UIUC Algebra Comprehensive Exams

Jiantong Liu

August 31, 2023

Introduction

I created this document in summer 2023 as an effort to prepare for the algebra comprehensive exam in August 2023, which I passed with 90/100. The document includes the specified syllabus and all comprehensive exams between January 2013 and May 2022, i.e., after the latest substantial revision of the syllabus in 2012. Most solutions are my own, although I did have to look up a few problems from forums like stackexchange, hence they are not guaranteed to be correct and should be used with caution, and I welcome improvements/corrections to the document.

MATH 500 Syllabus

Basic facts about groups, rings, vector spaces, such as those covered in Math 416 and Math 417 courses, are assumed. Instructors should not spend time on elementary material: the syllabus is quite full. Books that could be used include *Abstract Algebra* by Dummit and Foote, *Algebra* by Hungerford, and *Advanced Modern Algebra* by Rotman.

Math 500 exams from August 2012 and earlier are NOT a reliable guide to future exams, because the syllabus was revised substantially in Fall 2012.

1. Group Theory

    (a) Isomorphism theorems for groups.

    (b) Group actions on sets; orbits, stabilizers. Application to conjugacy classes, centralizers, normalizers.

    (c) The class equation with application to finite p-groups and the simplicity of A_5.

    (d) Composition series in a group. Refinement Theorem and Jordan-Hölder Theorem. Solvable and nilpotent groups.

    (e) Sylow Theorems and applications.

2. Commutative rings and Modules.

    (a) Review of subrings, ideals and quotient rings. Integral domains and fields. Polynomial rings over a commutative ring.

    (b) Euclidean rings, PID's, UFD's.

    (c) Brief introduction to modules (over commutative rings), submodules, uotient modules.

    (d) Free modules, invariance of rank. Torsion modules, torsion free modules. Primary decomposition theorem for torsion modules over PID's.

   (e) Structure theorem for finitely generated modules over a PID. Application to finitely-generated abelian groups and to canonical form of matrices.

   (f) Zorn's lemma and axiom of choice. Application to maximal ideals, bases of vector spaces.

3. Field Theory.

   (a) Prime fields, characteristic of a field.

   (b) Algebraic and transcendental extensions, degree of an extension. Irreducible polynomial of an algebraic element.

   (c) Normal extensions and splitting fields. Galois group of an extension.

   (d) Algebraic closure, existence and uniqueness via Zorn's Lemma. Finite fields.

   (e) Fundamental theorem of Galois theory.

   (f) Examples of Galois extensions. Cyclotomic extensions.

   (g) Application of Galois theory to solution of polynomial equations, symmetric functions and ruler and compass constructions.

1 May 2022

Problems

Problem 1.1. (a) Let H be a subgroup of a group G. Then G acts on the set G/H by left multiplication. This action naturally defines a homomorphism $\alpha : G \to S(G/H)$, where $S(X)$ is the group of permutations on a set X. Prove that the kernel of α is contained in H.

(b) Let L be a subgroup of a finite group K such that $[K : L] = p$, where p is the smallest prime that divides $|K|$. Prove that L is normal in K. *Hint*: Use part (a).

(c) Describe all finite groups of order p^2, where p is prime, up to isomorphism.

(d) Describe all finite groups of order 425 up to isomorphism.

Problem 1.2. Make $\mathbb{C}^3$ into a $\mathbb{C}[x]$-module by $f(x)v = f(A)v$ where $v \in \mathbb{C}^3$ and

$$A = \begin{pmatrix} 5 & 3 & 0 \\ 0 & 5 & 0 \\ 0 & 3 & 3 \end{pmatrix}.$$

Find polynomials $p_i(x)$ and exponents e_i such that $\mathbb{C}^3 \cong \bigoplus_i \mathbb{C}[x]/(p_i^{e_i})$ as $\mathbb{C}[x]$-modules.

Problem 1.3. Completely factor the following polynomials over the given fields, or prove they are irreducible.

(a) $x^3 + x + 2 \in \mathbb{Z}_3[x]$.

(b) $x^4 + x^3 + x + 3 \in \mathbb{Z}_5[x]$.

(c) $x^4 + x^3 + x^2 + 6x + 1 \in \mathbb{Q}[x]$.

Problem 1.4. (a) Let G be a finite subgroup of the multiplicative group K^* of a field K. Prove that G is cyclic.

(b) Let $k = \mathbb{Z}/p\mathbb{Z}$ be the finite field of order p, where p is a prime. Let K/k be a finite field extension of degree m. Prove that the elements of K are the roots of the polynomial $x^{p^m} - x$ over k.

(c) Prove that every irreducible polynomial $f(x) \in k[x]$ is separable.

Solutions

Problem 1. (a) By construction, the defined homomorphism is

$$\begin{aligned} \alpha : G &\to S(G/H) \\ g &\mapsto (f_g : hH \mapsto ghH) \end{aligned}$$

Therefore, take $g \in \ker(\alpha)$, we note that f_g is the identity map on the set G/H of cosets, and in particular the assignment $H \mapsto gH$ is the identity, i.e., $g \in H$. Therefore, $\ker(\alpha) \subseteq H$.

(b) Take $G = K$ and $H = L$, then by part (a) we define a homomorphism $\alpha : G \to S(G/H) = S_p$ via the action such that $\ker(\alpha) \subseteq H$, since $|G/H| = p$. By the first isomorphism theorem, we have $\frac{|G|}{|\ker(\alpha)|} = |\operatorname{im}(\alpha)| \mid p! = |S_p|$. In particular, $|\operatorname{im}(\alpha)|$ divides both $|G|$ and $p!$, but p is the smallest prime that divides $|G|$ already, then $|\operatorname{im}(\alpha)| = p$. Therefore, $[G : \ker(\alpha)] = p$, but $[G : H] = p$ as well, and $\ker(\alpha) \subseteq H$ by part (a), therefore $H = \ker(\alpha)$ and is normal in G, by construction.

(c) We claim that all such groups are either isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Let G be a group of order p^2. Suppose $x \in G$ has order p^2, then x generates G, therefore $G = \langle x \rangle = \mathbb{Z}/p^2\mathbb{Z}$. Now suppose there is no such $x \in G$ with order p^2, then we know that every non-trivial element has order p. Take some $e \neq x \in G$, then x has order p, therefore $X = \langle x \rangle \subseteq G$ is a subgroup of order p, therefore $G \neq X$. Now pick some $y \in G \setminus X$, then y also has order p, therefore $Y = \langle y \rangle$ is another subgroup of order p. Note that $X \cap Y = \{e\}$: indeed, suppose there exists some element in $X \cap Y$, then $x^i = y^j$ for some $0 \leq i, j < p$, but note that i would have an inverse in $\mathbb{Z}/p\mathbb{Z}$, so this means $x = y^k$ for some exponent k, contradiction. We claim that $G = XY = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. First note that $XY \subseteq G$, so it suffices to show that $XY \subseteq G$ has order p^2. Every element of this group is of the form $x^i y^j$ for some $0 \leq i, j < p$. Suppose $x^{i_1} y^{j_1} = x^{i_2} j^{i_2}$, then $x^{i_1 - i_2} = y^{j_2 - j_1}$, but we know $X \cap Y = \{e\}$, therefore we must have $i_1 = i_2$ and $j_1 = j_2$, therefore all elements of the form $x^i y^j$ are unique, therefore XY is a subgroup of G with exactly p^2 elements, therefore $G = XY$, as desired.

