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 $X = \{ H, g_1 H, \dots, g_{n-1} H \}$ the set of left-cosets of H in G with representatives $g_0 = e, g_1, \dots, g_{n-1}$. Let G act on X by left multiplication, i.e., $g \mapsto g g_i H$; this is indeed an action since $e(g_i H) = e g_i H = g_i H$ for all $g_i H \in X$ and for $k_1, k_2 \in G$ $k_2(k_1 g_i H) = k_2 k_1 g_i H = (k_2 k_1) g_i H$. 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 $[G : N] \le |S_n| = n!$ and $N \subset H$ since $g \in N$ if and only if $g g_i H = g_i H$ 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 $\mathrm{Syl}_2(G) = \{P, P_1, P_2\}$. 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 $\mathrm{Syl}_2(P)$ 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, $|\operatorname{Ker}\varphi| \ne 2^5 \cdot 3$ 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 $Q \in \mathrm{Syl}_3(\operatorname{Ker}\varphi)$ 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 $Q \simeq \mathbf{Z}/(2) \times \mathbf{Z}/(2) \times \mathbf{Z}/(2)$.

[*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 $\mathbf{R}[X]$ or X^3-2 in $\mathbf{F}_7[X]$. 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 $\pi(t)\equiv 0 \bmod \pi(t)$ becomes the equation $\pi(\bar{t})=0$ in F. ∎

Corollary 2. *Let K be a field and $f(X)=c_mX^m+\cdots+c_0$ 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 identity makes the left side 0 while the right side is 1. This is a contradiction, so $f(X)$ and $g(X)$ have no common root in any field extension of K.

Now assume $f(X)$ and $g(X)$ are not relatively prime in $K[X]$. Say, $h(X) \in K[X]$ is a (nonconstant) common factor. There is a field extension of K in which $h(X)$ has a root and this root will be a common root of $f(X)$ and $g(X)$. ■

2.1.2 Divisibility and roots in $K[X]$

There is an important connection between roots of a polynomial and divisibility by *linear* polynomials. For $f(X) \in K[X]$ and $\alpha \in K$, $f(\alpha) = 0 \iff (X-\alpha) \mid f(X)$. The next result is an analogue for divisibility by higher degree polynomials in $K[X]$, provided they are irreducible. (All linear polynomials are irreducible.)

Theorem 4. *Let $\pi(X)$ be an irreducible in $K[X]$ and let α be a root of $\pi(X)$ in some larger field. For $h(X)$ in $K[X]$, $h(\alpha) = 0 \iff \pi(X) \mid h(X)$ in $K[X]$.*

Proof. If $h(X) = \pi(X)g(X)$, then $h(\alpha) = \pi(\alpha)g(\alpha) = 0$.

Now assume $h(\alpha) = 0$. Then $h(X)$ and $\pi(X)$ have a common root, so by Corollary 2.4 they have a common factor in $K[X]$. Since $\pi(X)$ is irreducible, this means $\pi(X) \mid h(X)$ in $K[X]$. To see this argument more directly, suppose $h(\alpha) = 0$ and $\pi(X)$ does not divide $h(X)$. Then (because π is irreducible) the polynomials $\pi(X)$ and $h(Xx)$ are relatively prime in $K[X]$ so we can write

$$\pi(X)u(X) + h(X)v(X) = 1$$

for some $u(X), v(X) \in K[X]$. Substitute α for X and the left side vanishes. The right side is 1 so we have a contradiction. ■

Theorem 5. *Let K be a field and L be a larger field. For $f(X)$ and $g(X)$in $K[X]$, $f(X) \mid g(X)$ in $K[X]$ if and only if $f(X) \mid g(X)$ in $L[X]$.*

Proof. It is clear that divisibility inf $K[X]$ implies divisibility in larger $L[X]$. Conversely suppose $f(X) \mid g(X)$ in $L[X]$. Then

$$g(X) = f(X)h(X)$$

for some $h(X) \in L[X]$. By the division algorithm in $K[X]$,

$$g(X) = f(X)q(X) + r(X)$$

where $q(X)$ and $r(X)$ are in $K[X]$ and $r(X) = 0$ or $\deg r < \deg f$. Comparing these two formulas for $g(X)$, the uniqueness of the division algorithm in $L[X]$ implies $q(X) = h(X)$ and $r(X) = 0$. Therefore $g(X) = f(X)q(X)$, so $f(X) \mid g(X)$ in $L[X]$. ■

2.2 Raising to the pth power in characteristic p

Lemma 6. *Let A be a commutative ring with prime characteristic. Pick any a and b in A.*

(a) $(a+b)^p = a^p + b^p$.

