2019级答案

一、单项选择题（每小题 2 分，共 20 分）

1. D　2. A　3. D　4. B　5. B

6. D　7. D　8. C　9. D　10. D

二、简答题（每小题 2 分，共 20 分）

1. (1 5 3 6 4), 偶置换

2.

+	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

×	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

3. GF(3)，GF(9)，GF(27)

4. $(x+1)^9$

5. $\{1, -1\}$

6. (1)(3)(6)

7. $x^{12}+1$

8. x^3+x^2+1, x^3+x+1

9. 不是；不是

10. 是

三、解答题（共 30 分）

1. （10 分）

(1) $H=\{I, (1\ 4\ 2), (1\ 2\ 4)\}$

(2) H, $\{(1\ 2\ 3), (2\ 3\ 4), (1\ 4)(2\ 3)\}$, {(1 3 2), (1 3)(2 4), (1 3 4)}, {(2 4 3), (1 4 3), (1 2)(3 4)}

2. （10 分）

商式：bx^2+bx+a

余式：ax^2+b

3. （10 分）解：

四、 证明题（共 30 分）

1. （15 分）

证明：（1）因为 G 是循环群，则一定存在一个生成元 a，G=(a)，对于 G'任意的元素 b'，在 G 中一定对应一个 a^k，满足$\sigma(a^k)=b'$，根据同态性，则 $b'=\sigma(a^k)=\sigma(a^{k-1}\cdot a)=\sigma(a^{k-1})\sigma(a)=\sigma(a^{k-2}\cdot a)\sigma(a)=\sigma(a^{k-2})\sigma(a)^2=\ldots\ldots=\sigma(a)^k$，因此在 G'中任意的元素可由$\sigma(a)$生成，故 G'也是循环群。

（2）①H 非空。根据同态映射的性质， G 中有单位元 1，满足 $\sigma(1)=\tau(1)=1'$，1' 为 G'的单位元。

②对于任意的 a、b∈H，则有$\sigma(a)=\tau(a)$，$\sigma(b)=\tau(b)$，则$\sigma(b)^{-1}=\tau(b)^{-1}$，则$\sigma(b^{-1})=\sigma(b)^{-1}=\tau(b)^{-1}=\tau(b^{-1})$，因此$\sigma(ab^{-1})=\sigma(a)\sigma(b^{-1})=\tau(a)\tau(b^{-1})=\tau(ab^{-1})$，故 $ab^{-1}\in H$，因此 H 是 G 的子群。

（3）a 的周期可能有限，也可能无限。例如：设 G 是整数加法群，G'={-1,1,-i,i}复数乘法群；同态映射$\sigma(n)=i^n$, 显然$\sigma(0)=i^0=1$,1 的周期为 1，0 的周期有限也为 1； $\sigma(1)=i$，i 的周期为 4，而 1 的周期是无限的。

2. （10 分）

证明：须找到 GF（P^n）上一个 m 次质式。对任意 n ≥1，唯一存在 GF（P^n）。又因 n|mn，故 GF（P^n）是 GF（P^{nm}）子域。将$\Phi_{P^{mn-1}}(x)$看做 GF（P^n）上多项式。取它在 GF（P^n）上一不可约因式$\varphi(x)$，设次$\varphi(x)$＝r。因 GF（P^{mn}）中元都是 $xP^{mn}-x=0$ 的根，$\varphi(x)|x^{P^{mn}-x}$。故$\varphi(x)$在 GF（P^{mn}）上有根。设ξ为其中一个。令 F＝GF（P^n），规定 F［x］到 GF（P^{mn}）的一个映射如下：

$$\sigma(f(x))=f(\xi)$$

参照讲义上的证明过程容易验证：σ是 F［x］到 GF（P^{mn}）上的同态映射。核为$\varphi(x)F[x]$。

故

$$F[x]/\varphi(x)F[x]\cong GF(P^{mn})$$

因次$\varphi(x)=r$，故 F［x］/$\varphi(x)$F[x]中可做为剩余类代表元的是低于 r 次的多项式。共$(P^n)^r$个。

所以，F[x]/ $\varphi(x)$F[x]是 P^{nr} 元域。但 F[x]/ $\varphi(x)$F[x] $\cong$ GF(P^{mn})，F[x]/ $\varphi(x)$F[x]又应是 P^{mn} 元域，∴r=m。∴$\varphi(x)$便是 GF（P^n）上的一个 m 次质式。∴GF（P^n）上必有 m 次质式。

3. （5 分）

反证法