(d) Let G be a group of order $425 = 5^2 \times 17$. By Sylow's Third Theorem, we know G has a unique Sylow-5 subgroup (of order 25) and a unique Sylow-17 subgroup (of order 17). In particular, because they are unique, then they are normal subgroups. Hence, all Sylow subgroups are normal subgroups, therefore G is the internal product of all Sylow subgroups, hence G is the product of the Sylow-5 subgroup (of order 25) and the Sylow-17 subgroup (of order 17). But a group of order 25, by part (c), is either $\mathbb{Z}/25\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, therefore G is either isomorphic to $\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/85\mathbb{Z}$.

□

Problem 2. To find the decomposition, it suffices to find the invariant factors with respect to the matrix A. We can calculate that the characteristic polynomial of A is exactly $(5-\lambda)^2(3-\lambda)$, therefore it admits a complete factorization, and so A is diagonalizable. Since the minimal polynomial must contain all roots, therefore it is either $(5-\lambda)(3-\lambda)$ or $(5-\lambda)^2(3-\lambda)$. A quick calculation yields that A is not a root of $(5-\lambda)(3-\lambda)$, therefore the minimal polynomial is just the characteristic polynomial above. Since the two polynomials agree, we conclude that $(5-x)^2(3-x)$ is the unique invariant factor, therefore by the $\mathbb{C}[x]$-module structure, we have $\mathbb{C}^3 \cong \mathbb{C}[x]/((5-x)^2(3-x))$. □

Problem 3. (a) Note that this polynomial is reducible if and only if it has a root in $\mathbb{Z}_3$. By a quick calculation, when $x = 2$, we have $2^3 + 2 + 2 = 12 \equiv 0 \pmod 3$, therefore $x = 2$ is a root, hence we have a decomposition $(x^3 + x + 2) \equiv x^3 + 3x^2 + x - 1 = (x+1)(x^2 + 2x - 1)$ over $\mathbb{Z}_3$.

(b) A quick calculation shows that none of $x = 0, 1, 2, 3, 4$ is a root of $x^4 + x^3 + x + 3$, therefore the polynomial is irreducible if and only if we cannot obtain quadratic factors. Suppose such factorization exists, then we obtain

$$(ax^2 + bx + c)(dx^2 + ex + f) \equiv x^4 + x^3 + x + 3 \pmod 5,$$

so assuming all coefficients are between 0 and 4 (inclusive), we have

$$\begin{cases} ad \equiv 1 \pmod 5 \\ bd + ae \equiv 1 \pmod 5 \\ cd + af + be \equiv 0 \pmod 5 \\ bf + ce \equiv 1 \pmod 5 \\ cf \equiv 3 \pmod 5 \end{cases}$$

If $a \equiv 1$ and $d \equiv 1$, then

$$\begin{cases} b+e \equiv 1 \pmod 5 \\ c+f+be \equiv 0 \pmod 5 \\ bf+ce \equiv 1 \pmod 5 \\ cf \equiv 3 \pmod 5 \end{cases}$$

suppose $c \equiv 1$ and $f \equiv 3$, then we have

$$\begin{cases} b+e \equiv 1 \pmod 5 \\ be \equiv 1 \pmod 5 \\ 3b+e \equiv 1 \pmod 5 \end{cases}$$

and in particular $b \equiv 0 \pmod 5$, contradiction; supposing $c \equiv 3$ and $f \equiv 1$ gives a similar contradiction. Suppose $c \equiv 2$ and $f \equiv 4$, then

$$\begin{cases} b+e \equiv 1 \pmod 5 \\ be \equiv 4 \pmod 5 \\ 4b+2e \equiv 1 \pmod 5 \end{cases}$$

so $b \equiv 2$ and $e \equiv 4$, a contradiction, and we obtain a similar contradiction if we swap c and f. Therefore, we just have to study the case with $a \equiv 2$ and $d \equiv 3$, then

$$\begin{cases} 3b+2e \equiv 1 \pmod 5 \\ 3c+2f+be \equiv 0 \pmod 5 \\ bf+ce \equiv 1 \pmod 5 \\ cf \equiv 3 \pmod 5 \end{cases}$$

assuming $c \equiv 1$ and $f \equiv 3$, we have

$$\begin{cases} 3b+2e \equiv 1 \pmod 5 \\ be \equiv 1 \pmod 5 \\ 3b+e \equiv 1 \pmod 5 \end{cases}$$

a contradiction; assume $c \equiv 3$ and $f \equiv 1$ gives

$$\begin{cases} 3b+2e \equiv 1 \pmod 5 \\ be \equiv 4 \pmod 5 \\ b+3e \equiv 1 \pmod 5 \end{cases}$$

where $e \equiv 1$ and $b \equiv 3$, which does not work; now suppose $c \equiv 2$ and $f \equiv 4$, then

$$\begin{cases} 3b+2e \equiv 1 \pmod 5 \\ be \equiv 1 \pmod 5 \\ 4b+2e \equiv 1 \pmod 5 \end{cases}$$

which does not work; finally, we have $c \equiv 4$ and $f \equiv 2$, then

$$\begin{cases} 3b+2e \equiv 1 \pmod 5 \\ be \equiv 4 \pmod 5 \\ 2b+4e \equiv 1 \pmod 5 \end{cases}$$

then $b \equiv 3$ and $e \equiv 0$, contradiction. Therefore, this shows that there is the polynomial is irreducible over $\mathbb{Z}_5$.

(c) First note that the polynomial is primitive since the coefficients have greatest common divisor 1. By Gauss Lemma, a primitive polynomial is irreducible over $\mathbb{Z}$ if and only if it is irreducible over $\mathbb{Q}$, so it suffices to check irreducibility over $\mathbb{Z}$. By the rational root theorem, the possible roots are ± 1, which are both not roots, therefore it suffices to check it does not have quadratic factors. To see this, suppose we have

$$(x^2+ax+b)(x^2+cx+d) = x^4+x^3+x^2+6x+1,$$

then

$$\begin{cases} a+c=1 \\ ac+b+d=1 \\ bc+ad=6 \\ bd=1 \end{cases}$$

and so b, d are either 1 or -1, either way there is a contradiction. This shows irreducibility over $\mathbb{Z}$ hence over $\mathbb{Q}$.

Alternatively, taking $x = y+1$ shows that the polynomial is $y^4+5y^3+10y^2+15y+10$ with respect to y, which is irreducible over $\mathbb{Q}$ by the Eisenstein criterion over $p = 5$.

□

Problem 4. (a) Since multiplication is commutative, then G is a finite abelian group. By the fundamental theorem of finitely-generated abelian groups, we have a decomposition

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}.$$

Let $m = \operatorname{lcm}(p_1^{k_1}, \ldots, p_n^{k_n})$, so $m \leq \prod\limits_{1 \leq i \leq n} p_i^{k_i}$, and we claim that $G \cong \mathbb{Z}_m$. Note that for any $a \in \mathbb{Z}_{p_i^{k_i}}$ with any i, then $a^m = 1$ by construction. In particular, given any element a in G, we have $a^m = 1$ as well. Therefore, all elements of G are roots of the polynomial $x^m - 1$, but that would mean $\prod\limits_{1 \leq i \leq n} p_i^{k_i} \leq m$ and so $m = \prod\limits_{1 \leq i \leq n} p_i^{k_i}$. Hence, we note that all p_i's have to be distinct since this is the least common divisor, and so by the isomorphism theorem we know that G is a finite cyclic group of order m.

