Solutions Single Choice 7

---

1. Which of the following rings is not isomorphic to the others?

(a) $\mathbb{F}_3[X]/(X^2 + X + 2)$

(b) $\mathbb{F}_3[X]/(X^2 + 2X + 2)$

(c) $\mathbb{F}_3[X]/(X^2 + X + 1)$

(d) $\mathbb{F}_9$

Solution: The solution if (c). The polynomial $X^2 + X + 2$ is irrecucible over $\mathbb{F}_3$: none of the elements of $\mathbb{F}_3$ are a zero and since the polynomial has degree 2 it is irreducible. Hence we know from the lectures that $\mathbb{F}_3[X]/(X^2 + X + 2)$ is a finite field. All the elements of $\mathbb{F}_3[X]/(X^2 + X + 2)$ are polynomials of degree < 2 with coefficients in $\mathbb{F}_3$, so there are in total 9 elements in $\mathbb{F}_3[X]/(X^2 + X + 2)$. Hence $\mathbb{F}_3[X]/(X^2 + X + 2) \cong \mathbb{F}_9$.

Similarly, the polynomial $X^2 + 2X + 2$ has no zeros in $\mathbb{F}_3$ and since it has degree 2 it is irreducible over $\mathbb{F}_3$. A similar argument as before shows that $\mathbb{F}_3[X]/(X^2 + 2X + 2) \cong \mathbb{F}_9$.

For the last polynomial, note that $X^2 + X + 1 = (X + 2)^2$, so it is reducible and not an integral domain: note that $\overline{0} \neq \overline{X + 2} \in \mathbb{F}_3[X]/(X^2 + X + 1)$, but

$$\overline{(X + 2)} \cdot \overline{(X + 2)} = \overline{X^2 + X + 1} = \overline{0}.$$

2. How many irreducible factors does the polynomial $X^9 - X$ have over $\mathbb{F}_3$?

(a) 2

(b) 4

(c) 6

(d) 9

Solution: The answer is (c). The polynomial $X^9 - X$ is separable over $\mathbb{F}_3$, so it does not have multiple irreducible factors. The irreducible factors of degree 1 are the zeros in $\mathbb{F}_3$, so $0, 1$ and 2 (note that $2^8 - 1 = 256 - 1 \equiv 0 \pmod 3$).

Next we consider the irreducible factors of degree > 1. Let $f(X)$ be such a factor. From the lectures we know that the splitting field of $X^9 - X$ has degree 2 over $\mathbb{F}_3$. If a is a zero of f, then $[\mathbb{F}_3(a) : \mathbb{F}_3] \mid 2$, so $\deg(f) = [\mathbb{F}_3(a) : \mathbb{F}_3] = 2$. Since $9 = 3 \cdot 1 + 3 \cdot 2$, the polynomial $X^9 - X$ has 3 irreducible factors of degree 2 and 3 of degree 1, alltogether 6.

3. Which of the following elements is a generator of $\mathbb{F}_{19}^{\times}$

(a) $\overline{1}$

(b) $\overline{3}$

(c) $\overline{7}$

(d) $\overline{9}$

Solution: The answer is (b). The group $\mathbb{F}_{19}^{\times}$ is cyclic of order 18. Hence the element $\overline{1}$ is not a generator. Note that $\overline{7}^3 = \overline{1}$, so it has order less than 18. On the other hand, $(\overline{3}^3)^2 = \overline{8}^2 = \overline{7} \neq 1$, and hence $\overline{3}^9 = -\overline{1}$, so that $\overline{3}$ has order 18 and is a generator. Since $\overline{3}^2 = \overline{9}$, the element $\overline{9}$ has order 9.

4. Let p be a prime number. Which of the following statements are false?

(a) There exists a field of order p^p.

(b) If $F : \mathbb{F}_{p^p}$ is a finite field extension, then $F : \mathbb{F}_{p^p}$ is simple.

(c) The unit group $\overline{\mathbb{F}}_p^{\times}$ is cyclic.

(d) If a field F is a splitting field of $X^{p^p} - X \in \mathbb{F}_p[X]$ over $\mathbb{F}_p$, then F has p^p elements.

Solution: Statement (c) is false: Each element of $\overline{\mathbb{F}}_p^{\times}$ lies in a finite field extension of $\mathbb{F}_p$, so it also lies in a finite field. Hence it generates a finite subgroup of $\overline{\mathbb{F}}_p^{\times}$. But since $\overline{\mathbb{F}}_p$ is not finite, there does not exist an element generating its whole unit group. The remaining parts were done in the lecture (where we replaced p^n by p^p).

5. How many irreducible polynomials of degree 2 are there over $\mathbb{F}_2$?

(a) 1

(b) 2

(c) 3

(d) 4

Solution: There is only one, namely $X^2 + X + 1$. By checking that none of the elements of $\mathbb{F}_2$ is a zero, we conclude that it is irreducible.

Assume there is another one: say $aX^2 + bX + c$, with $a, b, c \in \mathbb{F}_2$ and $a \neq 0$ is irreducible. Then $c = 1$, as otherwise we could factor X out. If $b = 0$ then $X^2 + 1 = (X + 1)^2$.