(b) *When A is a domain, $a^p = b^p \implies a = b$.*

Proof. (a) By the binomial theorem,

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p.$$

For $1 \le k \le p-1$, the integer $\binom{p}{k}$ is a multiple of p, so the intermediate terms are 0 in A.

(b) Now assume A is a domain and $a^p = b^p$. Then $0 = a^p - b^p = (a-b)^p$. (Note $(-1)^p = -1$ for $p \neq 2$, and also for $p = 2$ since $2 = 0 \implies -1 = 1$ in A.) Since A is a domain, $a - b = 0$ so $a = b$. ∎

Lemma 7. *Let F be a field containing $\mathbf{F}_p$. For $c \in F$, $c \in \mathbf{F}_p \iff c^p = c$.*

Proof. Every element c of $\mathbf{F}_p$ satisfies the equation $c^p = c$. Conversely, solutions to this equation are the roots of $X^p - X$, which has at most p roots. The elements of $\mathbf{F}_p$already fulfill this upper bound, so there are no further roots in characteristic p. ∎

Theorem 8. *For any $f(X) \in \mathbf{F}_p[X]$, $f(X)^p = f(X^{p^r}) = f(X^{p^r})$ for $r \ge 0$. If F is a field of characteristic p other than $\mathbf{F}_p$, this is not always true in $F[X]$.*

Proof. Writing

$$f(X) = c_m X^m + c_{m-1} X^{m-1} + \cdots + c_1 X + c_0,$$

Lemma 4.1a with $A = \mathbf{F}_p[X]$ gives

$$\begin{aligned} f(X)^p &= \left(c_m X^m + c_{m-1} X^{m-1} + \cdots + c_1 X + c_0\right)^p \\ &= {c_m}^p X^{mp} + {c_{m-1}}^p X^{p(m-1)} + \cdots + {c_1}^p X^p + c_0^p \\ &= c_m (X^p)^m + c_{m-1} (X^p)^{m-1} + \cdots + c_1 X^p + c_0, \end{aligned}$$

since $c^p = c$ for any $c \in \mathbf{F}_p$. The last expression is $f(X^p)$. Applying this result r times, we find $f(X)^{p^r} = f(X^{p^r})$. ∎

Let $f(X) \in \mathbf{F}_p[X]$ be nonconstant, with degree m. Let $L \supset \mathbf{F}_p$ be a field over which $f(X)$ decomposes into linear factors, i.e., (2.1) holds. It is possible to that some roots of $f(X)$ are multiple roots. As long as that does not happen, the following corollary says something about the pth powers of the roots.

Corollary 9. *When $f(X) \in \mathbf{F}_p[X]$ has distinct roots, raising all roots of $f(X)$ to the pth power permutes the roots*

$$\{\alpha_1{}^p, \ldots, \alpha_m{}^p\} = \{\alpha_1, \ldots, \alpha_m\}.$$

Proof. Let $S = \{\alpha_1, \ldots, \alpha_m\}$. Since $f(X)^p = f(X^p)$ by Theorem 4.3, the pth power of each root of $f(X)$ is again a root of $f(X)$. Therefore raising to the pth power defines a function $\varphi\colon S \to S$. By Lemma 4.1b, φ takes different values on different elements of S. Since S is a finite set, φ must assume each element of S as a value (in the language of set theory, a one-to-one function from a finite set to itself is onto), so φ is a permutation of S. ■

2.3 Roots of irreducibles in $\mathbf{F}_p[X]$

Lemma 10. *For $h(X)$ in $\mathbf{F}_p[X]$ with degree m,*