(b) Since K/k is an extension of degree m, then K is a group of order p^m, so it suffices to show that every element of K is a root of $x^{p^m} - x$ over k. Obviously 0 is a root, so we now work over K^*, the multiplicative group, and given any element $x \in K^*$ we know that $x^{p^m - 1} = 1$, therefore every $x \in K^*$ is a root as well. Hence, K is exactly the set of roots.

(c) Recall that an irreducible polynomial $f \in k[x]$ is separable if and only if $f' \neq 0$. Having $f' = 0$ in this case indicates that $f = \sum\limits_{i=0}^{n} a_i x^{pi}$, and but that would not be irreducible since we obtain a decomposition through freshman's dream, i.e., $f = \sum\limits_{i=0}^{n} a_i x^{pi} = \left(\sum\limits_{i=0}^{n} a_i x^i\right)^p$, contradiction. Hence, $f' \neq 0$ and therefore f is separable.

□

2 August 2021

Problems

Problem 2.1. Let G be a non-trivial finite group acting on a finite set X. We assume that for all $G \setminus \{e\}$ there exists a unique $x \in X$ such that $g \cdot x = x$.

(a) Let $Y = \{x \in X \mid G_x \neq \{e\}\}$ where G_x denotes the stabilizer of x. Show that Y is stable under the action of G.

(b) Let $y_1, y_2, \ldots, y_n$ be a set of orbit representatives of Y/G (with $|Y/G| = n$), and let $m_i = |G_{y_i}|$. Show that:

$$1 - \frac{1}{|G|} = \sum_{i=1}^{n} \left(1 - \frac{1}{m_i}\right)$$

(c) Show that X has (at least) a fixed point under the action of G.

Problem 2.2. (a) Show that $x^6 + 69x^5 - 511x + 363$ is irreducible over the integers.

(b) Show that $x^4 + 5x + 1$ is irreducible over the rationals.

(c) Show that $x^4 + x^3 + x^2 + 6x + 1$ is irreducible over the rationals.

(d) Calculate the number of distinct, irreducible polynomials over $\mathbb{Z}_5$ that have the form

$$f(x) = x^2 + ax + b, \quad \text{or} \quad g(x) = x^3 + \alpha x^2 + \beta x + \gamma, \quad a, b, \alpha, \beta, \gamma \in \mathbb{Z}_5.$$

Problem 2.3. Find possible Jordan canonical forms of an 8×8 matrix M over the field $\mathbb{F}_5$ with five elements if it is known that the characteristic polynomial of M is $(x^2 + 1)^4$ and the minimal polynomial of M is $(x^2 + 1)^2(x + 2)$.

Problem 2.4. Let F be a field, $F[x]$ be the ring of polynomials over F, and $F(x)$ be the field of fractions of (the integral domain) $F[x]$. The map $F \to F(x)$ is an injective field homomorphism, so we view F as a subfield of $F(x)$: in this way, $F \subseteq F(x)$. In what follows, provide justification.

(a) Prove that the function $\sigma : F(x) \to F(x)$ given by

$$\sigma\left(\frac{f(x)}{g(x)}\right) := \frac{f(x+1)}{g(x+1)}$$

is a well-defined automorphism of the field $F(x)$. Prove that $\sigma \in \mathrm{Gal}(F(x)/F)$.

(b) Let G be the (cyclic) subgroup of $\mathrm{Gal}(F(x)/F)$ generated by σ. What is the order of G?

(c) Let $F := \mathbb{F}_2$, the field of order 2, an $E \subseteq \mathbb{F}_2(x)$ be the intermediate field corresponding to the subgroup $G \leq \mathrm{Gal}(\mathbb{F}_2(x)/\mathbb{F}_2)$ as in (b). Prove that $[E : \mathbb{F}_2] \geq 2$.

Solutions

Problem 1. (a) To show that Y is stable under the action of G, it suffices to show that the image of the action of Y is contained in Y. Take arbitrary $g \in G$ and $y \in Y$, then we want to show that $gy \in Y$. Since this is obvious for $g = e$, it is safe to assume that $g \neq e$. Therefore, there exists $e \neq h \in G$ such that $hy = y$. We want to show that there exists $e \neq a \in G$ such that $agy = gy$. Indeed, note that $(ghg^{-1})(gy) = ghy = gy$, therefore ghg^{-1} fixes gy. It suffices to show that $ghg^{-1} \neq e$, which is obvious since $gh \neq g$, as $h \neq e$.

(b) By part (a) we know Y is stable under the action of G, therefore the action of G on X restricts to a group action of G on Y. We have

$$\begin{aligned}|G|-1&=(|Y|+|G|-1)-|Y|\\&=\left(\sum_{g\in G}|Y^g|\right)-|Y|\\&=|G|\cdot|Y/G|-|Y|\\&=n|G|-|Y|\\&=n|G|-\sum_{i=1}^{n}|\operatorname{orb}(y_i)|\\&=n|G|-\sum_{i=1}^{n}\frac{|G|}{m_i}\end{aligned}$$

by Burnside's Lemma and Orbit-Stabilizer Theorem. Therefore, we have

$$1-\frac{1}{|G|}=n-\sum_{i=1}^{n}\frac{1}{m_i}=\sum_{i=1}^{n}\left(1-\frac{1}{m_i}\right).$$

(c) It suffices to show that Y has a fixed point under the action of G. By part (b), we have $|Y|=(n-1)|G|+1$. Suppose Y does not have a fixed point, then by the class equation, we have

$$|Y|=(n-1)|G|+1=\sum_{i=1}^{n}\frac{|G|}{|G_{y_i}|}\leq\sum_{i=1}^{n}\frac{|G|}{2}=\frac{n|G|}{2},$$

therefore

$$\left(\frac{n}{2}-1\right)|G|+1\leq 0,$$

which is impossible since G is non-trivial and hence $n\geq 2$. Therefore, Y must have a fixed point and therefore so does X.

□

Problem 2. (a) To see that the polynomial has no roots, suppose it has a root, then the roots descends to another root in $\mathbb{F}_7$, where we have x^6-x^5-1, but by Fermat's Little Theorem it has no roots, contradiction. To see that it has no cubic factors, suppose there is one, then this descends to a cubic factor in any finite fields, but note that the polynomial descends to x^6+x^5+x+1 in $\mathbb{F}_2$, which factors as $(x+1)^2(x^4+x^3+x^2+x+1)$, which cannot have a cubic factor anyways. Finally, we check that the polynomial has no quadratic factors. Adding $\mathbb{F}_3$ and $\mathbb{F}_{11}$ to the mix, the constant term c of a quadratic factor of $p(x)$ must satisfy:

- $p(x)=(x+1)^2(x^4+x^3+x^2+x+1)$ over $\mathbb{F}_2$ implies $c\equiv 1\pmod 2$;
- $p(x)=x(x-1)(x^4+x^3+x^2+x+1)$ over $\mathbb{F}_3$ implies $c\equiv 0\pmod 3$;
- $p(x)=(x^2-x+4)(x^4+3x^2+3x+5)$ over $\mathbb{F}_7$ implies $c\equiv 4\pmod 7$;
- $p(x)=x(x+2)(x^4+x^3+9x^2+4x+3)$ over $\mathbb{F}_{11}$ implies $c\equiv 0\pmod{11}$.

The general solution to the above is $c\equiv 165\pmod{462}$, but there is no such c that divides 363, the constant term of $p(x)$, so no quadratic factor exists.

