1. 叙述群的定义并证明：若$\{H_i\}_{i\in I}$是G的一族子群，则$H=\bigcap_{i\in I}H_i$是H的子群

定义：结合律、单位元、逆元

G和G上的乘法"·"满足：

(1) $\forall a,b\in G$, $a\cdot b\in G$　(2) $(a\cdot b)\cdot c=a\cdot(b\cdot c)$

(3) $\exists e\in G$, $a\cdot e=e\cdot a=a$　(4) $\forall a\in G$, $\exists b\in G$使$ab=ba=e$

证：$\forall x,y\in\bigcap_{i\in I}H_i$，则由$H_i$子群

$\Rightarrow x\cdot y\in H_i$, $e\in H_i$，且$\exists x^{-1}\in H_i$

$\Rightarrow x\cdot y\in\bigcap_{i\in I}H_i$, $e\in\bigcap_{i\in I}H_i$, $x^{-1}\in\bigcap_{i\in I}H_i$，(1)(3)(4)成立

(2)由H中结合律成立

2. 令$K=\left\{\begin{pmatrix}a&b\\-b&a\end{pmatrix}\middle|\,a,b\in\mathbb{R}\right\}\subset M_2(\mathbb{R})$，证：K对矩阵加乘是域

封闭性：$\begin{pmatrix}a&b\\-b&a\end{pmatrix}+\begin{pmatrix}c&d\\-d&c\end{pmatrix}=\begin{pmatrix}a+c&b+d\\-b-d&a+c\end{pmatrix}\in K$

$\begin{pmatrix}a&b\\-b&a\end{pmatrix}\begin{pmatrix}c&d\\-d&c\end{pmatrix}=\begin{pmatrix}ac-bd&ad+bc\\-bc-ad&-bd+ac\end{pmatrix}\in K$

由于K是矩阵环子环且$\begin{pmatrix}0&0\\0&0\end{pmatrix}\in K$知，加法结合律、乘法结合律，分配律成立，两个交换律

$\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix}\in K\Rightarrow$单位元

$\begin{pmatrix}a&b\\-b&a\end{pmatrix}+\begin{pmatrix}(-a)&(-b)\\-(-b)&(-a)\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$, $\begin{pmatrix}a&b\\-b&a\end{pmatrix}\begin{pmatrix}\frac{a}{a^2+b^2}&\frac{-b}{a^2+b^2}\\\frac{b}{a^2+b^2}&\frac{a}{a^2+b^2}\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$

$\Rightarrow$逆元

3. 叙述正规子群定义并证明$H,K\leq G$，若$K\lhd G$，则$H\cdot K=\{hk\mid h\in H,k\in K\}$也是G的子群且$H/(H\cap K)\cong(H\cdot K)/K$

定义：$H\leq G$且$\forall a\in G$有$aH=Ha$

封闭：$h_1k_1\cdot h_2k_2$　由$K\lhd G\Rightarrow K\cdot h_2=h_2K\Rightarrow k_1h_2=h_2k_3$

$\Rightarrow h_1k_1\cdot h_2k_2=(h_1h_2)\cdot(k_3k_2)\in H\cdot K$

结合律由G是群成立，单位元由$e=e\cdot e\in H\cdot K$，逆元：$(hk)^{-1}=k^{-1}h^{-1}\in K\cdot h^{-1}$

$= h^{-1}K = h^{-1}\cdot k_1 \Rightarrow hk\cdot h^{-1}k_1 = e \Rightarrow$ 是群

考虑同态 $H \xrightarrow{\varphi} (H\cdot K)/K$，$\varphi(h) = h\cdot K$，

注意到 $H\cdot K \xrightarrow{\psi} H\cdot K/K$，$\psi(hk) = hkK = hK$（左陪集）

所以 $(H\cdot K)/K = \{h\cdot K \mid h\in H\}$

所以 φ 是满射，$\ker\varphi = H\cap K \Rightarrow H/(H\cap K) \cong (H\cdot K)/K$

4. 证明：$\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$，$\mathbb{Q}[\sqrt{5}] = \{a+b\sqrt{5} \mid a,b\in\mathbb{Q}\}$ 都是 $\mathbb{R}$ 子域，它们同构吗？

