**Вариант №1**

; ; .

1. **Разложим многочлен *f(x)* на неприводимые множители над полем**
2. **Построим конечное поле . Составим таблицы сложения и умножения.**

Из-за своей громоздкости таблицы представлены в прикреплённом Excel файле.

1. **Решить при условии что: ; .**

**Ответы на вопросы:**

1. **Дайте определение группы, кольца, поля.**

**Группа** (M, \*) – это множество, на котором задана одна операция \* , удовлетворяющая следующим условиям (аксиомы группы):

• G0 аксиома замкнутости ∀ 𝑥, 𝑦 ∈ 𝑀 𝑥 ∗ 𝑦 ∈ 𝑀

• G1 аксиома ассоциативности ∀ 𝑥, 𝑦, 𝑧 ∈ 𝑀 (𝑥 ∗ 𝑦) ∗ 𝑧 = 𝑥 ∗ (𝑦 ∗ 𝑧)

• G1’ аксиома коммутативности ∀ 𝑥, 𝑦 ∈ 𝑀 𝑥 ∗ 𝑦 = 𝑦 ∗ 𝑥

• G2 аксиома существования нейтрального элемента ∃𝜃 ∈ 𝑀 ∀ 𝑥 ∈ 𝑀 𝑥 ∗ 𝜃 = 𝜃 ∗ 𝑥 = 𝑥

• G3 аксиома существования симметричного элемента ∀ 𝑥 ∈ 𝑀 ∃𝑥′ ∈ 𝑀 𝑥 ∗ 𝑥′ = 𝑥′ ∗ 𝑥 = 𝜃

**Кольцо** (К, +, ∙) – это множество, на котором заданы две операции: + - сложение и ∙ - умножение, удовлетворяющие следующим условиям:

1. (К, +) – абелева (коммутативная) группа;

2. (К, ∙) - полугруппа;

3. Операции + и ∙ связаны свойством дистрибутивности

∀ 𝑥,𝑦,𝑧∈𝑀 (𝑥+𝑦)∙𝑧=𝑥∙𝑧+𝑦∙𝑧 (правая дистрибутивность)

∀ 𝑥,𝑦,𝑧∈𝑀 𝑧∙(𝑥+𝑦)=𝑧∙𝑥+𝑧∙𝑦 (левая дистрибутивность)

**Поле** (Р, +, ∙) – это множество, на котором заданы две операции: + - сложение и ∙ - умножение, удовлетворяющие следующим условиям:

1. (Р, +) – абелева (коммутативная) группа;

2. (Р\{0}, ∙) - коммутативная группа;

3. Операции + и ∙ связаны свойством дистрибутивности.

1. **Приведите примеры конечной группы, конечного кольца, конечного поля**

G = – конечная группа, все элементы которых можно представить как последовательные степени некоторого фиксированного элемента a.

G = {0, 2, 4, 6} – конечное кольцо, операция сложения и умножения по модулю 8 даёт пример кольца без единицы и с делителями нуля.

G = {0, 1, 2} – конечное поле, сложения и умножения определены как сложение и умножение чисел по модулю 3.

1. **Дайте определение подгруппы, подкольца**

Если (𝐺,∗) – группа, 𝐻⊆𝐺 и (𝐻,∗) так же образует группу, то (𝐻,∗) **называют подгруппой** (𝐺,∗) и пишут 𝐻<𝐺

𝐻 подгруппа 𝐺 тогда и только тогда, когда для любых 𝑎,𝑏∈𝐻 выполняется условие 𝑎∙𝑏−1∈𝐻

**Подкольцо** – такое подмножество кольца, которое относительно операций, заданных в кольце, само образует кольцо.

Критерий подкольца: К подкольцо R тогда и только тогда, когда

(1) ∀𝑥,𝑦∈𝐾 ∶ 𝑥−𝑦∈𝐾

(2) ∀𝑥,𝑦∈𝐾 ∶ 𝑥∙𝑦∈𝐾

1. **Дайте определение фактор-группы. Постройте фактор-группу**

Множество всех смежных классов группы 𝐺 по подгруппе 𝐻 называется фактор-множеством 𝐺/𝐻

Пусть 𝐻⊲𝐺. Зададим на фактор множестве 𝐺/𝐻 операцию 𝑥𝐻⋅𝑦𝐻=(𝑥⋅𝑦)𝐻

Фактор множество относительно заданной операции образует группу, которую называют **фактор-группой**

1. **Дайте определение идеала кольца**

Идеал – такое подмножество 𝐼 кольца 𝐾 , для которого выполнено

(1) ∀𝑥,𝑦∈𝐼 ∶ 𝑥−𝑦∈𝐼

(2) ∀𝑥∈𝐾 ∀𝑖∈𝐼: 𝑥∙𝑖∈𝐼

1. **Какие многочлены называются неприводимыми над кольцом К**

f(x) ∈ K[x] K- область целостности

Многочлен f(x) называется приводимым над K, если его можно представить в виде двух множителей:

f(x) = g(x) \* h(x)

deg g < deg f иначе f(x) – неприводимый

deg h < deg f

1. **Сколько элементов содержит фактор-кольцо , является ли оно полем?**

Фактор кольцо не будет являться полем так как содержит элементов.