(b) Note that this is a primitive polynomial, so by Gauss Lemma, it suffices to show that x^4+5x+1 is irreducible over the integers. By rational root theorem, it has no integer roots, and it suffices to check it has no quadratic factors. Suppose we have

$$(x^2+ax+b)(x^2+cx+d) = x^4+5x+1,$$

then

$$\begin{cases} a+c & =0 \\ ac+b+d & =0 \\ bc+ad & =5 \\ bd & =1 \end{cases}$$

and therefore $b=d=\pm 1$, but either way we have a contradiction. Therefore, this is irreducible over the rationals indeed.

(c) Again, $x^4+x^3+x^2+6x+1$ is primitive so it suffices to show that it is irreducible over the integers. By rational root theorem, it has no roots, and we just need to check for quadratic factors. Take $(x^2+ax+b)(x^2+cx+d) = x^4+x^3+x^2+6x+1$, then

$$\begin{cases} a+c & =1 \\ ac+b+d & =1 \\ bc+ad & =6 \\ bd & =1 \end{cases}$$

therefore $b=d=\pm 1$, but either way we have a contradiction.

(d) Consider $f(x)=x^2+ax+b$, then this is irreducible if and only if it has no roots. Therefore, we can count the number of reducible polynomials instead. Note that being reducible means factoring completely in this case, so there are $5+\binom{5}{2}=15$ ways to pick such roots, therefore the number of irreducible polynomials is just $5\times 5-15=10$.

Consider $g(x)=x^3+\alpha x^2+\beta x+\gamma$, then for it to be reducible, we must obtain a root and a polynomial of degree 2. If the polynomial of degree 2 is reducible, then we obtain three roots, so this is just $5+\binom{5}{2}\times 2+\binom{5}{3}=35$ ways by picking roots; if the polynomial of degree 2 is irreducible, then we have $5\times 10=50$ ways. Therefore, there are $35+50=85$ of them in total.

□

Problem 3. Recall that the minimal polynomial is the largest invariant factor, and the characteristic polynomial is the product of all invariant factors, so the invariant factors are either $\{(x-2)^2(x+2),(x-2)^2(x+2)^3\}$ or $\{(x-2),(x-2)(x+2),(x-2)^2(x+2)^3\}$. Transforming this to Jordan blocks, we either have

$$\begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

or have

$$\begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

□

Problem 4. (a) We first show that this is a well-defined field homomorphism. Note that

- $\sigma(1) = \sigma\left(\frac{f(x)}{f(x)}\right) = \sigma\left(\frac{f(x+1)}{f(x+1)}\right) = 1$,
- $\sigma\left(\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)}\right) = \sigma\left(\frac{f_1(x)g_2(x)+f_2(x)g_1(x)}{g_1(x)g_2(x)}\right) = \frac{f_1(x+1)g_2(x+1)+f_2(x+1)g_1(x+1)}{g_1(x+1)g_2(x+1)} = \sigma\left(\frac{f_1(x)}{g_1(x)}\right)+\sigma\left(\frac{f_2(x)}{g_2(x)}\right)$, and
- $\sigma\left(\frac{f_1(x)}{g_1(x)} \cdot \frac{f_2(x)}{g_2(x)}\right) = \sigma\left(\frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}\right) = \frac{f_1(x+1)f_2(x+1)}{g_1(x+1)g_2(x+1)} = \sigma\left(\frac{f_1(x)}{g_1(x)}\right) \cdot \sigma\left(\frac{f_2(x)}{g_2(x)}\right)$.

Therefore, this is a homomorphism, and clearly this is an injection and a surjection, so this is a field isomorphism hence a field automorphism. Finally, to see that $\sigma \in \mathrm{Gal}(F(x)/F)$, it suffices to show that σ fixes F. Indeed, for any element $f \in F$, we regard it as $f(x) \equiv f$ and have $\sigma(f) = \sigma\left(\frac{f(x)}{1}\right) = \frac{f(x+1)}{1} = \frac{f}{1} = f$.

(b) The order of $G = \langle\sigma\rangle$ is exactly the characteristic of F. Indeed, given any $n \geq 0$, we have $\sigma^n\left(\frac{f(x)}{g(x)}\right) = \frac{f(x+n)}{g(x+n)}$. Because G is cyclic, the order of G is just the order of σ. For $\frac{f(x)}{g(x)} = \frac{f(x+n)}{g(x+n)}$, we must have $x = x+n$ for all x, and the order of σ is just the smallest such n, which is just the characteristic of F by definition.

(c) By part (b), we know that G is a group of order 2, therefore $G \cong \mathbb{Z}/2\mathbb{Z}$, and σ is a field automorphism of order 2. By the fundamental theorem of Galois theory, $\mathbb{F}_2(x)/E$ is a field extension of degree 2 as well. Now suppose $[E : \mathbb{F}_2] < 2$, then $E = \mathbb{F}_2$, therefore $\mathbb{F}_2(x)/\mathbb{F}_2$ is a field extension of degree 2, but this is clearly absurd, contradiction. Hence, we conclude that $[E : \mathbb{F}_2] \geq 2$.

□

3 January 2021

Problems

Problem 3.1. Let G be a group of order 2057.

(a) Show that $G \cong P \times Q$ where P is a group of order 17 and Q is a group of order 121. Determine all groups of order 2057 up to isomorphism.

(b) Show that $\operatorname{Aut}(G) \cong \operatorname{Aut}(P) \times \operatorname{Aut}(Q)$.

(c) Show that if Q is cyclic, then so is $\operatorname{Aut}(Q)$. What is the order of $\operatorname{Aut}(Q)$ in this case?

(d) If Q is not cyclic, find an isomorphic description of $\operatorname{Aut}(Q)$ and compute its order.

Problem 3.2. (a) Let R be the ring of 3×3 matrices over $\mathbb{Q}$, and S denote the ring of 2×2 matrices over $\mathbb{Q}$. Is there a surjective ring homomorphism $\varphi : R \to S$? Justify your answer.

(b) Compute $\gcd(17 + i, 24 + 2i)$ in the ring $\mathbb{Z}[i]$.

Problem 3.3. Suppose A is a 9×9 matrix over the field $\mathbb{F}_5$ with 5 elements such that the characteristic polynomial of A is $(x-1)^2(x-3)^4(x^3-1)$ and the minimal polynomial of A is $(x-1)(x-3)^3(x^3-1)$. Compute the following:

(a) The possible Jordan canonical form (or forms) of A over a suitable extension of $\mathbb{F}_5$;

(b) The possible rational canonical form (or forms) of A.

Problem 3.4. Answer the following questions and provide justification.

(a) Let K be a field. Define the ring homomorphism $\varphi : \mathbb{Z} \to K$ by $\varphi(n) = n \cdot 1$. If φ is injective and $\iota : \mathbb{Z} \to \mathbb{Q}$ is the standard inclusion, prove that there exists an injective ring homomorphism $\tilde{\varphi} : \mathbb{Q} \to K$ such that the diagram

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\varphi"] \arrow[d, "\iota"'] & K \\
\mathbb{Q} \arrow[ur, dashed, "\tilde{\varphi}"'] &
\end{tikzcd}$$

is commutative.

(b) Let $f(x) = x^4 + 4x^3 + 6x^2 + 4x \in \mathbb{Q}[x]$ and E be a splitting field of $f(x)$. Does $f(x)$ have four pairwise distinct roots in E?

(c) For E as in part (b), what is the order of the Galois group, $|\operatorname{Gal}(E/\mathbb{Q})|$?

(d) For E as in part (b), is the extension $E/\mathbb{Q}$ a Galois extension?

