Homework 8

Aleck Zhao

April 9, 2017

1. (a) Let $z = a + bi \in \mathbb{C}$ with $a, b \in \mathbb{R}$. Explain why the quantities

$$\frac{a + \sqrt{a^2 + b^2}}{2} \quad \text{and} \quad \frac{-a + \sqrt{a^2 + b^2}}{2}$$

are non-negative, and hence have real square roots. Then use these square roots to produce a square root of z in $\mathbb{C}$, i.e. a $w \in \mathbb{C}$ such that $w^2 = z$. (Be careful about signs)

Solution. Since $a, b \in \mathbb{R}$, we have

$$\frac{a + \sqrt{a^2 + b^2}}{2} \geq \frac{a + \sqrt{a^2}}{2} = \frac{a + |a|}{2} \geq 0$$
$$\frac{a - \sqrt{a^2 + b^2}}{2} \geq \frac{-a + \sqrt{a^2}}{2} = \frac{-a + |a|}{2} \geq 0$$

Since these quantities are non-negative, their square roots are real. Now, the square root of z is

$$\begin{aligned}
w &= \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + \frac{b}{|b|}\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}i \\
\implies w^2 &= \frac{b^2}{|b|^2}\left(\frac{a + \sqrt{a^2 + b^2}}{2} - \frac{-a + \sqrt{a^2 + b^2}}{2}\right) + 2\frac{b}{|b|}\sqrt{\frac{(a + \sqrt{a^2 + b^2})(-a + \sqrt{a^2 + b^2})}{4}}i \\
&= \frac{2a}{2} + 2\frac{b}{|b|}\sqrt{\frac{-a^2 + (a^2 + b^2)}{4}}i \\
&= a + \frac{b}{|b|} \cdot |b|\, i = a + bi
\end{aligned}$$

□

(b) Let $f(x) = x^2 + \alpha x + \beta \in \mathbb{C}[x]$, with $\alpha, \beta \in \mathbb{C}$. Use the quadratic formula to show directly that f splits into linear factors over $\mathbb{C}$, and hence the roots of f lie in $\mathbb{C}$.

Proof. By the quadratic formula, the roots of f are

$$u = \frac{-\alpha + \sqrt{\alpha^2 - 4\beta}}{2}$$
$$v = \frac{-a - \sqrt{\alpha^2 - 4\beta}}{2}$$

Since $\alpha, \beta \in \mathbb{C}$, it follows that $(\alpha^2 - 4\beta) \in \mathbb{C}$, and from (a), the square root exists in $\mathbb{C}$, so $u, v \in \mathbb{C}$ and thus the roots of f lie in $\mathbb{C}$, so f splits into linear factors over $\mathbb{C}$. □

Section 4.5: Symmetric Polynomials

6. Show that $f(x_1, \cdots, x_n)$ is homogeneous of degree m in $R[x_1, \cdots, x_n]$ if and only if $f(tx_1, \cdots, tx_n) = t^m \cdot f(x_1, \cdots, x_n)$ in $R[t, x_1, \cdots, x_n], t$ another indeterminate.

Proof. ($\Longrightarrow$) : If f is homogeneous of degree m, then each term is of the form $ax_1^{e_1} \cdots x_n^{e_n}$ where $a \in R$ and $0 \le e_i \le m$ for each i and $\sum e_i = m$. Then in $f(tx_1, \cdots, tx_n)$, this term becomes

$$\begin{aligned} a(tx_1)^{e_1} \cdots (tx_n)^{e_n} &= at^{e_1} x_1^{t_1} \cdots t^{e_n} x_n^{e_n} \\ &= at^{\sum e_i} x_1^{e_1} \cdots x_n^{e_n} \\ &= t^m \cdot (ax_1^{e_1} \cdots x_n^{e_n}) \end{aligned}$$

so $f(tx_1, \cdots, tx_n) = t^m \cdot f(x_1, \cdots, x_n)$ as desired.

($\Longleftarrow$) : If $ax_1^{e_1} \cdots x_n^{e_n}$ is a term of $f(x_1, \cdots, x_n)$ where $a \in R$ and $0 \le e_i$, then since $f(tx_1, \cdots, tx_n) = t^m \cdot f(x_1, \cdots, x_n)$, the corresponding term of $f(tx_1, \cdots, tx_n)$ is $t^m \cdot (ax_1^{e_1} \cdots x_n^{e_n})$. We also have

$$a(tx_1)^{e_1} \cdots (tx_n)^{e_n} = at^{e_1} x^{e_1} \cdots t^{e_n} x^{e_n} = t^{\sum e_i} \cdot (ax_1^{e_1} \cdots x_n^{e_n}) = t^m \cdot (ax_1^{e_1} \cdots x_n^{e_n}) \implies \sum e_i = m$$

Thus, the degree of every term of f is m, so f is homogeneous of degree m. $\square$

