Solutions 2014 – 12 – 15

1. (a) A subset $H \subset G$ is a <u>subgroup</u> in case the following holds:

$e \in H$,

$x \in H \Rightarrow x^{-1} \in H$,

$x, y \in H \Rightarrow xy \in H$.

(b) $\{1, -1, i, -i\} = \{ i^n \mid n \in \mathbb{Z} \} = \langle i \rangle < \mathbb{C}^*$.

(c) $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ classify all groups of order 4.

(d) $C_4 \xrightarrow{\sim} \mathbb{Z}_4$, because $o(i) = 4$, while $\mathbb{Z}_2 \times \mathbb{Z}_2$ contains no element of order 4.

2. (a) Since $243 = 3^5$, the abelian groups of order 243 are classified by

$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9$

$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{27}$

$\mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_9$

$\mathbb{Z}_3 \times \mathbb{Z}_{81}$

$\mathbb{Z}_9 \times \mathbb{Z}_{27}$

$\mathbb{Z}_{243}$

(b) Since $289 = 17^2$, the groups of order 289 are classified by $\mathbb{Z}_{17} \times \mathbb{Z}_{17}$, $\mathbb{Z}_{289}$.

(c) The following general results are used in (a) and (b):

Theorem 1. The finite abelian groups are classified by the list $\prod_{i=1}^{\ell} \mathbb{Z}_{p_i^{m_i}}$, where $\ell \in \mathbb{N}$, all p_i are prime, all $m_i \in \mathbb{N}\setminus\{0\}$, and $(p_1, m_1) \leq \dots \leq (p_\ell, m_\ell)$ in lexicographical ordering.

Theorem 2. Every group of prime squared order is abelian.

3. (a) $\sigma = (1\ 12\ 3\ 7\ 2)(4\ 11\ 5\ 10)(6\ 8\ 9)$ shows that $o(\sigma) = \operatorname{lcm}(5,4,3) = 60$.

(b) $A_{12} = \{\sigma \in S_{12} \mid \sigma \text{ is even}\}$.

(c) Every cycle of length n is a product of $n-1$ transpositions. Hence σ is a product of $4+3+2 = 9$ transpositions. Accordingly σ is odd, i.e. $\sigma \notin A_{12}$.

4. (a) A domain is a commutative ring R such that $1 \neq 0$ and R has no zero divisors (i.e. $xy = 0 \Rightarrow x = 0$ or $y = 0$).

(b) $\Phi_p(X) = 1 + X + \dots + X^{p-1}$ is irreducible in $\mathbb{Z}[X]$ for all prime numbers p

$\Rightarrow$ $\Phi_3(X) = 1 + X + X^2$ is irreducible in $\mathbb{Z}[X]$

$\Rightarrow$ $\Phi_3(X)$ is prime in $\mathbb{Z}[X]$ (since $\mathbb{Z}[X]$ is a ufd)

$\Rightarrow$ R_1 is a domain.

$\alpha^2 \geq 0 \ \forall \alpha \in \mathbb{Q} \Rightarrow X^2 + 1$ has no rational root $\Rightarrow X^2+1 \in \operatorname{irr}(\mathbb{Q}[X])$

$\Rightarrow$ X^2+1 is prime in $\mathbb{Q}[X]$ (since $\mathbb{Q}[X]$ is a ufd)

$\Rightarrow$ R_2 is a domain.

We observe that $\overline{X} \neq \overline{0}$ in R_3. Indeed, if $\overline{X} = \overline{0}$, then

$$X + (XY) = 0 + (XY) \Rightarrow X \in (XY)$$
$$\Rightarrow X = XYf(X,Y) \quad \text{for some } f(X,Y) \in \mathbb{C}[X,Y].$$

According to $\mathbb{C}[X,Y] = (\mathbb{C}[X])[Y]$ we view $X = XYf(X,Y)$ as a polynomial in Y with coefficients in $\mathbb{C}[X]$, and find that its degree (in Y) is

$$\begin{aligned} 0 = \deg_Y(X) &= \deg_Y(XYf(X,Y)) \\ &= \deg_Y(X) + \deg_Y(Y) + \deg_Y(f(X,Y)) \geq 1 \quad \lightning \end{aligned}$$

Likewise, $\overline{Y} \neq \overline{0}$. Now $\overline{X}\,\overline{Y} = \overline{XY} = \overline{0}$ shows that R_3 has zero divisors, i.e. R_3 <u>is not a domain</u>.