Solutions

Problem 1. (a) Let n_k be the number of Sylow-k groups. Since $2057 = 17 \times 121 = 17 \times 11^2$, then both P and Q are Sylow subgroups. By Sylow's Third Theorem, we have $n_{17} \mid 121$ and $n_{17} \equiv 1 \pmod{17}$, therefore $n_{17} = 1$; similarly $n_{11} \mid 17$ and $n_{11} \equiv 1 \pmod{11}$, therefore $n_{11} = 1$. Hence, all Sylow subgroups of G are unique hence normal, therefore G is the product of all its Sylow subgroups, namely $G \cong P \times Q$, as desired. Since by Sylow's First Theorem, Sylow subgroups always exist, therefore for any group G of order 2057, we know $G \cong P \times Q$ where P is a subgroup of order 17 and Q is a subgroup of order 121. In particular, $P \cong \mathbb{Z}/17\mathbb{Z}$. Because $121 = 11^2$ and a group of order p^2 is always abelian, then Q is an abelian group, then by the fundamental theorem of finitely-generated abelian groups, we have $Q \cong \mathbb{Z}/121\mathbb{Z}$ or $Q \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$. Hence, we either have $G \cong \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/121\mathbb{Z}$ or $G \cong \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.

(b) Note that $\operatorname{Aut}(P) \times \operatorname{Aut}(Q) \to \operatorname{Aut}(G)$ gives a natural monomorphism. To see that this is a surjection, for any $g \in \operatorname{Aut}(G)$, we send the projected versions $(g_P, g_Q) \mapsto g$, which is well-defined because P and Q are characteristic subgroups, so $g(P) = P$ and $g(Q) = Q$ for any automorphism g of G. Therefore, this gives an isomorphism.

(c) If Q is cyclic, then $Q \cong \mathbb{Z}/121\mathbb{Z}$, but an element of $\operatorname{Aut}(Q)$ just sends the generator of Q to some other generator, therefore the automorphism group $\operatorname{Aut}(Q) \cong Q^\times \cong (\mathbb{Z}/121\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(121)\mathbb{Z} = \mathbb{Z}/119\mathbb{Z}$. The fact that this is cyclic follows from Gauss, and has order of 119.

(d) Suppose Q is not cyclic, then $Q \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$. The automorphism of this group is just 2×2 invertible matrices with entries in $\mathbb{Z}/11\mathbb{Z}$, therefore this is just $\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z})$. We now calculate the order of this group. There are $11^2 - 1$ ways of picking the first column, where we only need to ensure not both entries are zero. To pick the second column, we want it to be linearly independent from the first column, so we cannot pick a linear multiple of the first column, therefore there are $11^2 - 11$ ways of picking, so in total there are $(11^2 - 1) \times (11^2 - 11) = 120 \times 110 = 13200$ ways of picking this.

□

Problem 2. (a) No. Since $\mathbb{Q}$ is a field, it is a simple ring and hence $M_n(\mathbb{Q})$ is also a simple ring. Moreover, any non-trivial homomorphism from a simple ring must be an isomorphism onto its image, therefore if there is a surjective ring homomorphism $\varphi : R \to S$, then $R \cong S$, which is obviously not true by considering the rank.

(b) Since the Gaussian integers give a Euclidean domain, we use Euclidean algorithm to calculate the greatest common divisor. Since $\frac{24+2i}{17+i} = \frac{410+10i}{290} = \frac{41+i}{29}$, we get $24 + 2i = (17 + i) \cdot 1 + (7 + i)$; since $\frac{17+i}{7+i} = \frac{120-10i}{50} = \frac{12-i}{5}$, then we have $17 + i = (7 + i) \cdot 2 + (3 - i)$, then finally we see that $\frac{7+i}{3-i} = 2 + i$, therefore the greatest common divisor is $3 - i$.

□

Problem 3. (a) If we want to calculate the possible Jordan canonical forms, we need the polynomial to split, hence let ζ be a primitive third root of unity, then for suitable extensions, we have characteristic polynomial $(x-1)^3(x-3)^4(x-\zeta)(x-\zeta^2)$ and minimal polynomial $(x-1)^2(x-3)^3(x-\zeta)(x-\zeta^2)$. Recall that the characteristic polynomial is the product of all invariant factors, and the minimal polynomial is the largest invariant factor, then the invariant factor has to be $\{(x-1)(x-3), (x-1)^2(x-3)^3(x-\zeta)(x-\zeta^2)\}$. Therefore, the Jordan canonical form is given by the following blocks: $J(1,1)$, $J(3,1)$, $J(1,2)$, $J(3,3)$, $J(\zeta,1)$, $J(\zeta^2,1)$, with the following Jordan canonical form:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \zeta & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \zeta^2 \end{pmatrix}$$

(b) Recall that the rational canonical form is given by the companion matrices of each invariant factor. Therefore, the rational canonical form is

$$\begin{pmatrix} 0 & -3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 27 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -54 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 36 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -37 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 55 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -36 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 10 \end{pmatrix}$$

□

Problem 4. (a) The obvious construction is to define

$$\begin{aligned} \tilde{\varphi} : \mathbb{Q} &\to K \\ \frac{n}{m} &\mapsto (n \cdot 1)(m \cdot 1)^{-1} \end{aligned}$$

for $n \in Q$ and $m \in \mathbb{Q} \setminus \{0\}$. This construction allows the diagram to commute, since for any $n \in \mathbb{Z}$, we have

$$\varphi(n) = n \cdot 1 = (n \cdot 1)(1 \cdot 1)^{-1} \tilde{\varphi}\left(\frac{n}{1}\right) = \tilde{\varphi} \circ \iota(n),$$

and to see this is an injection, note that if $\tilde{\varphi}(\frac{n}{m}) = 0$, then we must have $m \neq 0$ and $n = 0$.

(b) Observe that $f(x) + 1 = x^4 + 4x^3 + 6x^2 + 4x + 1 = (x+1)^4$, therefore the factorization is

$$f(x) = (x+1)^4 - 1 = ((x+1)^2 + 1)((x+1)^2 - 1) = (x^2 + 2x + 2)(x^2 + 2x).$$

In particular, the four roots are $\frac{-2 \pm \sqrt{-4}}{2} = -1 \pm i$, as well as 0 and -2. Therefore, f admits four distinct roots over any splitting field.

(c) Since E is a splitting field, then $E \cong \mathbb{Q}(i)$ by construction. We note that $\mathrm{Gal}(E/\mathbb{Q})$ actually has two automorphisms, namely the trivial automorphism and the conjugation automorphism sending $i \mapsto -i$. Therefore, the order of the Galois group is 2.

(d) This is a Galois extension for two different reasons: 1) since $E/\mathbb{Q}$ is a splitting field of F, then this extension is normal, and since this extension is such that f splits with no repeated roots, then this is a separable extension, so by definition $E/\mathbb{Q}$ is Galois; 2) since $E \cong \mathbb{Q}(i)$, then $E/\mathbb{Q}$ is a field extension of degree 2, and since $\operatorname{Gal}(E/\mathbb{Q})$ has order 2, then by definition $E/\mathbb{Q}$ is Galois.

$\square$

4 August 2020

Problems

Problem 4.1. (a) A finite group G is called *cool* if G has precisely four Sylow subgroups (over all primes p). The order $|G|$ of a cool group is called a *cool* number. For example, S_3 is a cool group and 6 is a cool number. Describe the set of all cool numbers. Hint: Use prime factorization in your description.

(b) For each cool number n that you found in part (a), determine whether every cool group of order n is nilpotent.

(c) For each cool number n that you found in part (a), determine whether every cool group of order n is solvable.

