2021 秋: 代数学一 (实验班) 期中考试

姓名: ____________ 院系: ____________ 学号: ____________ 分数:

时间：110 分钟 满分：100 分

所有的环都有乘法单位元, 且与其加法单位元不相等; 所有环同态把 1 映到 1.

All rings contains 1_R and $1_R \neq 0_R$; all ring homomorphism takes 1 to 1.

判断题 在下表中填写 T 或 F (10 分)

1	2	3	4	5	6	7	8	9	10
F	F	T	F	F	T	T	T	F	F

1. 如果 H 是群 G 的正规子群, K 是 H 的正规子群, 那么 K 是 G 的正规子群.

If H is a normal subgroup of G and K is a normal subgroup of H, then K is a normal subgroup of G.

False. A typical situation is when H is abelian, e.g. $G = (Z_p)^2 \rtimes S_2$, $H = (Z_p)^2$ the standard normal subgroup; here the semi-direction product is by letting S_2 to permute the two factors. If we take K to be the first factor Z_p of H, then K is clearly normal in H yet not normal in G.

2. 对 $i = 1, 2$, 设 H_i 是 G_i 的正规子群满足 $H_1 \cong H_2$ 和 $G_1 \cong G_2$, 则 $G_1/H_1 \cong G_2/H_2$.

For $i = 1, 2$, let H_i be a normal subgroup of G_i satisfying $H_1 \cong H_2$ and $G_1 \cong G_2$, then $G_1/H_1 \cong G_2/H_2$.

False. If one wants $G_1/H_1 \cong G_2/H_2$, one needs the isomorphism $\varphi : G_1 \cong G_2$ to induce the corresponding isomorphism $H_1 \cong H_2$. A typical example is to take $G_1 = G_2 = \mathbb{Z}$ and $H_1 = 4\mathbb{Z}$ and $H_2 = 2\mathbb{Z}$. Clearly H_1 and H_2 are abstractly isomorphic, but $G_1/H_1 \cong Z_4$ and $G_2/H_2 \cong Z_2$.

3. 任一非平凡的循环群的非平凡子群一定是循环群.

All nontrivial subgroups of a nontrivial cyclic group is cyclic.

True. Say we consider a subgroup $H < G = \langle \sigma \rangle$, then it suffices to find the minimal $n \in \mathbb{N}$ such that $\sigma^n \in H$, then σ^n would generate H.

4. 如果 N 是群 G 的正规子群, 则 G 是 N 和 G/N 的半直积.

If N is a normal subgroup of G, then G is a semi-direct product of N with G/N.

False. It is not true in general that one can embed G/N back to G. Semi-direct product requires that G/N can be realized as a subgroup of G. (This is a hard T/F question.)

5. 若 P 是群 G 的一个西罗 p-子群, 则 P 在 G 中的正规化子是 G 的正规子群.

If P is a Sylow p-subgroup of G, then the normalizer of P in G is normal in G.

False. A corollary of Sylow's theorem says that, for a Sylow p-subgroup P, $N_G(N_G(P)) = N_G(P)$. So as long as $N_G(P) \neq G$ (when P is not a normal Sylow p-subgroup), $N_G(P)$ is NOT normal in G.

6. 两个有限交换群的半直积是可解群.

A semi-direct product of two finite abelian groups is solvable.

True. Say this semi-direct product is $G = H_1 \rtimes H_2$ then $[G, G] \subseteq H_1$ which is abelian. So G is solvable.

7. 群同态 $\varphi : Z_{12} \to Z_{35}$ 必然是平凡的.

A homomorphism $\varphi : Z_{12} \to Z_{35}$ of groups must be the trivial homomorphism.

True. This is because $\#\mathrm{Im}(G)|\#Z_{35}$ and $\#\mathrm{Im}(G)|\#Z_{12}$. So $\#\mathrm{Im}(G) = 0$.

8. 整环的子环一定是整环.

A subring of an integral domain is an integral domain.

True. This is because if the big ring does not have zero-divisors, the subring cannot have zero-divisors.

9. 两个整环的直积还是整环.

The direct product of two integral domains is again an integral domain.

False. The direct product of two integral domain is never an integral domain, because $(1, 0) \cdot (0, 1) = (0, 0)$ gives zero-divisors.

10. 若 R 是一个主理想整环, 则 $R[x]$ 是一个主理想整环.

If R is a PID, then $R[x]$ is a PID.