5. (a) An element p in a domain R is called <u>irreducible</u> if $p \neq 0$ and $p \notin R^\times$ and $p = ab \Rightarrow a \in R^\times \vee b \in R^\times$.

(b) An element p in a domain R is called <u>prime</u> if $p \neq 0$ and $p \notin R^\times$ and $p \mid ab \Rightarrow p \mid a \vee p \mid b$.

(c) Let $p = XY - Z^2 \in \mathbb{C}[X,Y,Z] = (\mathbb{C}[X,Y])[Z]$. Then p is primitive, $\mathbb{C}[X,Y]$ is ufd, and $X \in \operatorname{irr}(\mathbb{C}[X,Y])$ such that $X \nmid -1$, $X \mid 0$, $X \mid XY$, and $X^2 \nmid XY$. Now Eisenstein's Criterion implies that p is irreducible in $\mathbb{C}[X,Y,Z]$.

(d) Since $\mathbb{C}[X,Y,Z]$ is ufd, every irreducible polynomial in $\mathbb{C}[X,Y,Z]$ is prime. In particular, $XY - Z^2$ is prime in $\mathbb{C}[X,Y,Z]$.

6. $r = \sqrt[19]{17\,000} \notin \mathbb{Q}$.

Proof. $r^{19} = 17\,000$ shows that r is a root of the polynomial $f(X) = X^{19} - a$, where $a = 17\,000 = 2^3 \cdot 5^3 \cdot 17$. Eisenstein's Criterion (with $p = 17$) shows that $f(X)$ is irreducible in $\mathbb{Z}[X]$. Gauß's Lemma implies that $f(X)$ is irreducible in $\mathbb{Q}[X]$. Accordingly, $f(X)$ has no rational root. So $r \notin \mathbb{Q}$. $\square$

7. $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = \deg(\mathrm{irrpol}_{\mathbb{Q}}(\sqrt{5})) = 2$, since $\mathrm{irrpol}_{\mathbb{Q}}(\sqrt{5}) = X^2 - 5$.

$[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = \deg(\mathrm{irrpol}_{\mathbb{Q}}(\sqrt[3]{5})) = 3$, since $\mathrm{irrpol}_{\mathbb{Q}}(\sqrt[3]{5}) = X^3 - 5$.

We claim that $[\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}(\sqrt[3]{5})] = 2$. Consequently

$$[\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}(\sqrt[3]{5})]\,[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Proof of claim. $\left[\mathbb{Q}(\sqrt{5},\sqrt[3]{5}):\mathbb{Q}(\sqrt[3]{5})\right] = \left[(\mathbb{Q}(\sqrt[3]{5}))(\sqrt{5}):\mathbb{Q}(\sqrt[3]{5})\right] = \deg\left(\operatorname{irrpol}_{\mathbb{Q}(\sqrt[3]{5})}(\sqrt{5})\right)$

$= 2$, because

$\operatorname{irrpol}_{\mathbb{Q}(\sqrt[3]{5})}(\sqrt{5}) = X^2-5$. Indeed, $X^2-5 \in \mathbb{Q}(\sqrt[3]{5})[X]$ is monic and has $\sqrt{5}$ as a root.

Moreover, X^2-5 is irreducible over $\mathbb{Q}(\sqrt[3]{5})$. Indeed, if not, then

$$X^2-5 \text{ splits over } \mathbb{Q}(\sqrt[3]{5}) \Rightarrow \sqrt{5} \in \mathbb{Q}(\sqrt[3]{5})$$

$$\Rightarrow \underbrace{\underbrace{\mathbb{Q} \subset \mathbb{Q}(\sqrt{5})}_{2} \subset \mathbb{Q}(\sqrt[3]{5})}_{3} \Rightarrow 2 \mid 3 \ \lightning \qquad \square$$

