MA553: Qual Preparation

Carlos Salinas

July 21, 2016

Contents

1 Ulrich

1.1 Ulrich: Winter 2002

Problem 1. Let G be a group and H a subgroup of finite index. Show that there exists a normal subgroup N of G of finite index with $N \subset H$.

Solution. ▶ Let $n = [G : H]$ and $X = \{ H, g_1H, \ldots, g_{n-1}H \}$ the set of left-cosets of H in G with representatives $g_0 = e, g_1, \ldots, g_{n-1}$. Let G act on X by left multiplication, i.e., $g \mapsto gg_iH$; this is indeed an action since $e(g_iH) = eg_iH = g_iH$ for all $g_iH \in X$ and for $k_1, k_2 \in G$ $k_2(k_1g_iH) = k_2k_1g_iH = (k_2k_1)g_iH$. By Cayley's theorem, this induces a homomorphism $\varphi\colon G \to S_n$. Note that the action is not necessarily faithful. However, by the first isomorphism theorem, the kernel of φ, $N = \operatorname{Ker}\varphi$, is a normal subgroup of G with index $[G : N] \leq |S_n| = n!$ and $N \subset H$ since $g \in N$ if and only if $gg_iH = g_iH$ which, in particular, implies that $gH = H$. Thus, $N \subset H$ and $[G : N] < \infty$. ◀

Problem 2. Show that every group of order 992 ($= 32 \cdot 31$) is solvable.

Solution. ▶ Suppose G is a group with order $|G| = 992 = 2^5 \cdot 3$. By Sylow's theorem, the number of 2-Sylow subgroups in G is either 1 or 3. If the number of 2-Sylow subgroups is 1, then $P \lhd G$ and the quotient G/P has order $[G : P] = 3$, hence, is cyclic. Moreover, since P is a p-group, it is solvable. Since P and G/P are solvable, G is solvable.

Now, suppose the number of 2-Sylow subgroups is 3. Let $\operatorname{Syl}_2(G) = \{P, P_1, P_2\}$. Then, by Sylow's theorem, the three 2-Sylow subgroups are conjugate, i.e., there exists $g_1, g_2 \in G$ such that $P_1 = g_1 P {g_1}^{-1}$ and $P_2 = g_2 P {g_2}^{-1}$. Thus, G acts on the set $\operatorname{Syl}_2(P)$ by conjugation. This actions defines a (not necessarily injective) homomorphism $\varphi\colon G \to S_3$. Now, we ask: What is the kernel of this homomorphism? By the first isomorphism theorem, we know that the index of the kernel in G divides the order of S_3, i.e., $[G : \operatorname{Ker}\varphi] \mid 6$. Since $|G| < \infty$ implies that the order of the kernel is one of the following values

$$|\operatorname{Ker}\varphi| = 2^4, 2^4 \cdot 3, 2^5, 2^5 \cdot 3.$$

Now, $|\operatorname{Ker}\varphi| \neq 2^5 \cdot 3$ since we know at least one automorphism, namely conjugation by g_1, which sends $P \mapsto P_1$. Thus, the order of the kernel is either 2^4, $2^4 \cdot 3$ or 2^5. If the $|\operatorname{Ker}\varphi| = 2^4$ or 2^5, we are done for similar reasons to the argument we gave in the previous paragraph, namely, that $\operatorname{Ker}\varphi \lhd G$ and $G/\operatorname{Ker}\varphi$ is solvable (for $|\operatorname{Ker}\varphi| = 2^4$, the quotient $G/\operatorname{Ker}\varphi$ has order 6 so is isomorphic to one of two groups, S_3 or Z_6, both of which are solvable).

Suppose $\operatorname{Ker}\varphi$ has order $2^4 \cdot 3$. Then the number of 3-Sylow subgroups is either 1, 4 or 16. If this number is 1, we are done as $Q \in \operatorname{Syl}_3(\operatorname{Ker}\varphi)$ is a normal subgroup and the quotient is a p-group. Suppose the number of 3-Sylow subgroups is 16. Then there are $16 \cdot 2 = 32$ elements of order 3 in $\operatorname{Ker}\varphi$. ◀

Problem 3. Let G be a group of order 56 with a normal 2-Sylow subgroup Q, and let P be a 7-Sylow subgroup of G. Show that either $G \simeq P \times Q$ or $Q \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

[*Hint*: P acts on $Q \setminus \{e\}$ via conjugation. Show that this action is either trivial or transitive.]

Solution. ► First, note that, by the fundamental theorem of arithmetic, the order of G can be broken down into $56 = 2^3 \cdot 7$. Suppose G has a normal 2-Sylow subgroup Q and let $P \in \mathrm{Syl}_3(G)$. Then $|\mathrm{Syl}_3(G)| = 1, 4$. If $|\mathrm{Syl}_3(G)| = 1$, then P is the unique 3-Sylow subgroup of G, hence it is normal. Thus, $|P||Q| = |G|$ and $PQ = G$ since, if $g \in Q \cap G$, then $|g| = 3$, but $2 \mid |g|$ so $g = e$. Thus, $G \simeq P \times Q$.