False. $R = \mathbb{Z}$ is a PID, but $\mathbb{Z}[x]$ is not a PID, e.g. the ideal $(2, x)$.

解答题一 (10 分) 证明: 阶为 132 的群不是单群.

Prove that no simple group has order 132.

证明. $132 = 3 \times 4 \times 11$.

Suppose that there exists a simple group G of order 132. In particular G does not contain any normal Sylow p-subgroups.

We apply Sylow's theorems to each of the primes 3 and 11. For $p = 3, 11$, write n_p for the number of Sylow p-subgroups of G.

$n_{11} \equiv 1 \bmod 11$ and $n_{11}|12$. As $n_{11} \neq 1$, so $n_{11} = 12$. We count the number of elements of order precisely 11: as each Sylow 11-subgroup is isomorphic to Z_{11}, so each Sylow 11-subgroup contains exactly 10 elements of order 11. Yet two Sylow 11-subgroup can only intersect at the identity elements of the groups. So there are $12 \times 10 = 120$ elements of order 11.

$n_3 \equiv 1 \bmod 3$ and $n_3|4 \times 11$. As $n_3 \neq 1$, so $n_3 = 4$ or 22. By exactly the same argument above, we see that there are at least $2 \times 4 = 8$ elements of order 3.

This then leaves 4 elements whose order are not 3 or 11. Yet there is always a Sylow 2-group which has order 4. So this group must consist of exactly the 4 elements whose order are not 3 or 11. This Sylow 2-group must be normal, contradicting to our assumption on G being simple. $\square$

解答题二 (10 分) 设 $\varphi : R \to S$ 为两个交换环之间的同态.

(1) 证明: 若 P 是一个 S 的素理想, 则 $\varphi^{-1}(P)$ 是 R 的一个素理想.

(2) 证明: 若 M 是 S 的一个极大理想且 φ 是满射, 则 $\varphi^{-1}(M)$ 是 R 的一个极大理想.

(3) 给出一个例子说明 (2) 在不假设 φ 满射时不成立.

Let $\varphi : R \to S$ be a homomorphism of commutative rings.

(1) Prove that if P is a prime ideal of S, then $\varphi^{-1}(P)$ is a prime ideal of R.

(2) Prove that if M is a maximal ideal of S and φ is surjective, then $\varphi^{-1}(M)$ is a maximal ideal of R.

(3) Give an example to show that (2) does not hold without assuming φ to be surjective.

证明. (1) First show that $\varphi^{-1}(P)$ is an ideal. Indeed, if $a, b \in \varphi^{-1}(P)$ and $c \in R$, then $\varphi(a-b) = \varphi(a) - \varphi(b) \in P$ and $\varphi(ca) = \varphi(c)\varphi(a) \in P$. So $a - b, ca \in \varphi^{-1}(P)$.

We need to show that if $a, b \in R$ satisfies $ab \in \varphi^{-1}(P)$, then either $a \in \varphi^{-1}(P)$ or $b \in \varphi^{-1}(P)$. Indeed, the condition implies $\varphi(ab) \in P$, so $\varphi(a)\varphi(b) \in P$. As P is a prime ideal, either $\varphi(a) \in P$ or $\varphi(b) \in P$; so either $a \in \varphi^{-1}(P)$ or $b \in \varphi^{-1}(P)$.

(2) If $\varphi : R \to S$ is surjective, we may view S as the quotient ring $R/\ker\varphi$. As M is a maximal ideal, S/M is a field. By Second Isomorphism Theorem, $R/\varphi^{-1}(M) \cong S/M$, so the former is a field. Thus $\varphi^{-1}(M)$ is a maximal ideal of R.

(3) Consider the natural inclusion $\varphi : \mathbb{Z} \to \mathbb{Q}$. The ideal $(0) \in \mathbb{Q}$ is a maximal ideal (as $\mathbb{Q}$ only has two ideals (0) and (1)). Yet $\varphi^{-1}(0) = (0)$ is a prime ideal but not a maximal ideal. $\square$

解答题三 (10 分) 记 R 为一整环, F 为其分式域. 对 F 中任一元素 q, 定义 $I_q := \{r \in R \,|\, rq \in R\}$.

(1) 证明: I_q 是环 R 的一个理想.

(2) 现设 $R = \mathbb{Z}[\sqrt{-3}]$ 及 $q = (1-\sqrt{-3})/2 = 2/(1+\sqrt{-3}) \in F$. 证明: I_q 不是主理想.

