Modern Algebra HW 9

Michael Nameika

November 2022

Section 20 Problems

3. Find a generator for the multiplicative group $\mathbb{Z}_{17}$

I claim that $3 \in \mathbb{Z}_{17}$ is a generator for $\langle \mathbb{Z}_{17}^{\neq 0}, \cdot \rangle$. To see this, notice the following:

$$\begin{aligned}
3 \times 3 &= 9 \mod 17 \\
9 \times 3 &= 10 \mod 17 \\
10 \times 3 &= 13 \mod 17 \\
13 \times 3 &= 5 \mod 17 \\
5 \times 3 &= 15 \mod 17 \\
15 \times 3 &= 11 \mod 17 \\
11 \times 3 &= 16 \mod 17 \\
16 \times 3 &= 14 \mod 17 \\
14 \times 3 &= 8 \mod 17 \\
8 \times 3 &= 7 \mod 17 \\
7 \times 3 &= 4 \mod 17 \\
4 \times 3 &= 12 \mod 17 \\
12 \times 3 &= 2 \mod 17 \\
2 \times 3 &= 6 \mod 17 \\
6 \times 3 &= 1 \mod 17
\end{aligned}$$

Notice that every element of $\mathbb{Z}_{17}^{\neq 0}$ appears in the list above. That is, 3 is a generator for $\mathbb{Z}_{17}^{\neq 0}$.

4. Using Fermat's theorem, find the remainder of 3^{47} when it is divided by 23.

Notice that 3 is prime and 23 is prime, so clearly, $\gcd(3, 23) = 1$, so Fermat's theorem applies. Now, notice $3^{47} = 3^3(3^{22})^2$. By Fermat's theorem, we have $3^{22} \equiv 1 \mod 23$, so we have $3^3(3^{22})^2 \equiv 3^3(1)^2 \equiv 3^3 \equiv 4 \mod 23$.
That is,

$$3^{47} \equiv 4 \mod 23$$

10. Use Euler's generalization of Fermat's theorem to find the remainder of 7^{1000} when divided by 24.

Begin by noticing that $\gcd(7, 24) = 1$, so Euler's Generalization of Fermat's theorem applies, hereafter, Euler's theorem. By Euler's theorem, we have $7^{\phi(24)} \equiv 1 \mod 24$. From problem 7 (not shown), we have

$\phi(24) = 8$, so $7^8 \equiv 1 \mod 24$. Now notice

$$7^{1000} = (7^8)^{125}$$
$$(7^8)^{125} \equiv 1^{125} = 1 \mod 24$$

That is,

$$7^{1000} \equiv 1 \mod 24$$

Section 22 Problems

5. How many polynomials are there of degree ≤ 3 in $\mathbb{Z}_2[x]$? (Include 0.)

I claim that there are $2^{3+1} = 2^4 = 16$ polynomials of degree ≤ 3 in $\mathbb{Z}_2[x]$. To see this, observe the following list of polynomials:

$$\begin{aligned}
&0,\ 1\\
&x,\ 1+x\\
&x^2,\ x+x^2,\ 1+x+x^2,\ 1+x^2\\
&x^3,\ x^2+x^3,\ x+x^2+x^3,\ 1+x+x^2+x^3\\
&1+x^3,\ 1+x+x^3,\ x+x^3,\ 1+x^2+x^3
\end{aligned}$$

Which contains 16 polynomials.

21. Consider the evaluation homomorphism $\phi_5 : \mathbb{Q}[x] \to \mathbb{R}$. Find six elements in the kernel of the homomorphism ϕ_5.

Notice that the following polynomials in $\mathbb{Q}[x]$ are in the kernel of ϕ_5:

$$\begin{aligned}
f(x) &= x - 5\\
g(x) &= x^2 - x - 20\\
h(x) &= x^3 - x^2 - x - 95\\
p(x) &= -4x^2 + 18x + 10\\
q(x) &= -\frac{90443}{30}x^3 + \frac{107014}{5}x^2 - \frac{970351}{30}x + 3501
\end{aligned}$$

and finally,

$$l(x) = \frac{339491546130958040001}{100000000000000}x^7 - \frac{1018568402170152619}{1250000000000}x^6 + \frac{153479601104168565 61}{200000000000}x^5 - \frac{4482664476519146389}{12500000000}x^4 + \cdots$$

$$\cdots \frac{216101094526043850 23}{25000000000}x^3 - \frac{2005784801822241183}{2000000000}x^2 + \frac{214138209023811458 61}{50000000000}x + 1000$$