9. Show that the number of terms in $s_k(x_1, \cdots, x_n)$ is $\binom{n}{k}$.

Proof. Every term in s_k is of the form $x_{i_1} \cdots x_{i_k}$ where each of the subscripts is distinct. There are n possible subscripts, and we are choosing k to be in the term, so the number of terms is $\binom{n}{k}$. $\square$

10. Show that the number of monomials of degree m in $R[x_1, \cdots, x_n]$ is $\binom{m+n-1}{m}$.

Proof. Every monomial of degree m is of the form

$$x_1^{e_1} \cdots x_n^{e_n}$$

where $0 \le e_i \le m$ for each i. Consider a combinatorial argument: suppose we have m 1's in a row, corresponding to the m degree of the monomial. We wish to place $n-1$ "dividers" among these 1's that separate these 1's into n parts, where there may be zero 1's between two dividers. The number of 1's in the ith part corresponds to e_i. There are $\binom{m+n-1}{m}$ ways to order these 1's and dividers, which is the number of monomials of degree m. $\square$

Section 8.3: Group Actions

7. If H and K are subgroups of G, show that $\operatorname{core}(H \cap K) = \operatorname{core} H \cap \operatorname{core} K$.

Proof. ($\subseteq$) : Let $x \in \operatorname{core}(H \cap K)$. Then $x \in g(H \cap K)g^{-1}$ for every $g \in G$, which is to say that $x = gyg^{-1}$ for some $y \in (H \cap K)$ for each $g \in G$. Now, since $y \in H$ and $y \in K$, it follows that $x = gyg^{-1} \implies x \in gHg^{-1}$ and $x \in gKg^{-1}$ for each $g \in G$, and thus $x \in \operatorname{core} H \cap \operatorname{core} K$.

($\supseteq$) : Let $x \in \operatorname{core} H \cap \operatorname{core} K$. Then $x \in gHg^{-1}$ for each $g \in G$, so $x = gyg^{-1}$ for some $y \in H$. However, since $x \in gKg^{-1}$ as well, we must have $x = gzg^{-1}$ for some $z \in K$. Obviously then $y = z$, so $y \in H \cap K$, and thus $x \in g(H \cap K)g^{-1}$ for each $g \in G$, so $x \in \operatorname{core}(H \cap K)$. $\square$

12. Given $m > 1$, show that a finitely generated group G has at most a finite number of subgroups of index m.

Proof. Let $C = \{ \operatorname{core} H \mid |G : H| = m \}$. Now, since H has finite index m in G, there is a homomorphism $\theta : G \to S_m$ with $\ker \theta = \operatorname{core} H$. Since G is finitely generated, say by $\{g_1, \cdots, g_n\}$, this homomorphism is determined exactly by where these generators are mapped to. Since S_m is a finite set, there are finitely many different homomorphisms, and thus finitely many different possibilities for $\ker \theta = \operatorname{core} H$. Thus, C is a finite set.

Now, for any $K \in C$, suppose $K = \operatorname{core} H$ for some subgroup H of G with index m. Since $\operatorname{core} H \trianglelefteq G$, by the correspondence theorem, we have

$$\Theta : \{ H \mid K \subseteq H \subseteq G \} \to \{ M \mid M \subseteq G/K \}$$

is a bijection, where H is a subgroup of G and M is a subgroup of G/K. Since G is finitely generated, it follows that G/K is also finitely generated, say by $g_1K, \cdots, g_nK$. Then if M is a subgroup of G/K, it must contain some subset of these generators. Since there are only finitely many of them, there are a finite number of subgroups of G/K, and since Θ is a bijection, there are finitely many subgroups H of G. Thus, the total number of subgroups of index m is finite. □

23. Let X be a G-set and let x and y denote elements of X.

(a) Show that $S(x)$ is a subgroup of G.

Proof. By definition, $1_G \cdot x = x$ so $1_G \in S(x)$. If $a, b \in S(x)$, then

$$\begin{aligned} (ab) \cdot x = a \cdot (b \cdot x) = a \cdot x = x &\implies ab \in S(x) \\ (a^{-1}) \cdot x = (a^{-1}) \cdot (a \cdot x) = (a^{-1}a) \cdot x = 1 \cdot x = x &\implies a^{-1} \in S(x) \end{aligned}$$

Thus $S(x)$ is a subgroup of G. □

(b) If $x \in X$ and $b \in G$, show that $S(b \cdot x) = bS(x)b^{-1}$.

Proof. $(\subseteq)$: Let $g \in S(b \cdot x)$, so $g \cdot (b \cdot x) = (gb) \cdot x = b \cdot x$. Then by Lemma 2, we have $(b^{-1}gb) \cdot x = x$, so $b^{-1}gb \in S(x)$, and thus $bS(x)b^{-1} \ni b(b^{-1}gb)b^{-1} = g$.
$(\supseteq)$: Let $g \in bS(x)b^{-1}$, so $g = bhb^{-1}$ for some $h \in S(x)$. Then

$$\begin{aligned} g \cdot (b \cdot x) &= (bhb^{-1}) \cdot (b \cdot x) = (bhb^{-1}b) \cdot x = (bh) \cdot x \\ &= b \cdot (h \cdot x) = b \cdot x \end{aligned}$$

so $g \in S(b \cdot x)$. □

(c) If $S(x)$ and $S(y)$ are conjugate subgroups, show that $|G \cdot x| = |G \cdot y|$.