Let R be an integral domain and F be its quotient field. For any element $q \in F$, define $I_q := \{r \in R \,|\, rq \in R\}$.

(1) Show that each I_q is a nonzero ideal of R.

(2) Now suppose that $R = \mathbb{Z}[\sqrt{-3}]$ and let $q = (1-\sqrt{-3})/2 = 2/(1+\sqrt{-3}) \in F$. Show that I_q is not a principal ideal.

证明. (1) For $r_1, r_2 \in I_q$, namely $r_1 q \in R$ and $r_2 q \in R$, we must have $(r_1 - r_2)q = r_1 q - r_2 q \in R$ and thus $r_1 - r_2 \in I_q$. Similarly, if $r \in I_q$ and $a \in R$, then $(ar)q = a \cdot rq \in R$. So $ar \in I_q$. From this, I_q is an ideal.

To see that $I_q \neq (0)$, we may write $q = a/b \in F$ with $a, b \in R$ and $b \neq 0$. Then $b \in I_q$; so I_q is nonzero.

(2) First of all, $2 \in I_q$ because $2q = 1 - \sqrt{-3} \in R$, and $1 + \sqrt{-3} \in I_q$ because $(1+\sqrt{-3})q = 2 \in R$. Suppose that I_q is principal, say $I_q = (\alpha)$ with $\alpha \in R$, then $2 = \alpha\beta$ for some $\beta = x + \sqrt{-3}y \in R$ (with $x, y \in \mathbb{Z}$). Consider the norm map $N : \mathbb{Z}[\sqrt{-3}] \to \mathbb{Z}$; $N(z) = z\bar{z}$, where $\bar{z}$ is the complex conjugation. We have

$$4 = N(2) = N(\alpha)N(\beta).$$

So $N(\alpha) = x^2 + 3y^2$ is a divisor of 4. There are only two options:

- either $\alpha = \pm 1$, in which case, $1 \in I_q$, meaning $q \in R$, but it is not,
- or $N(\alpha) = 4$, then $N(\beta) = 1$ forcing $\beta = \pm 1$ and thus $\alpha = \pm 2$. But then $1 + \sqrt{-3} \in I_q = (2)$ is absurd, as $\frac{1+\sqrt{-3}}{2} \notin R$.

To sum up, I_q is not a principal ideal. $\square$

解答题四 (15 分) 记 $R=\mathbb{Z}+x\mathbb{Q}[x]\subset\mathbb{Q}[x]$ 是由常数项为整数的有理系数多项式构成的集合.

(1) 证明: R 是一个整环, 且它的可逆元只有 ±1.

(2) 证明: R 中的不可约元恰为

- $\pm p$ (对所有素数 p),
- 常数项为 ±1 的且在 $\mathbb{Q}[x]$ 中不可约的多项式 $f(x)$.

证明这些不可约元都是 R 中的素元.

(3) 证明 x 不可以被写成 R 中不可约元的乘积, 从而证明 R 不是唯一分解整环.

Let $R=\mathbb{Z}+x\mathbb{Q}[x]\subset\mathbb{Q}[x]$ be the set of polynomials in x with rational coefficients whose constant term is an integer.

(1) Prove that R is an integral domain and its units are ±1.

(2) Show that the irreducibles in R are $\pm p$ where p is a prime in $\mathbb{Z}$ and the polynomials $f(x)$ that are irreducible in $\mathbb{Q}[x]$ and have constant term ±1. Prove that these irreducibles are prime in R.

(3) Show that x cannot be written as a product of irreducibles in R and conclude that R is not a U.F.D.

证明. (1) Since R is a subring of an integral domain $\mathbb{Q}[x]$, zero-divisors of R are automatically zero-divisors of $\mathbb{Q}[x]$, where there is none. So R is an integral domain. For the same reasoning, a unit of R must be a unit of $\mathbb{Q}[x]$ which are precisely nonzero constant polynomials. Yet polynomials in R have constants in $\mathbb{Z}$, so the units in R can only be those constants $a\in\mathbb{Z}$ whose inverse a^{-1} are also in $\mathbb{Z}$. So $R^\times=\{\pm1\}$.

(2) First consider the constant polynomials $f(x)=a$ with $a\in\mathbb{Z}$; it is irreducible if and only if a is irreducible in $\mathbb{Z}$ and thus if and only if $a=\pm p$.