27. Let F be a field of characteristic zero and let D be the formal polynomial differentiation map, so that

$$D(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_1 + 2 \cdot a_2x + \cdots + n \cdot a_nx^{n-1}.$$

a. Show that $D : F[x] \to F[x]$ is a group homomorphism of $\langle F[x], +\rangle$ into itself. Is D a ring homomorphism?
Proof: We must show that for $f(x), g(x) \in F[x]$, $D(f(x)+g(x)) = D(f(x))+D(g(x))$. Well, let $f(x) \in F[x]$ be defined as $f(x) = a_0+a_1x+\cdots+a_nx^n$ and similarly for $g(x) \in F[x]$, $g(x) = b_0+b_1x+\cdots+b_nx^n$ where $a_i, b_i \in F$ for all $0 \le i \le n$. Begin by considering $D(f(x) + g(x))$:
By definition, we have

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n$$

and so

$$\begin{aligned} D(f(x) + g(x)) &= (a_1 + b_1) + 2(a_2 + b_2)x + \cdots + n(a_n + b_n)x^{n-1} \\ &= a_1 + 2a_2x + \cdots + na_nx^{n-1} + b_1 + 2b_2x + \cdots + nb_nx^{n-1} \\ &= D(f(x)) + D(g(x)) \end{aligned}$$

So D is a group homomorphism into itself.

However, D is not a ring homomorphism. To see this, we must show that $D(f(x) \cdot g(x)) \neq D(f(x)) \cdot D(g(x))$. Well,

$$\begin{aligned} f(x) \cdot g(x) &= (a_0 + a_1x + a_2x^2 + \cdots a_nx^n)(b_0 + b_1x + b_2x^2 + \cdots b_nx^n) \\ &= a_0b_0 + a_0b_1x + a_0b_2x^2 + \cdots + a_0b_nx^n + \cdots \\ &\quad a_1b_0 + a_1b_1x + a_1b_2x^2 + \cdots + a_1b_nx^n + \cdots \\ &\quad \vdots \\ &\quad a_nb_0 + a_nb_1x + a_nb_2x^2 + \cdots a_nb_nx^n \end{aligned}$$

Then

$$\begin{aligned} D(f(x) \cdot g(x)) &= a_0b_1 + 2a_0b_2x + \cdots + na_0b_nx^{n-1} + \cdots \\ &\quad a_1b_1 + 2a_1b_2x + \cdots + na_1b_nx^{n-1} + \cdots \\ &\quad \vdots \\ &\quad a_nb_1 + 2a_nb_2x + \cdots + na_nb_nx^{n-1} \end{aligned}$$

Not let us inspect $D(f(x))D(g(x))$:

$$\begin{aligned}
D(f(x))D(g(x)) &= (a_1 + 2a_2x + \cdots + na_nx^{n-1})(b_1 + 2b_2x + \cdots nb_nx^{n-1}) \\
&= a_1b_1 + 2a_1b_2x + \cdots na_1b_n + \cdots \\
& 2a_2b_1x + 4a_2b_2x^2 + \cdots + 2na_2b_nx^n + \cdots \\
& \vdots \\
& na_nb_1x^{n-1} + 2na_nb_2x + \cdots + n^2a_nb_nx^{2n-2} \\
&\neq D(f(x)g(x))
\end{aligned}$$

So D is not a ring homomorphism.

b. Find the kernel of D.
Clearly, $f(x) = a \in \text{Ker}(D)$ for all $a \in F$. Additionally, since F is a field, we have F is an integral domain, so any polynomial of degree ≥ 1 is not a zero divisor, so $\ker(D) = \{f(x) = a \mid f(x) \in F[x], a \in F\} = F$.

c. Find the image of $F[x]$ under D.
Clearly, we have $\text{Im}(F[x]) = F[x]$ since for any $f(x) \in F[x]$, we can find a $g(x) \in F[x]$ such that $D(g(x)) = f(x)$. In fact, if $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $g(x) = c + a_0x + a_1/2x^2 + \cdots + a_n/n!x^{n+1}$ where $c \in F$.