Since $(1, \sqrt[3]{5}, \sqrt[3]{25})$ is a $\mathbb{Q}$-basis in $\mathbb{Q}(\sqrt[3]{5})$,

and $(1, \sqrt{5})$ is a $\mathbb{Q}(\sqrt[3]{5})$-basis in $\mathbb{Q}(\sqrt[3]{5}, \sqrt{5})$,

a $\mathbb{Q}$-basis in $\mathbb{Q}(\sqrt{5}, \sqrt[3]{5})$ is given by $(1, \sqrt[3]{5}, \sqrt[3]{25}, \sqrt{5}, \sqrt{5}\sqrt[3]{5}, \sqrt{5}\sqrt[3]{25})$,
which can be rewritten as

$$(1, 5^{1/3}, 5^{1/2}, 5^{2/3}, 5^{5/6}, 5^{7/6}).$$

Dividing $5^{7/6} = 5\sqrt[6]{5}$ by 5 gives the more streamlined $\mathbb{Q}$-basis

$$(1, 5^{1/6}, 5^{2/6}, 5^{3/6}, 5^{4/6}, 5^{5/6}).$$

8. (a) A <u>Galois extension</u> is an algebraic field extension, which is normal and separable.

(b) For each $f(X) \in \mathbb{Q}[X] \setminus \mathbb{Q}$, the splitting field $\operatorname{sf}_{\mathbb{Q}}(f(X))$ is a finite Galois extension of $\mathbb{Q}$. Now $E = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta, \zeta^2, \zeta^3, \zeta^4) = \operatorname{sf}_{\mathbb{Q}}(\Phi_5(X))$, where $\Phi_5(X) = 1+X+X^2+X^3+X^4$. So $\mathbb{Q} \subset E$ is finite Galois.

(c) Set $G = \mathrm{Gal}(E/\mathbb{Q})$. Then $|G| \overset{(b)}{=} [E:\mathbb{Q}] = \deg(\mathrm{irrpol}_{\mathbb{Q}}(\zeta)) = 4$, since $\mathrm{irrpol}_{\mathbb{Q}}(\zeta) = \Phi_5(X)$. The unique $\sigma \in G$ which is determined by $\sigma(\zeta) = \zeta^2$ has order 4. Hence $G = \langle \sigma \rangle \xrightarrow{\sim} C_4$. The Fundamental Theorem of Galois Theory asserts that the intermediate fields $\mathbb{Q} \subset I \subset E$ correspond bijectively to the subgroups of G:

$$\begin{array}{ccc} \langle \mathbb{1}_E \rangle & \qquad\qquad & E^{\mathbb{1}} = E \\ \wedge & & \cup \\ \langle \sigma^2 \rangle & & E^{\sigma^2} = I \\ \wedge & & \cup \\ \langle \sigma \rangle = G & & E^{\sigma} = \mathbb{Q} \end{array}$$

Since G has precisely one proper nontrivial subgroup, namely $\langle \sigma^2 \rangle$, the extension $\mathbb{Q} \subset E$ has precisely one proper nontrivial intermediate field, namely $I = E^{\sigma^2}$.

(d) <u>Every finite separable field extension is simple</u>. The field extension $\mathbb{Q} \subset I$ has degree 2 and is separable (since $\mathrm{char}(\mathbb{Q}) = 0$).

(e) $I = E^{\sigma^2} = \{\alpha \in E \mid \sigma^2(\alpha) = \alpha\}$. E has $\mathbb{Q}$-basis $(1, \zeta, \zeta^2, \zeta^3)$. Every $\alpha \in E$ can be written $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$, with unique $a_i \in \mathbb{Q}$. Now

$$\begin{aligned} \sigma^2(\alpha) &= a_0 + a_1\zeta^4 + a_2\zeta^3 + a_3\zeta^2 \\ &= a_0 + a_1(-1-\zeta-\zeta^2-\zeta^3) + a_3\zeta^2 + a_2\zeta^3 \\ &= (a_0 - a_1) - a_1\zeta + (a_3 - a_1)\zeta^2 + (a_2 - a_1)\zeta^3 \end{aligned}$$

shows that $\alpha \in I \Leftrightarrow \sigma^2(\alpha) = \alpha \Leftrightarrow a_1 = 0 \wedge a_2 = a_3 \Leftrightarrow \alpha = a_0 + a_2(\zeta^2 + \zeta^3)$.

Thus $I = \mathbb{Q}(\zeta^2 + \zeta^3)$, i.e. $s = \zeta^2 + \zeta^3 \in E$ will do.