Now consider a polynomial $f(x)\in R$ with degree ≥ 1. There are three cases:

(i) If the constant term $f(0)\neq\pm1$, then we may take $n=f(0)$ if $f(0)\neq 0$ and $n=2$ if $f(0)=0$. Then $f(x)=n\cdot\frac{1}{n}f(x)$ is a factorization of $f(x)$ into product of two non-unit elements in R; so $f(x)$ is not irreducible.

(ii) If the constant term of $f(x)$ is ±1, and if $f(x)$ factors as $a(x)b(x)$ in $\mathbb{Q}[x]$ with $\deg a(x)\geq 1$ and $\deg b(x)\geq 1$, then we may modify $a(x)$ and $b(x)$ so that their constant terms are both in $\{\pm1\}$, and thus $f(x)$ is not irreducible in R.

(iii) If the constant term of $f(x)$ is ±1 and if $f(x)$ is irreducible in $\mathbb{Q}[x]$, we claim that $f(x)$ is also irreducible. Suppose not, $f(x)=a(x)b(x)$. If both functions have degree ≥ 1, this would then show that $f(x)$ is not irreducible in $\mathbb{Q}[x]$, which is a contradiction. So WLOG, we may assume that $a(x)$ is a constant polynomial. But then comparing the constant coefficients $f(x) = a(x)b(x)$, we see that $a(x) = \pm 1$, which means that $a(x)$ is a unit. This shows that such $f(x)$ is irreducible.

We now show that the irreducible elements above are prime elements, starting with $\pm p$: if $\pm p$ divides $f(x)g(x)$, then the constant term of either $f(x)$ or $g(x)$ is divisible by p. WLOG it is $f(x)$, then $f(x) = (\pm p) \cdot (\pm \frac{1}{p} f(x))$ is a factorization in R, so $\pm p$ divides $f(x)$.

Next, if $p(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$ with constant ± 1, and suppose that $p(x)|a(x)b(x)$ in R. Then in $\mathbb{Q}[x]$, $p(x)$ divides $a(x)$ or $b(x)$. WLOG, say it is $a(x)$, then $a(x) = p(x)c(x)$. Comparing the constant term, the constant term of $c(x)$ is plus-minus of the constant of $a(x)$. So $c(x) \in R$ as well. So $p(x)$ divides $a(x)$ in R. This shows that all elements above are prime elements.

(3) If x is factored as a product of polynomials in R (or even in $\mathbb{Q}[x]$), one of the factors must be a nonzero multiple of x. But such an element does not belong to the list in (2). So x cannot be written as a product of irreducible elements. So R is not a UFD. $\square$

解答题五 (15 分) 设 H 是 G 的子群, 令

$$K := \bigcap_{g \in G} gHg^{-1}$$

为群 H 所有共轭的交.

(1) 证明: K 是 G 的正规子群.

(2) 证明: 若 $[G : H]$ 是有限的, 则 $[G : K]$ 也是有限的.

Let H be a subgroup of G. Define

$$K := \bigcap_{g \in G} gHg^{-1}$$

to be the intersection of all conjugates of H.

(1) Show that K is a normal subgroup of G.

(2) Show that if $[G : H]$ is finite, then $[G : K]$ is finite. (Hint: first show that the intersection above defining K is essentially a finite intersection.)

证明. (1) We check that for any $s \in G$,

$$sKs^{-1} := s\Big(\bigcap_{g \in G} gHg^{-1}\Big)s^{-1} = \bigcap_{g \in G} sgHg^{-1}s^{-1} = \bigcap_{g' \in G} g'Hg'^{-1} = K$$

with $g' = sg$ in the notation. So K is a normal subgroup of G.

(2) We start with a lemma: if H_1 and H_2 are subgroups of G of finite index. Then $H_1 \cap H_2$ is a subgroup of G of finite index. The easiest way to see this is to let H_1 act on the left cosets G/H_2 by left multiplication. Then the stabilizer group at H_2 is precisely $H_1 \cap H_2$. We know that the index of $H_1 \cap H_2$ inside H_1 is precisely the number of elements in the orbit of the identity coset H_2 in G/H_2 under this action. In particular, $[H_1 : H_1 \cap H_2] \leq \#(G/H_2)$. It then follows that $[G : H_1 \cap H_2] \leq [G : H_1] \cdot [G : H_2]$.