Now, suppose $|\mathrm{Syl}_3(G)| = 4$. Then G contains 4 3-Sylow subgroups which, by Sylow's theorem, are conjugate, i.e., there exists $g_1, g_2, g_3 \in G$ such that $\mathrm{Syl}_p(G) = \left\{P, g_1 P {g_1}^{-1}, g_2 P {g_2}^{-1}, g_3 P {g_3}^{-1}\right\}$. Let P act on Q by conjugation. Then ◄

Problem 4. Let R be a commutative ring and $\mathrm{Rad}(R)$ the intersection of all maximal ideals of R.

(a) Let $a \in R$. Show that $a \in \mathrm{Rad}(R)$ if and only if $1 + ab$ is a unit for every $b \in R$.
(b) Let R be a domain and $R[X]$ the polynomial ring over R. Deduce that $\mathrm{Rad}(R[X]) = 0$.

Solution. ► ◄

Problem 5. Let R be a unique factorization domain and P a prime ideal of $R[X]$ with $P \cap R = 0$.

(a) Let n be the smallest possible degree of a nonzero polynomial in P. Show that P contains a primitive polynomial f of degree n.
(b) Show that P is the principal ideal generated by f.

Solution. ► ◄

Problem 6. Let k be a field of characteristic zero. assume that every polynomial in $k[X]$ of odd degree and every polynomial in $k[X]$ of degree two has a root in k. Show that k is algebraically closed.

Solution. ► ◄

Problem 7. Let $k \subset K$ be a finite Galois extension with Galois group $\mathrm{Gal}(K/k)$, let L be a field with $k \subset L \subset K$, and set $H = \{\, \sigma \in \mathrm{Gal}(K/k) : \sigma(L) = L \,\}$.

(a) Show that H is the normalizer of $\mathrm{Gal}(K/L)$ in $\mathrm{Gal}(K/k)$.
(b) Describe the group $H/\mathrm{Gal}(K/L)$ as an automorphism group.

Solution. ► ◄

2 Field Theory and Galois Theory

Notes taken from Keith Conrad's blurbs.

2.1 Roots and irreducibles

This handout discusses relationships between roots of irreducible polynomials and field extensions.

2.1.1 Roots in larger fields

For most fields K, there are polynomials in $K[X]$ without a root in K. Consider X^2+1 in $\mathbb{R}[X]$ or X^3-2 in $\mathbb{F}_7[X]$. If we are willing to enlarge the field. The following is due to Kronecker.

Theorem 1. *Let K be a field and $f(X)$ be a nonconstant polynomial in $K[X]$. There exists a field extension of K containing a root of $f(X)$.*

Proof. It suffices to prove the theorem when $f(X) = \pi(X)$ is irreducible.

Set $F = K[t]/(\pi(t))$ where t is an indeterminate. Since $\pi(t)$ is irreducible in $K[t]$, F is a field. Inside of F we have K as a subfield: the congruence classes represented by constants. There is also a root of $\pi(X)$ in F, namely the class of t. Indeed, writing $\bar{t}$ for the congruence class of t in F, the congruence $\pi(t) \equiv 0 \mod \pi(t)$ becomes the equation $\pi(\bar{t}) = 0$ in F. ■

Corollary 2. *Let K be a field and $f(X) = c_m X^m + \cdots + c_0$ a polynomial in $K[X]$ with degree $m \geq 1$. There is a field $L \supset K$ such that in $L[X]$*

$$F(X) = c_m(X - \alpha_1)\cdots(X - \alpha_m).$$

Proof. We induct on the degree m. The case $m = 1$ is clear, using $L = K$. By Theorem 2.1, there is a field $F \supset K$ such that that $f(X)$ has a root in F, say α. Then in $F[X]$,

$$f(X) = (X - \alpha_1)g(X),$$

where $\deg g(X) = m - 1$. The leading coefficient of $g(X)$ is also c_m.

Since $g(X)$ has smaller degree than $f(X)$, by induction on the degree there is a field $L \supset F$ (so $L \supset K$) such that $g(X)$ decomposes into linear factors in $L[X]$, so we get the desired factorization of $f(X)$ in $L[X]$. ■

Corollary 3. *Let $f(X)$ and $g(X)$ be nonconstant in $K[X]$. They are relatively prime in $K[X]$ if and only if they do not have a common root in any extension field of K.*

Proof. Assume $f(X)$ and $g(X)$ are relatively prime in $K[X]$. Then we can write

$$f(X)u(X) + g(X)v(X) = 1$$

for some $u(X)$ and $v(X)$ in $K[X]$. If there were an α in a field extension of K which is a common root of $f(X)$ and $g(X)$, then substituting α for X in the above polynomial ■