证：$(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ } 封闭

单位元 1，零元 0，逆元 $(a+b\sqrt{2})+(-a-b\sqrt{2})=0$，$(a+b\sqrt{2})\cdot\frac{a-b\sqrt{2}}{a^2-2b^2}=1$

且 $a^2-2b^2=0$ 在 $\mathbb{Q}$ 中无解

类似的 $\mathbb{Q}[\sqrt{5}]$

反证 $\mathbb{Q}[\sqrt{2}]$ 和 $\mathbb{Q}[\sqrt{5}]$ 同构，设 $\varphi: \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{5}]$

则 $\varphi(0)=0$，$\varphi(1)=1$，$\Rightarrow \varphi(q)=q, \forall q\in\mathbb{Q}$

设 $\varphi(\sqrt{2}) = a+b\sqrt{5} \Rightarrow 2 = (a+b\sqrt{5})^2 = a^2+5b^2+2ab\sqrt{5}$，若 $b=0$ ×

若 $a=0$，× $\Rightarrow$ 矛盾

5. 设 $L\supset K$ 域扩张，证：$\mathrm{Gal}(L/K) = \{L \xrightarrow{\sigma} L \mid \sigma$ 是同构且 $\sigma(a)=a, \forall a\in K\}$ 关于映射合成是群

封闭性成立.

结合律由映射结合律保证

单位元 id，逆元：$\forall\sigma\in\mathrm{Gal}(L/K)$，由 σ 同构 $\Rightarrow$ σ 逆映射 σ^{-1} 存在.

由 $\sigma(a)=a, \forall a\in K \Rightarrow \sigma^{-1}(a)=a$，$\forall a\in K \Rightarrow \sigma^{-1}\in\mathrm{Gal}(L/K)$

6. 设 $K\subset L$ 是域扩张，$\alpha\in L$ 是 K 上代数元，令 $K[x] \xrightarrow{\varphi_\alpha} L$，$f(x)\to f(\alpha)$ 为取值映射，证：

(1) $\ker\varphi_\alpha$ 由极小多项式 $\mu_\alpha(x)$ 生成

(2) φ_α 诱导了域同构 $K[x]/(\mu_\alpha(x)) \cong K[\alpha]$

证：(1) $\forall f(x)\in\ker\varphi_\alpha \Rightarrow f(\alpha)=0 \Rightarrow \mu_\alpha(x)\mid f(x)$，即 $f(x)\in\langle\mu_\alpha(x)\rangle$

另一方面 $\forall g(x)=\mu_\alpha(x)p(x)\in\langle\mu_\alpha(x)\rangle \Rightarrow g(\alpha)=0 \Rightarrow g(x)\in\ker\varphi_\alpha$

$\Rightarrow \ker\varphi_\alpha=\langle\mu_\alpha(x)\rangle$

(2) 考虑 $\mathrm{Im}(\varphi_\alpha)=\{f(\alpha)\mid\forall f\in K[x]\}$，由 α 代数元，$\Rightarrow \mathrm{Im}(\varphi_\alpha)=K[\alpha]$

故 $\varphi_\alpha: K[x]\to K[\alpha]$ 是满同态，由同态基本定理

$K[x]/(\mu_\alpha(x))\cong K[\alpha]$

7. 设 $E=F[\alpha]$，$\alpha^N\in F$，若 F 包含 N 次本原单位根 θ，则 $Gal(E/F)$ 是循环群

证：设 $\alpha^N=a\in F$，则 $x^N-a=(x-\alpha)(x-\theta\alpha)\cdots(x-\theta^{n-1}\alpha)$

$\forall\varphi\in Gal(E/F)$，则 $\varphi(\alpha)=\theta^k\cdot\alpha$，定义 $\chi: Gal(E/F)\to\langle\theta\rangle$，

$\chi(\varphi)=\frac{\varphi(\alpha)}{\alpha}\ (=\theta^k)$，则设 $\varphi(\alpha)=\theta^k\alpha$，$\psi(\alpha)=\theta^s\alpha$，$\psi,\varphi\in Gal(E/F)$

有 $\chi(\varphi\psi)=\frac{\varphi(\psi(\alpha))}{\alpha}=\theta^{k+s}=\chi(\varphi)\chi(\psi)\Rightarrow\chi$ 是同态，且明显单同态