Now, we come back to the proof of (2). As $[G : H]$ is assumed to be finite, we may choose a finite set of coset representatives $g_1H, \dots, g_rH$ of G/H. Then for every element $g \in g_iH$ (writing $g = g_ih$), we have

$$gHg^{-1} = g_ihHh^{-1}g_i^{-1} = g_iHg_i^{-1}.$$

So K is the intersection

$$\bigcap_{i=1}^{r} g_iHg_i^{-1},$$

which is the intersection of finitely many finite index subgroups. By the lemma above, $[G : K]$ is finite as well. $\square$

解答题六 (15 分) 设 R 为一交换环. 一个导数算子是指一个映射 $D: R \to R$ 满足对所有 $a, b \in R$: $D(a+b) = D(a) + D(b)$ 和 $D(ab) = aD(b) + D(a)b$.

(1) 考虑环 $R[x]/(x^2)$, 证明: 存在一个双射

$$\{\text{导数算子 } D: R \to R\} \longleftrightarrow \{\text{环同态 } \varphi: R \to R[x]/(x^2) \text{ 使得 } \varphi \bmod x \text{ 是恒同}\}.$$

(2) 如果 D 是 R 上的一个导数算子且 $e \in R$ 是一个幂等元 (即 $e = e^2$), 证明: $D(e) = 0$.

Let R be a commutative ring. A *derivation* $D: R \to R$ is a map satisfying $D(a+b) = D(a) + D(b)$ and $D(ab) = aD(b) + D(a)b$ for all $a, b \in R$.

(1) Consider the ring $R[x]/(x^2)$, show that there is a bijection

$$\{\text{Derivations } D: R \to R\} \longleftrightarrow \left\{ \begin{array}{l} \text{Ring homomorphisms } \varphi: R \to R[x]/(x^2) \\ \text{ such that } \varphi \bmod x = \mathrm{id} \end{array} \right\}.$$

(2) If D is a derivation of R and $e \in R$ is an idempotent (i.e. $e = e^2$), prove that $D(e) = 0$.

证明. (1) The derivation automatically satisfies the condition that $D(0) = 0$ and $D(1) = 0$ (by setting $a = b = 0$ and $a = b = 1$ in the first and the second equation, respectively.)

The bijection is given by, sending a derivation $D: R \to R$ to the homomorphism

$$\varphi_D(a) = a + xD(a),$$

for every $a \in R$. The condition that φ_D is a homomorphism is equivalent to, for $a, b \in R$

$$\varphi_D(ab) = \varphi_D(a)\varphi_D(b) \text{ and } \varphi_D(a+b) = \varphi_D(a) + \varphi_D(b), \quad \text{equivalently,}$$

$$ab + xD(ab) = (a + xD(a))(b + xD(b)) = ab + bxD(a) + axD(b) + x^2 D(a)D(b)$$
$$\text{and } a + b + x(D(a+b)) = a + xD(a) + b + xD(b).$$

Noting that $x^2 = 0$, this is clearly equivalent to the condition that $D(ab) = aD(b) + bD(a)$ and $D(a+b) = D(a) + D(b)$ for $a, b \in R$. Conversely, given a homomorphism $\varphi: R \to R[x]/(x^2)$, we may recover the derivation $D(a)$ for $a \in R$ by taking the x-coefficient of $\varphi(a) - a$.

(2) Note that $D(e) = D(e^2) = 2eD(e)$. So $(1-2e)D(e) = 0$. Yet we observe

$$(1-2e)^2 = 1 - 4e + 4e^2 = 1.$$

So $D(e) = (1-2e)^2 D(e) = (1-2e) \cdot 0 = 0$.

(Remark: applying $(1-2e)$ to the equation might seem a little tricky, indeed, it is not. Note that an idempotent e splits R into the product $eR \times (1-e)R$. And $1 - 2e = (1-e) - e$ corresponds to the element $(-1, 1)$. In order to turn that into the identity element $(1, 1)$, we need to multiply with $(-1, 1)$, namely $1 - 2e$.) $\square$

解答题七 (15 分) 令 p 为一奇素数. 设 G 是一个阶为 $p(p+1)$ 的有限群, 且假设 G 没有正规的西罗-p 子群.

(1) 求 G 中阶不为 p 的元素的个数.

(2) 证明: G 中阶不整除 p 的元素构成一个共轭类.

(3) 证明: $p+1$ 是 2 的幂.

Let p be an odd prime number, and let G be a finite group of order $p(p+1)$. Assume that G does not have a normal Sylow p-subgroup.

