Solutions 2016-03-21

1. (a) $\psi(wz) = \dfrac{wz}{|wz|} = \dfrac{wz}{|w||z|} = \dfrac{w}{|w|}\cdot\dfrac{z}{|z|} = \psi(w)\psi(z) \quad \forall w,z \in \mathbb{C}^\iota$.

(b) $\ker\psi = \{z\in\mathbb{C}^\iota \mid z = |z|\} = \mathbb{R}_{>0}$ shows that, for any $z \in \mathbb{C}^\iota$,

$z(\ker\psi) = \mathbb{R}_{>0}z$ is the ray from 0 (but not containing 0) through z.

(c) The group morphism $\psi: \mathbb{C}^\iota \longrightarrow \mathbb{S}^1$ induces a group isomorphism

$$\overline{\psi}: \mathbb{C}^\iota/\ker\psi \xrightarrow{\sim} \operatorname{im}\psi, \quad \overline{\psi}(z(\ker\psi)) = \psi(z) = \frac{z}{|z|}.$$

As $\ker\psi = \mathbb{R}_{>0}$ and $\operatorname{im}\psi = \mathbb{S}^1$, $\overline{\psi}$ is an isomorphism from $\mathbb{C}^\iota/\mathbb{R}_{>0}$ to $\mathbb{S}^1$.

2. (a) Let $N = \{ n \in \mathbb{N} \mid 1 \le n \le 9 \wedge \exists G \text{ non-abelian with } |G| = n \}$.

Since D_3 and D_4 are non-abelian groups of order 6 and 8 respectively, we have $\{6,8\} \subset N$. Since the trivial group is abelian, every group of prime order is cyclic and hence abelian, and every group of prime squared order is abelian, we conclude that $\{6,8\} = N$.

(b) Applying the Fundamental Theorem for finitely generated abelian groups, and setting $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, we obtain the following classification of $Ab_{\le 9}$:

$n = 1$	$\mathbb{Z}_1$	$n = 6$	$\mathbb{Z}_2 \times \mathbb{Z}_3$
$n = 2$	$\mathbb{Z}_2$	$n = 7$	$\mathbb{Z}_7$
$n = 3$	$\mathbb{Z}_3$	$n = 8$	$\mathbb{Z}_8,\ \mathbb{Z}_2\times\mathbb{Z}_4,\ \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$
$n = 4$	$\mathbb{Z}_4,\ \mathbb{Z}_2\times\mathbb{Z}_2$	$n = 9$	$\mathbb{Z}_9,\ \mathbb{Z}_3\times\mathbb{Z}_3$
$n = 5$	$\mathbb{Z}_5$		

3. $\sigma = (1\,9\,11\,5\,3\,8)(2\,10\,6\,7\,4)$

$ct(\sigma) = (5,6)$

$o(\sigma) = \operatorname{lcm}(5,6) = 30$

$|K(\sigma)| = |ct^{-1}(5,6)| = \binom{11}{5} 4!\,5! = \frac{11!}{\cancel{5!}6!} 4!\cancel{5!} = 11\cdot 10\cdot 9\cdot 8\cdot 7\cdot 1\cdot 2\cdot 3\cdot 4 =$

$= 1'130'976$.

$|C(\sigma)| = \frac{|S_{11}|}{|K(\sigma)|} = \frac{\cancel{11!}\cdot 6!}{\cancel{11!}\cdot 4!} = 6\cdot 5 = 30$.

4. (a) The map $\varphi : \mathbb{Z} \to R$, $\varphi(n) = n1$ is a ring morphisms, because

$\varphi(m+n) = (m+n)1 = (m1)(n1) = \varphi(m)\varphi(n)$,

$\varphi(mn) = (mn)1 = m(n1) = (m1)(n1) = \varphi(m)\varphi(n)$, and

$\varphi(1) = 11 = 1$.

