus $\langle f(x) \rangle = \langle g(x) \rangle = \ker(\phi_\alpha)$. □

8 (a) Show that $A = \{\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} : a, b \in \mathbb{Q}\}$ is a subring of $M_2(\mathbb{Q})$.

Proof. It is clearly closed under matrix addition. We will show that it is closed under multiplication.

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \times \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} ac + 2bd & 2(ad + bc) \\ (ad + bc) & (ac + 2bd) \end{bmatrix} \in A$$

□

(b) Prove that $f : \mathbb{Q}[\sqrt{2}] \to A$ given by $f(a + b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ is a ring isomorphism.

Proof. Note that $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$, which matches with the corresponding matrix multiplication, i.e $f((a+b\sqrt{2})(c+d\sqrt{2})) = f((a+b\sqrt{2})) \times f((c+d\sqrt{2}))$. It is easy to see that $f((a + b\sqrt{2}) + (c + d\sqrt{2})) = f((a + b\sqrt{2})) + f((c + d\sqrt{2}))$. Hence f is a homomorphism. It is bijective since $\phi : A \to \mathbb{Q}[\sqrt{2}]$ given by $\phi(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}) \to (a + \sqrt{2}b)$ is the inverse map of f. □

Chapter 22

17 Use Fermat's theorem to find zeros in $\mathbb{Z}_5$ of $f(x) = 2x^{219} + 3^{74} + 2x^{57} + 3x^{44}$.

Answer. By Fermat's theorem, $a^5 \equiv a$ for $a \in \mathbb{Z}_5$. Note that $a^4 \equiv 1$ when $a \neq 0$ in $\mathbb{Z}_5$.

Observe that $f(0) = 0$, hence 0 is a zero of $f(x)$. Let $0 \neq a \in \mathbb{Z}_5$ be a root of $f(x)$, then $0 = f(a) = 2a^{219} + 3a^{74} + 2a^{57} + 3a^{44} = 2a^3 + 3a^2 + 2a + 3 = (2a + 3)(a^2 + 1) = (2a + 3)(a - 2)(a - 3)$. Here 1 is the only root of $(2a + 3) = 0$. Note that since $\mathbb{Z}_5$ is a field, the above equation implies $a \in \{1, 2, 3\}$. The set of zeros is $\{0, 1, 2, 3\}$. □

Chapter 23

34 Show that for p a prime, the polynomial $x^p + a$ in $\mathbb{Z}_p[x]$ is not irreducible for any $a \in \mathbb{Z}_p$.

Proof. By Fermat's theorem, $(-a)^p = (-a)$ in $\mathbb{Z}_p$, thus $x = (-a)$ is a zero of the polynomial $x^p + a$. Hence it can not be irreducible for any a. □

37 (c) Show that $f(x) = x^3 + 17x + 36$ is irreducible in $\mathbb{Q}[x]$.

Proof. Reducing the polynomial mod $p = 5$, we get $\bar{f}(x) = x^3 + 2x + 1 \in \mathbb{Z}_5[x]$. It is enough to shoe that $\bar{f}$ is irreducible in $\mathbb{Z}_5[x]$. Since degree of polynomial is 3, it is enough to show that $\bar{f}(x)$ does not have a root.

So we evaluate and see $\bar{f}(0) = 1, \bar{f}(1) = 4, \bar{f}(2) = 3, \bar{f}(3) = 4, \bar{f}(4) = 3$, hence $\bar{f}$ is irreducible in $\mathbb{Z}_5[x]$ which implies $f(x)$ is irreducible in $\mathbb{Z}[x]$ (and by Gauss' lemma in $\mathbb{Q}[x]$).

□