(1) Find the number of elements of G with order different from p.

(2) Show that the set of elements of G whose order does not divide p form exactly one conjugacy class.

(3) Prove that $p+1$ is a power of 2.

证明. (1) Let n_p denote the number of Sylow p-subgroups. By Third Sylow Theorem, $n_p|p+1$ and $n_p \equiv 1 \bmod p$. As G has no normal Sylow p-subgroups, $n_p = p+1$. Note that each Sylow p-subgroup has order p so is isomorphic to Z_p. It follows that the number of elements of order p in each Sylow p-subgroups is $p-1$, and *the order p elements in different Sylow p-subgroups are different as they generate different Sylow p-subgroups.* So the total number of order p elements is $(p-1)(p+1) = p^2-1$. So the number of elements in G whose order does not divide p is $p(p+1)-(p^2-1)-1 = p$.

(2) The set A of elements in G whose order does not divide p is p. Let P be a Sylow p-subgroup. Consider the conjugation action of P on A. We claim that this action is nontrivial. Then it would follow that one orbit has size at least p. So the entire A is already a conjugacy class under the P-action. (2) follows from this.

Let $a \in A$. Consider the action of G on $\mathrm{Syl}_p(G)$, especially the stabilizer group K at P. Clearly, P is contained in the stabilizer group K. If P commutes with a, then a also belongs to the stabilizer group K. Then the stabilizer group K would be bigger than p elements, and then n_p cannot be as big as $p+1$.

So the conjugation action of P on a is nontrivial, proving (2).

(3) Fix $a \in A$. Then G acts on A by conjugation by (2). Let H denote the stabilizer group at a. As proved in (2), none of the nontrivial elements in P fixes a. So $H \subseteq A \cup \{e\}$. But looking at the size of elements, we deduce that $H = A \cup \{e\}$; and elements in H commutes with every element in A. Thus H is an abelian group.

Yet as nontrivial elements in H are conjugate, they have the same order, which must be a factor of $p+1$ (and taking any prime factors of $p+1$ at least once). It follows that $p+1$ must be a prime power. Already $p+1$ is an even number. So $p+1$ is a power of 2. □

Remark: it seems that the problem is modeled on the following example: let p be a prime of the form $2^N - 1$; consider the finite field $\mathbb{F}_{2^N}$ of 2^N-elements (there is a unique such field). Then $\mathbb{F}_{2^N}^{\times}$ is a cyclic group of order p. The group in the problem can be the semi-direct product $\mathbb{F}_{2^N} \rtimes \mathbb{F}_{2^N}^{\times}$.

附加题一 (+5 分) 设 $K \subseteq H$ 为群 G 的子群满足 $K \lhd H$.

(1) 证明: H 在共轭作用下保持 $C_G(K)$ 不动 ($C_G(K)$ 是 K 在 G 中的中心化子).

(2) 设 $H \rhd G$ 和 $C_H(K) = 1$, 证明: H 与 $C_G(K)$ 交换.

Let G be a group and let $K \subseteq H$ be subgroups of G with $K \lhd H$.

(1) Prove that H normalizes $C_G(K)$ (the centralizer of K in G).

(2) If $H \lhd G$ and $C_H(K) = 1$, prove that H centralizes $C_G(K)$.

证明. (1) We need to show that for any $c \in C_G(K)$ and $h \in H$, we have $hch^{-1} \in C_G(K)$. For this we need to prove that for any $k \in K$, we have

$$hch^{-1}k = khch^{-1}.$$

This is equivalent to

$$ch^{-1}kh = h^{-1}khc$$

As $K \lhd H$, we have $h^{-1}kh \in K$, so c must commute with $h^{-1}kh$, proving the equality above.

(2) It suffices to show that for any $h \in H$ and $c \in C_G(K)$, we have $hch^{-1}c^{-1} = 1$. As $C_H(K) = 1$, it suffices to check that $hch^{-1}c^{-1} \in C_H(K)$. As H is normal in G, $ch^{-1}c^{-1} \in H$; so $hch^{-1}c^{-1} \in H$. As proved in (1), H normalizes $C_G(K)$; so $hch^{-1} \in C_G(K)$. Thus $hch^{-1}c^{-1} \in C_G(K)$. Combining these two gives

$$hch^{-1}c^{-1} \in H \cap C_G(K) = C_H(K) = \{1\}.$$

The problem is solved. $\square$

附加题二 (+5 分) 设 G 是一个有限群, 记 $\mathrm{Syl}_p(G)$ 为它的西罗 p-子群的集合.