It is unique, because every ring morphism $\psi : \mathbb{Z} \to R$ satisfies $\psi(x+y) = \psi(x) + \psi(y)$ and $\psi(1) = 1$, whence

$\psi(n) = \psi(n1) = n\psi(1) = n1 = \varphi(n) \quad \forall n \in \mathbb{Z}$.

(b) For all $n \in \mathbb{Z}$ we have $\varphi(n) = n1_S = n(1+2\mathbb{Z}, 1+3\mathbb{Z}, 1+5\mathbb{Z}) =$
$= (n+2\mathbb{Z}, n+3\mathbb{Z}, n+5\mathbb{Z})$.

Thus $n \in \ker\varphi \Leftrightarrow 2|n \wedge 3|n \wedge 5|n \Leftrightarrow 30|n$. So $\ker\varphi = 30\mathbb{Z}$.

$\operatorname{im}\varphi \subset S$ and $|\operatorname{im}\varphi| = |\mathbb{Z}/\ker\varphi| = 30$ and $|S| = 30$ shows that $\operatorname{im}\varphi = S$.

(c) $A = \mathbb{Z}/\ker\varphi = \mathbb{Z}/30\mathbb{Z}$, $B = \operatorname{im}\varphi = S = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

5. (a) A domain is a commutative ring R such that $1 \neq 0$ and $xy = 0 \Rightarrow x = 0 \vee y = 0$.

(b) It suffices to show that $X^2+Y^2-1 \in \operatorname{irr}(\mathbb{C}[X,Y])$, since then X^2+Y^2-1 is prime, whence R is a domain. Irreducibility of X^2+Y^2-1 can be shown by means of Eisenstein's Criterion. (See exercise 43.)

6. (a) The map $\varphi : K^\iota \to K^\iota_{sq}$, $\varphi(x) = x^2$ is a group epimorphism with $\ker\varphi = \{\pm 1\}$. Hence $|K^\iota_{sq}| = |K^\iota/\ker\varphi| = \dfrac{|K^\iota|}{|\ker\varphi|} = \dfrac{q-1}{2}$, and

$$[K^\iota : K^\iota_{sq}] = \frac{|K^\iota|}{|K^\iota_{sq}|} = \frac{q-1}{\frac{q-1}{2}} = 2.$$

(b) $a \in K^\iota \setminus K^\iota_{sq} \Rightarrow X^2 - a \in \operatorname{irr}(K[X]) \Rightarrow E_a$ is a field, and

$$[E_a : K] = \deg(X^2-a) = 2, \text{ so } |E_a| = |K|^2 = q^2.$$

(c) $|E_a| = q^2 = |E_b|$. Finite fields of the same order are isomorphic.

7. (a) Since $\mathbb{F}_p \subset \mathbb{F}_q$ is finite Galois, Artin's Theorem asserts that $|G| = [\mathbb{F}_q : \mathbb{F}_p] = n$.

(b)
$$\left.\begin{aligned} \sigma(x+y) &= (x+y)^p = x^p + y^p = \sigma(x)+\sigma(y) \\ \sigma(xy) &= (xy)^p = x^p y^p = \sigma(x)\sigma(y) \\ \sigma(1) &= 1^p = 1 \end{aligned}\right\}$$
shows that $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ is an endomorphism of the field. Since every field morphism is injective and $\mathbb{F}_q$ is finite, it follows that $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ is an automorphism. Moreover, $\sigma(x) = x^p = x$ holds for all $x \in \mathbb{F}_p$. So $\sigma \in G$.

(c) For all $x \in \mathbb{F}_q$ we have $\sigma^n(x) = x^{p^n} = x^q = x$. So $o(\sigma) \leq n$.
If $o(\sigma) = m < n$, then $x^{p^m} = \sigma^m(x) = x \quad \forall x \in \mathbb{F}_q$ shows that the polynomial
$X^{p^m} - X \in \mathbb{F}_q[X]$ has $q = p^n$ distinct zeros in $\mathbb{F}_q$, which implies $p^n < p^m < p^n$. ↯
So $o(\sigma) = n$.