Problem 4.2. Suppose a finite group G acts on a set A so that for every non-trivial $g \in G$ there exists a unique fixed point (i.e., there is exactly one $a \in A$, depending on g, such that $g(a) = a$). Prove that this fixed point is the same for all $g \in G$.

Problem 4.3. (a) Compute, if possible, $\gcd(2+8i, 17-17i)$ in the ring $\mathbb{Z}[i]$ of Gaussian integers.

(b) Determine whether the following polynomials are reducible or irreducible in given rings:

- $x^4 + x^2 + 1$ in $\mathbb{Z}_2[x]$, where $\mathbb{Z}_2$ is the field of two elements;
- $x^4 + 5x^3 + 10x^2 + 15x + 5$ in $R[x]$, where $R = \mathbb{Z}[i]$;
- $2x^4 + 4x^3 + 8x^2 + 12x + 20$ in $\mathbb{Z}[x]$.

Problem 4.4. (a) Let A be an $n \times n$ complex matrix and let f and g be the characteristic and minimal polynomials of A, respectively. Suppose that $f(x) = g(x)(x-i)$ and $g(x)^2 = f(x)(x^2+1)$. Determine all possible Jordan canonical forms of A.

(b) Let $\mathbb{F}$ be a field of characteristic $p > 0$ and $p \neq 3$. If α is a root of the polynomial $f(x) = x^p - x + 3$, in an extension of the field $\mathbb{F}$, show that $f(x)$ has p distinct roots in the field $\mathbb{F}(\alpha)$.

Problem 4.5. (a) Compute a factorization for $x^{26} - 1$ into irreducible polynomials over $\mathbb{Z}$.

(b) Find the number of all subfields of the splitting field K of $x^{26} - 1$ over $\mathbb{Q}$ and prove that all of them are Galois over $\mathbb{Q}$.

Solutions

Problem 1. (a) Let $a = |G| > 1$ be the cool number, and consider the prime factorization $a = p_1^{n_1} \cdots p_m^{n_m}$. Since G has exactly four Sylow subgroups, and by Sylow First Theorem we know every prime factor admits a Sylow subgroup, then $1 \leq m \leq 4$.

If $m = 1$, then $a = p^n$, therefore we have the unique Sylow subgroup which is G itself, so there cannot be a cool group; if $m = 3$, then exactly one the the primes p_i has two Sylow subgroups, but this is impossible since by Sylow Third theorem we know $n_{p_i} \equiv 1 \pmod{p_i}$. Therefore, we either have $m = 2$ or $m = 4$. If $m = 2$, then with the same reasoning we know (without loss of generality) that p_1 has 1 Sylow subgroup and p_2 has 3 Sylow subgroups, but now $n_{p_2} \equiv 1 \pmod{p_2}$, therefore $p_2 = 2$. Moreover, we know $n_2 = 3 \mid p_1^{n_1}$, therefore $p_1 = 3$ by force. In particular, in this case G is a group of order $2^{n_1}3^{n_2}$. Finally, if $m = 4$, we know that every prime p_i admits a unique Sylow subgroup, therefore all of them are normal and hence G is the product of all four Sylow subgroups.

Collecting the properties above, we know that the cool number is either of the form $2^{n_1}3^{n_2}$ where there are 1 Sylow-3 subgroup and 3 Sylow-2 subgroups, or of the form $p_1^{n_1}p_2^{n_2}p_3^{n_3}p_4^{n_4}$.

(b) Recall that a finite group is nilpotent if and only if it is the direct product of its Sylow subgroups. Therefore, this is obviously the case for groups of order $p_1^{n_1}p_2^{n_2}p_3^{n_3}p_4^{n_4}$, since it is the direct product of Sylow-p groups, as mentioned above. For groups of order $2^{n_1}3^{n_2}$, if it is nilpotent, then all Sylow subgroups are normal, contradiction.

(c) Since nilpotent groups are solvable, then groups of order $p_1^{n_1}p_2^{n_2}p_3^{n_3}p_4^{n_4}$ are solvable. For groups of order $2^{n_1}3^{n_2}$, take the Sylow-3 subgroup N, then note that $N \lhd G$ by uniqueness. Moreover, N and G/N are 3-group and 2-subgroups respectively, therefore both are solvable, therefore G is solvable. (Alternatively, this is true by Burnside's Theorem.) Therefore, all cool groups are solvable.

□

Problem 2. See August 2021, Problem 1 (Problem 2.1). □

Problem 3. (a) We proceed by the Euclidean algorithm on Gaussian integers. We first have $\frac{17-17i}{2+8i} = \frac{(17-17i)(2-8i)}{68} = \frac{-3-5i}{2}$, therefore we have $17-17i = (2+8i)(-1-2i)+(3-5i)$. We then have $\frac{2+8i}{3-5i} = \frac{-34+34i}{34} = -1+i$, therefore $\gcd(2+8i, 17-17i) = 3-5i$.

(b)
- Obviously the polynomial has no roots over $\mathbb{Z}_2$, and therefore we just have to check if it factors as quadratics. Suppose we have $(x^2+ax+b)(x^2+cx+d) = x^4+x^2+1$, then
$$\begin{cases} a+c \equiv 0 \pmod 2 \\ ac+b+d \equiv 1 \pmod 2 \\ bc+ad \equiv 0 \pmod 2 \\ bd \equiv 1 \pmod 2 \end{cases}$$
therefore $b, d \equiv 1 \pmod 2$, so $ac \equiv 1 \pmod 2$, therefore $a, c \equiv 1 \pmod 2$, hence we have
$$(x^2+x+1)^2 \equiv x^4+x^2+1 \pmod 2,$$
which means it is reducible.
- First note that this is irreducible over $\mathbb{Q}$ by Eisenstein's criterion over prime $p = 5$, which then implies irreducibliy over $\mathbb{Z}$ since this is primitive. However, 5 is not a prime over $\mathbb{Z}[i]$ since $5 = (2+i)(2-i)$, but now $2+i$ is a prime over $\mathbb{Z}[i]$, and we can Eisenstein's criterion over $p = 2+i$. We just need to check that $(2+i)^2 = 3+4i \nmid 5$, which is easy. Therefore, by Eisenstein's criterion, this is irreducible over $\mathbb{Q}[i]$, but $\mathbb{Z}[i]$ is the UFD with quotient field $\mathbb{Q}[i]$, therefore being primitive implies irreduciblity over $\mathbb{Z}[i]$.
- Note that $2 \in \mathbb{Z}$ is not a unit and is therefore irreducible. Therefore, 2 carries over and is irreducible over $\mathbb{Z}[x]$. Therefore, the polynomial is obviously reducible since it has a factor of 2.