(1) 如果 S 和 T 是 $\mathrm{Syl}_p(G)$ 中不同的元素使得 $\#(S\cap T)$ 取得最大值. 证明: $N_G(S\cap T)$ 没有正规的西罗 p-子群.

(2) 证明: $S\cap T=1$ 对所有 $S,T\in \mathrm{Syl}_p(G)$ $(S\neq T)$ 成立当且仅当对任一 G 的非平凡 p-子群 P, $N_G(P)$ 包含一个正规西罗 p-子群.

Let G be a finite group and let $\mathrm{Syl}_p(G)$ denote its set of Sylow p-subgroups.

(1) Suppose that S and T are distinct members of $\mathrm{Syl}_p(G)$ chosen so that $\#(S\cap T)$ is maximal among all such intersections. Prove that the normalizer $N_G(S\cap T)$ does not admit normal Sylow p-subgroup.

(2) Show that $S\cap T=1$ for all $S,T\in\mathrm{Syl}_p(G)$, with $S\neq T$, if and only if $N_G(P)$ has exactly one Sylow p-subgroup for every nonidentity p-subgroup P of G.

证明. (1) We shall exhibit two Sylow p-subgroups of $N_G(S\cap T)$ as follows:

$$S' := \big\{s\in S \,\big|\, sTs^{-1}\cap S = T\cap S\big\},$$

$$T' := \big\{t\in T \,\big|\, tSt^{-1}\cap T = S\cap T\big\}.$$

Clearly, both S' and T' contain $S\cap T$. We shall show that each S' and T' strictly contains $S\cap T$ and that they are indeed Sylow p-subgroups of $N_G(S\cap T)$; part (1) would then follow from this because we have exhibited two different Sylow p-subgroups of $N_G(S\cap T)$. By symmetry, it suffices to treat one of them, say S'.

First of all, $N_S(S\cap T)$ is contained in S'. Yet S is a p-group, so the normalizer of $S\cap T$ is strictly larger than $S\cap T$. So S' strictly contains $S\cap T$.

We next show that S' is a Sylow p-subgroup of $N_G(S\cap T)$. Suppose not, then S' is strictly contained in a Sylow p-subgroup $P\subseteq N_G(S\cap T)$, which in turn is contained in a Sylow p-subgroup $\widetilde{P}$ of G. We note that $\widetilde{P}\neq S$; this is because

$$N_G(S\cap T)\cap S = S' \subsetneq P \subseteq \widetilde{P}\cap N_G(S\cap T).$$

Yet $\widetilde{P}\cap S$ contains S' which is strictly bigger than $S\cap T$. This contradicts with the maximality of $S\cap T$. Therefore, we see that S' is a Sylow p-subgroup of $N_G(S\cap T)$. This completes the proof of (1).

(2) We first show the sufficiency: suppose that $N_G(P)$ contains exactly one Sylow p-subgroup of every nonidentity p-subgroup P of G, and suppose that it is not true that $S\cap T = 1$ for all $S,T\in\mathrm{Syl}_p(G)$ with $S\neq T$. Then take $S,T\in\mathrm{Syl}_p(G)$ so that $\#(S\cap T)$ is maximal, by (1), $N_G(S\cap T)$ does not admit normal Sylow p-subgroups. This is a contradiction, proving the necessity.

We now prove the necessity. As the intersection any two distinct Sylow p-subgroups is trivial, each nonidentity p-subgroup P is contained in a unique Sylow p-subgroup S of G. Then any element $g \in G$ that normalizes P must force $P = gPg^{-1} \subseteq gSg^{-1}$. This then forces $S = gSg^{-1}$. So we deduce that $N_G(P) \leqslant N_G(S)$. It is well-known that S is a normal Sylow p-subgroup of $N_G(S)$. So $S \cap N_G(P)$ is a normal subgroup of $N_G(P)$. Moreover, there is a natural injective homomorphism

$$N_G(P)/\big(N_G(P) \cap S\big) \hookrightarrow N_G(S)/S$$

this then implies that $[N_G(P) : N_G(P) \cap S]$ divides $[N_G(S) : S]$ which is prime-to-p. So $N_G(P) \cap S$ is a normal Sylow p-subgroup of $N_G(P)$. $\square$