故 $Gal(E/F)$ 同构于 $\langle\theta\rangle$ 子群 H，由 $\langle\theta\rangle$ 循环群可知 H 为循环群

（否则考虑 H 中指数最小的 θ^k，$\exists\,\theta^s$，$k\nmid s$，则 $s-[\frac{s}{k}]k$ 是比 k 更小的，矛盾）

即 $Gal(E/F)\cong H$ 是循环群

8. 求 $[\mathbb{Q}[\sqrt2,\sqrt3]:\mathbb{Q}]$，并证明

$[\mathbb{Q}[\sqrt2,\sqrt3]:\mathbb{Q}]=[\mathbb{Q}[\sqrt2,\sqrt3]:\mathbb{Q}[\sqrt2]]\cdot[\mathbb{Q}[\sqrt2]:\mathbb{Q}]=2[\mathbb{Q}[\sqrt2,\sqrt3]:\mathbb{Q}[\sqrt2]]$

由于 $\sqrt3\notin\mathbb{Q}[\sqrt2]$，否则 $\sqrt3=a+b\sqrt2$，$3=a^2+2b^2+2ab\sqrt2\Rightarrow a=0/b=0$ 矛盾

故 $[\mathbb{Q}[\sqrt2,\sqrt3]:\mathbb{Q}[\sqrt2]]>1$，又 x^2-3 零化 $\sqrt3\Rightarrow[\mathbb{Q}[\sqrt2,\sqrt3]:\mathbb{Q}[\sqrt2]]\le2$

$\Rightarrow[\mathbb{Q}[\sqrt2,\sqrt3]:\mathbb{Q}[\sqrt2]]=2\Rightarrow[\mathbb{Q}[\sqrt2,\sqrt3]:\mathbb{Q}]=4$

9. 设 $K\subset L$ 是有限可分，正规扩张，$G=Gal(L/K)$，$K\subset E\subset L$ 是中间域，试证明：

$K\subset E$ 正规扩张 $\Leftrightarrow\eta(E)\subset E$，$\forall\eta\in G$

"$\Rightarrow$" 由 $K\subset E$ 正规，$\Rightarrow\forall\alpha\in E$，$\mu_\alpha(x)$ 根全在 E 中，而 $\forall\alpha\in E$，有 $\eta(\mu_\alpha(\alpha))=0$，

即 $\mu_\alpha(\eta(\alpha))=0$. 即 $\eta(\alpha)$ 是 $\mu_\alpha(x)$ 根 $\Rightarrow \eta(\alpha)\in E$, $\Rightarrow \eta(E)\subset E$

"$\Leftarrow$" $\forall \alpha\in E$, 考虑 α 极小多项式 $\mu_\alpha(x)$, 另一根 β, $\exists \varphi\in Gal(L/K)$, 使 $\varphi(\alpha)=\beta$. $\Rightarrow \beta\in E$.

10. 证明6阶非Abel群同构于 S_3

证明: 考虑6阶非Abel群 G. G 的 Sylow 3-子群 $P(G)$, 由西罗定理Ⅱ, $|P(G)|\equiv 1 \pmod 3$ 且 $|P(G)|\,\big|\,2 \Rightarrow |P(G)|=1$, 设 $P(G)=\{P\}$, $P=\{e,g,g^2\}$

由 Sylow 定理Ⅰ, G 中存在2阶元 a, 则 $G=P\cup aP$ (因 $a\notin P$)

且由 $|P(G)|=1 \Rightarrow P\triangleleft G$, 故 $aga^{-1}\in P$. 若 $aga^{-1}=e \Rightarrow g=e$, 矛盾.

若 $aga^{-1}=g \Rightarrow$ Abel群, 矛盾. $\Rightarrow aga^{-1}=g^2=g^{-1}$, 即 $ag=g^{-1}a$

故 $G=\{e,g,g^2,a,ag,ag^2\}=\{a^ig^j \mid ag=g^{-1}a,\ a^2=b^3=e\}$

而 $S_3=\{id,(12),(13),(23),(123),(132)\}=\{a^ib^j \mid ag=g^{-1}a,\ a=(12), b=(123)\}$

故 $G\cong S_3$