□

Problem 4. (a) Since $f(x) = g(x)(x-i)$ where $g(x)$ is the minimal polynomial, and recall that the characteristic polynomial is the product of all invariant factors and the minimal polynomial is the largest invariant factor, therefore the invariant factors are just $\{(x-i), g(x)\}$. Now we note that $f(x)^2 = g(x)^2(x-i)^2 = f(x)(x+i)(x-i)^3$, so $f(x) = (x+i)(x-i)^3$, hence $g(x) = (x+i)(x-i)^2$. We conclude that the invariant factors are $\{(x-i), (x+i)(x-i)^2\}$. The corresponding Jordan canonical form is just
$$\begin{pmatrix} i & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & i & 1 \\ 0 & 0 & 0 & i \end{pmatrix}$$

(b) First note that $f'(x) = -1$, so $\gcd(f, f') = 1$. In particular, f is separable and therefore should give no repeated roots. Therefore, it suffices to show that f splits in $\mathbb{F}(\alpha)$, where $\alpha \in \mathbb{K}$ is a root of f in some field extension $\mathbb{K}/\mathbb{F}$. We claim that the roots of f are exactly $\alpha, \alpha - 1, \ldots, \alpha - p + 1$, which are all elements in $\mathbb{K}$ by construction. Indeed, if $\alpha - k$ is a root of f, then $(\alpha - k)^p - (\alpha - k) + 3 = 0$, now by Freshman's Dream

$$\begin{aligned}(\alpha - k - 1)^p - (\alpha - k - 1) + 3 &= (\alpha - k)^p + (-1)^p - (\alpha - k) + 4 \\ &= (-1)^p + 1 \\ &= 0\end{aligned}$$

for all p: the last line is obviously true for odd p, and for even $p = 2$, we have $(-1)^p + 1 = 2 = 0$.

□

Problem 5. (a) Note that the roots of $x^{26} - 1$ are exactly the complex numbers on the unit circle that divide the circle by 26 portions. Recall that $x^n - 1 = \prod_{d|n} \Phi_d(x)$, where Φ_d is the dth cyclotomic polynomial. Therefore, $x^{26} - 1$ can be factored into the product of four irreducible polynomials, namely Φ_1, Φ_2, Φ_{13} and Φ_{26}. It is obvious that we have

$$x^{26} - 1 = (x^{13} - 1)(x^{13} + 1) = (x - 1)(x^{12} + \cdots + x + 1)(x + 1)(x^{12} - x^{11} + \cdots + x^2 - x + 1).$$

(In particular, for prime n, we know $\Phi_n = x^{n-1} + \cdots + x + 1$.) By the above fact, we know this is a factorization of irreducible polynomials, as desired.

(b) It is obvious that the splitting field is $K = \mathbb{Q}(\zeta_{26})/\mathbb{Q}$, where ζ_{26} is a primitive 26th root of unity, therefore this is obviously Galois and has a Galois group given by $(\mathbb{Z}/26\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(26)\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$. (This group of unit is cyclic by a theorem of Gauss, whenever $\mathbb{Z}/n\mathbb{Z}$ has $n = 2, 4, p^n, 2p^n$ for prime p.) By the fundamental theorem of Galois theory, the subfields of the Galois extension are in one-to-one correspondence with the subgroups of the Galois group. Because the subgroups of cyclic group are cyclic, then the subgroups are the trivial subgroup, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$. Hence, the number of subfields of the splitting field is 6.

Because the subextension of Galois extension is always separable, it suffices to show that all these extensions are normal, but that corresponds to the fact that these subgroups are all normal, which is obvious because $\mathbb{Z}/12\mathbb{Z}$ is abelian.

□

5 January 2020

Problems

Problem 5.1. Let G be a finite group of order 100.

(a) Show that G is solvable. (You can use the fact that groups of order p^2 are abelian for p a prime number.)

(b) Show, by giving a counterexample, that G need not be nilpotent.

Problem 5.2. Decide which of the following sets are ideals of the ring $\mathbb{Z}[x]$. Provide justification.

(a) The set of all polynomials whose coefficient of x^2 is a multiple of 3.

(b) $\mathbb{Z}[x^2]$, the set of all polynomials in which only even powers of x appear.

(c) The set of polynomials whose coefficients sum to zero.

Problem 5.3. Find the possible Jordan canonical forms of 7×7 matrices M with entries in $\mathbb{C}$ satisfying the following criteria:

- the characteristic polynomial of M is $(z-3)^4(z-5)^3$,
- the minimal polynomial of M is $(z-3)^2(z-5)^2$, and
- the $\mathbb{C}$-vector space dimension of the nullspace of $3 \cdot \mathrm{id} - M$ is 2.

Problem 5.4. Determine if the following polynomials are irreducible over $\mathbb{Z}$.

(a) $x^3 - 5x - 1$,

(b) $x^4 + 10x^2 + 5$.

Problem 5.5. (a) Describe the subgroups of S_4 that can occur as Galois group of an irreducible quartic polynomial.

(b) Determine the Galois group of the irreducible polynomial $x^4 + 2x^2 + 4$. (You can use the fact that a quartic polynomial $f(x) = x^4 + qx^2 + rx + s$ has resolvent cubic $g(x) = x^3 - 2qx^2 + (q^2 - 4s)x + r^2$.)

Solutions

Problem 1. (a) By Sylow Theorem, the number n_5 of Sylow-5 subgroup of G satisfies $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 4$, therefore $n_5 = 1$, so Sylow-5 subgroup N is unique and hence normal. In particular, G/N is a group of order 4, which is a p-group and therefore solvable. Moreover, N is also a p-group and therefore solvable, so G is solvable since both N and G/N are solvable.

Alternatively, using the hint, we know N is normal in G, and that G/N is a group of order p^2 for $p = 5$ therefore abelian. Moreover, $\{e\}$ is normal in N and $N/\{e\} \cong N$ is a group of order p^2 for $p = 5$, therefore this is an abelian group as well. We therefore obtain a sequence $\{e\} \subset N \subset G$, hence G is solvable.

Alternatively, this is true by Burnside's Theorem.

Alternatively, group of order p^2q^2 is solvable.

(b) Pick $G = \mathbb{Z}_{10} \times D_5$. Suppose this is nilpotent, then every Sylow subgroup is normal. In particular, every p admits a unique Sylow-p group, and thus the group is a product of its Sylow subgroups. But obviously G has multiple Sylow-2 subgroup, namely given by the rotation operator in D_5 and any two elements of order 10 in $\mathbb{Z}_{10}$.

□

Problem 2. (a) No. $x+1$ has coefficient of x^2 to be $3 \mid 0$, but $(x+1)^2 = x^2+2x+1$ has $3 \nmid 1$.

(b) No. $x^2 \cdot x = x^3 \notin \mathbb{Z}[x^2]$.

(c) Yes. A polynomial with coefficients sum to 0 is exactly a polynomial with a root $x = 1$. This is obviously an abelian group with respect to addition. Given any polynomial in $\mathbb{Z}[x]$, and any polynomial with a root $x = 1$, the product must also have root $x = 1$, therefore this is an ideal.

□

Problem 3. The first two restraints show that the invariant factors are either $\{(z-3)^2(z-5), (z-3)^2(z-5)^2\}$ or $\{z-3, (z-3)(z-5), (z-3)^2(z-5)^2\}$. Because the $\mathbb{C}$-vector space dimension of the nullspace of $3 \cdot \mathrm{id} - M$ is 2, so there are 2 Jordan blocks with eigenvalue 3. In particular, this means the invariant factors are $\{(z-3)^2(z-5), (z-3)^2(z-5)^2\}$, hence the corresponding Jordan canonical form is

$$\begin{pmatrix} 5 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{pmatrix}$$

□

Problem 4. (a) Since this is of degree 3, then it suffices to see whether it has a root. By the rational root theorem, any rational root should be in $\{\pm 1\}$, which are both not roots. Hence, this polynomial does not have a root in $\mathbb{Z}$, therefore the polynomial is irreducible.

(b) By Eisenstein criterion over $p = 5$, this polynomial is irreducible over $\mathbb{Q}$, but since this polynomial is also primitive, then irreducible over $\mathbb{Q}$ implies irreducible over $\mathbb{Z}$.