(d) $\langle\sigma\rangle < G$ and $|\langle\sigma\rangle| = o(\sigma) = n$ and $|G| = n$ shows that $G = \langle\sigma\rangle$ is a cyclic group of order n.

8. $\mathbb{Q} \subset E$ is Galois of degree 6, with cyclic Galois group G of order 6, generated by (e.g.) $\sigma : \zeta \mapsto \zeta^3$. The proper intermediate fields of $\mathbb{Q} \subset E$ are $I = E^{\sigma^2}$, $J = E^{\sigma^3}$.

General elements in E are of the form $x = \sum_{i=0}^{5} a_i \zeta^i$, all $a_i \in \mathbb{Q}$.

ζ^i	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5	ζ^6
$\sigma(\zeta^i)$	1	ζ^3	ζ^6	ζ^2	ζ^5	ζ	ζ^4
$\sigma^2(\zeta^i)$	1	ζ^2	ζ^4	ζ^6	ζ	ζ^3	ζ^5
$\sigma^3(\zeta^i)$	1	ζ^6	ζ^5	ζ^4	ζ^3	ζ^2	ζ

and $\zeta^6 = -1-\zeta-\dots-\zeta^5$ imply that

$$\sigma^2(x) = \sum_{i=0}^{5} a_i \sigma^2(\zeta^i) = a_0 + a_1\zeta^2 + a_2\zeta^4 + a_3(-1-\zeta-\dots-\zeta^5) + a_4\zeta + a_5\zeta^3$$

$$= (a_0 - a_3) + (a_4 - a_3)\zeta + (a_1 - a_3)\zeta^2 + (a_5 - a_3)\zeta^3 + (a_2 - a_3)\zeta^4 - a_3\zeta^5$$

So $x \in E^{\sigma^2} \Leftrightarrow \sigma^2(x) = x \quad \Leftrightarrow \quad \begin{cases} -a_3 = 0 \\ -a_1 - a_3 + a_4 = 0 \\ a_1 - a_2 - a_3 = 0 \\ -2a_3 + a_5 = 0 \\ a_2 - a_3 - a_4 = 0 \\ -a_3 - a_5 = 0 \end{cases}$

$\Leftrightarrow \begin{cases} a_1 = a_2 = a_4 \\ a_3 = a_5 = 0 \end{cases} \Leftrightarrow x = a_0 + a_1(\zeta + \zeta^2 + \zeta^4)$, all $a_0, a_1 \in \mathbb{Q}$. So $I = E^{\sigma^2} = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$.

Likewise, $\sigma^3(x) = a_0 + a_1(-1-\zeta-\dots-\zeta^5) + a_2\zeta^5 + a_3\zeta^4 + a_4\zeta^3 + a_5\zeta^2$

$$= (a_0-a_1) - a_1\zeta + (a_5-a_1)\zeta^2 + (a_4-a_1)\zeta^3 + (a_3-a_1)\zeta^4 + (a_2-a_1)\zeta^5$$

shows that

$$x \in E^{\sigma^3} \iff \sigma^3(x) = x \iff \begin{cases} -a_1 = 0 \\ -2a_1 = 0 \\ -a_1 - a_2 + a_5 = 0 \\ -a_1 - a_3 + a_4 = 0 \\ -a_1 + a_3 - a_4 = 0 \\ -a_1 + a_2 - a_5 = 0 \end{cases}$$

$$\iff \begin{cases} a_1 = 0 \\ a_2 = a_5 \\ a_3 = a_4 \end{cases} \iff x = a_0 + a_2(\zeta^2+\zeta^5) + a_3(\zeta^3+\zeta^4), \quad \text{all } a_0, a_2, a_3 \in \mathbb{Q}.$$

So $J = E^{\sigma^3} = \mathbb{Q}(\zeta^2+\zeta^5) = \mathbb{Q}(\zeta^3+\zeta^4)$.