Proof. Suppose $S(x) = aS(y)a^{-1} \implies a^{-1}S(x)a = S(y)$ for some $a \in G$. Then define the map

$$\begin{aligned} \varphi : G \cdot x &\to G \cdot y \\ g \cdot x &\mapsto (ga) \cdot y \end{aligned}$$

Now, this map is well-defined and injective because

$$\begin{aligned} g \cdot x = h \cdot x &\iff (h^{-1}g) \cdot x = x \iff h^{-1}g \in S(x) \\ &\iff a^{-1}h^{-1}ga \in a^{-1}S(x)a = S(y) \\ &\iff (a^{-1}h^{-1}ga) \cdot y = y \\ &\iff (ga) \cdot y = (ha) \cdot y \end{aligned}$$

This map is also surjective because for any $b \cdot y \in G \cdot y$, we can recover $(ba^{-1}) \cdot x$ that maps to it. Thus, φ is a bijection, so $|G \cdot x| = |G \cdot y|$. □

32. Let H and K be subgroups of a group G and let $H \times K$ act on G by $(h,k) \cdot x = hxk^{-1}$ for all $x \in G$ and $(h,k) \in H \times K$. Show

(a) This is an action and the orbit of $x \in G$ is HxK.

Proof. We have

$$\begin{aligned}(1_H, 1_K) \cdot x &= 1_G x 1_k = x \\ (h,k) \cdot [(a,b) \cdot x] &= (h,k) \cdot (axb^{-1}) = haxb^{-1}k^{-1} = (ha)x(kb)^{-1} \\ &= (ha, kb) \cdot x = [(h,k)(a,b)] \cdot x\end{aligned}$$

so this an action.
$(\subseteq)$: If $y \in (H \times K) \cdot x$, then $y = hxk^{-1} \in HxK$ trivially.
$(\supseteq)$: If $y \in HxK$, then $y = hxk$ for some $h \in H$ and $k \in K \implies k^{-1} \in K$. Then

$$y = hx(k^{-1})^{-1} = (h, k^{-1}) \cdot x \implies y \in (H \times K) \cdot x.$$

□

(b) If $x \in G$, then $|S(x)| = \left|H \cap xKx^{-1}\right| = \left|x^{-1}Hx \cap K\right|$.

Proof. If $(h,k) \in S(x)$, then $hxk^{-1} = x \implies k = x^{-1}hx$. Now define the map

$$\begin{aligned}\varphi : S(x) &\to H \cap xKx^{-1} \\ (h, x^{-1}hx) &\mapsto h\end{aligned}$$

Now, this map is well-defined and injective because

$$(h, x^{-1}hx) = (g, x^{-1}gx) \iff h = g$$

This map is also surjective because if $h \in (H \cap xKx^{-1})$, then $h = xkx^{-1} \implies k = x^{-1}hx$ for some $k \in k$, so we can recover $(h, x^{-1}hx)$ that maps to h. Thus, φ is a bijection, so $|S(x)| = \left|H \cap xKx^{-1}\right|$.
Similarly, if $(h,k) \in S(x)$, then $hxk^{-1} = x \implies h = xkx^{-1}$, Now define the map

$$\begin{aligned}\sigma : S(x) &\to x^{-1}Hx \cap K \\ (xkx^{-1}, k) &\mapsto k\end{aligned}$$

Now, this map is well defined and injective because

$$(xkx^{-1}, k) = (xgx^{-1}, g) \iff k = g$$

This map is also surjective because if $k \in (x^{-1}Hx \cap K)$, then $k = x^{-1}hx \implies h = xkx^{-1}$ for some $h \in H$, so we can recover (xkx^{-1}, k) that maps to k. Thus, σ is a bijection, so $|S(x)| = \left|x^{-1}Hx \cap K\right|$. □

(c) Frobenius' theorem: If $Hx_1K, Hx_2K, \cdots, Hx_nK$ are the distinct double cosets, then

$$|G| = \sum_{i=1}^{n} \frac{|H|\,|K|}{\left|x_i^{-1}Hx_i \cap K\right|}$$

Proof. From the orbit decomposition theorem, and the result of (b), we have

$$\begin{aligned}|G| &= \sum_{i=1}^{n} |(H \times K) \cdot x_i| = \sum_{i=1}^{n} |(H \times K) : S(x_i)| \\ &= \sum_{i=1}^{n} \frac{|H \times K|}{|S(x_i)|} = \sum_{i=1}^{n} \frac{|H|\,|K|}{\left|x_i^{-1}Hx_i \cap K\right|}\end{aligned}$$

□