□

Problem 5. (a) Note that S_4 is the permutation of four objects, therefore the Galois group of an irreducible quartic polynomial embeds into S_4. In particular, since the polynomial is quartic, then the corresponding Galois group is transitive, i.e., given any $i \neq j \in \{1,2,3,4\}$ there exists a permutation that sends i to j. By orbit-stabilizer theorem, the order of the group is divisible by the orbit, i.e., the number of elements permuted which is 4 in this case, so the group order is divisible by 4. We now consider the index $[G : G \cap V]$ to classify all transitive subgroups of this form, where $V = V_4$ is the Klein-4 group. Recall that $S_4/V \cong S_3$ has order 6, and by the second isomorphism theorem we know $G/G \cap V \cong GV/V \subseteq S_4/V \cong S_3$ is a subgroup of S_3, therefore $[G : G \cap V] \mid 6$.

If $[G : G \cap V] = 6$, then since V has order 4 itself, this forces $G \cong S_4$; if $[G : G \cap V] = 1$, then $G = G \cap V$, so $G = V = V_4$; if $[G : G \cap V] = 3$, then $|G|$ is divisible be 3, but $|G|$ is also divisible by 4, and then we conclude that $|G| = 12$, therefore $G = A_4$ is the only choice. Finally, we consider the case when $[G : G \cap V] = 2$, then G has either order 4 or order 8.

- If G has order 8, then $G \cap V = V = V_4$ has order 4. In particular, $G/(G \cap V)$ is a group of order 2, so let $g \in G \setminus V$, then $g^2 \in G \cap V$, in particular $g^2 \in V$. But recall that $V \cong \{(\,), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, therefore for $g^2 \in V$ but $g \notin V$, therefore g must be a 4-cycle, say $g = (1\,2\,3\,4)$. In particular, all such subgroups containing g must be transitive. For $a = (1\ 2)(3\ 4) \in V$, we have $aga^{-1} = (2\ 3\ 4\ 1) = g^{-1}$, and since a has order 2 and g has order 4, this shows that $G \cong D_4$.
- If G has order 4, then $G \cap V \cong \mathbb{Z}/2\mathbb{Z}$, and without loss of generality say this is given by $(1\,2)(3\,4)$. Therefore, for $g \in G \setminus V$, we have $g^2 \in V$ again, therefore g is still a 4-cycle. In particular, $g^2 \neq e$, so $G \cong \langle g \rangle$ is generated by the 4-cycle, hence this gives $\mathbb{Z}/4\mathbb{Z}$.

Therefore, G is one of the following: $\mathbb{Z}_4$, D_4, V_4, A_4, S_4.

(b) Let use say we are working over $\mathbb{Q}$. Let f be the polynomial above with four roots x_1, x_2, x_3, x_4. Now define $\alpha = x_1x_2 + x_3x_4$, $\beta = x_1x_3 + x_2x_4$, and $\gamma = x_1x_4 + x_2x_3$, then $g(x) = (x - \alpha)(x - \beta)(x - \gamma)$ is the resolvent of f. Let $K = \mathbb{Q}(\alpha, \beta, \gamma)$, then K is the splitting field of g over $\mathbb{Q}$. Let G be the Galois group of f over $\mathbb{Q}$, then we know G embeds into S_4, and since f is irreducible, then G is transitive, hence it is one of the five groups above in part (a). Let $L/\mathbb{Q}$ be the field extension corresponding to the Galois group G. Since K is an intermediate field extension of $L/\mathbb{Q}$, by the definition of K above, we note that the Klein group $V = V_4$ gives $G \cap V$ to be the Galois group corresponding to K. Therefore, $G/(G \cap V)$ corresponds the field extension $K/\mathbb{Q}$ and the resolvant cubic g above by the fundamental theorem of Galois theory. By the hint, we know that $g(x) = x^3 - 4x^2 - 12x = x(x^2 - 4x - 12) = x(x - 6)(x + 2)$, therefore g splits in $\mathbb{Q}$, therefore K as the splitting field of g must be $\mathbb{Q}$ itself. Hence, the fundamental theorem of Galois theory tells us that $G = G \cap V$, and this corresponds to the case $[G : G \cap V] = 1$ above, which is $G = V = V_4$.

□

6 August 2019

Problems

Problem 6.1. Let p, q be two prime integers. Prove that a group of order p^2q is not simple.

Problem 6.2. Consider the symmetric group S_n with $n \geq 5$.

(a) Show that any 3-cycle is a commutator.

(b) Let H be a subgroup of S_n and let H_1 be a normal subgroup of H such that H/H_1 is abelian. If H contains all 3-cycles then show that H_1 contains all 3-cycles.

(c) Deduce that S_n is not solvable.

Problem 6.3. Let V be a finite-dimensional real vector space and $\varphi : V \to V$ a linear transformation with invariant factors $q_1 = x^4 - 4x^3 + 5x^2 - 4x + 4 = (x-2)^2(x^2+1)$ and $q_2 = x^7 + 6x^6 + 14x^5 - 20x^4 + 25x^3 - 22x^2 + 12x - 8 = (x-2)^3(x^2+1)^2$ in $\mathbb{R}[x]$.

(a) Find the rational canonical form of φ with respect to some basis.

(b) Suppose V is a complex vector space and $\psi : V \to V$ is a linear transformation with same invariant factors as above.

(i) Find the elementary divisors of ψ in $\mathbb{C}[x]$.

(ii) Find the Jordan canonical form of ψ with respect to some basis.

Problem 6.4. Consider the polynomial $f(x) = x^4 - 2$ on $\mathbb{Q}[x]$.

(a) Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(b) Let L denote the splitting field of $f(x)$ and let G denote its Galois group over $\mathbb{Q}$. Determine L and G. Also find a relation between the generators of G.

Problem 6.5. Let $p > 2$ be a prime integer.

(a) Show that for any integer n, $n^p \equiv n \pmod{p}$.

(b) Let k be a field of characteristic p and let $f(x) = x^p - x - a \in k[x]$, $a \in k$. Show that

(i) if $f(x)$ has a root in k, then $f(x)$ has all its roots in k;

(ii) if $f(x)$ does not have any root in k, then $f(x)$ is irreducible in $k[x]$;

(iii) in case (ii) above, the Galois group of $f(x)$ is cyclic of order p.

Solutions

Problem 1. By Sylow Theorems, the number of Sylow subgroups satisfy $n_p \equiv 1 \pmod{p}$, $n_p \mid q$, and $n_q \equiv 1 \pmod{q}$, and $n_q \mid p^2$. Since q is prime, then $n_p \in \{1, q\}$. If $p > q$, then $n_p = 1$, which means there exists a unique Sylow p-subgroup, hence it is normal. If $p = q$, then the group is of order p^3, then by Sylow Theorem we know there exists a normal subgroup of order p^2. If $p < q$, then since $n_q \mid p^2$, we have $n_q \in \{1, p, p^2\}$, and suppose $n_q \neq 1$, then $n_q = p$ or p^2. If $n_q = p$, since $p < q$, we have $p \equiv 1 \pmod{q}$ which is a contradiction. Therefore, $n_q = p^2$. In particular, there are $p^2(q-1) = p^2q - p^2$ elements of order q, and this forces there to be exactly one Sylow p-group. Therefore, the group either has a unique Sylow p-group or a unique Sylow q-group. □

Problem 2. (a) Let $(a\,b\,c)$ be a 3-cycle in S_n. We have $(a\,b\,c) = (a\,b)(a\,c)(a\,b)(a\,c) = [(a\,b),(a\,c)]$ to be a commutator.

(b) Note that H/H_1 is abelian if and only if $[H,H] \subseteq H_1$. Recall that A_n is generated by 3-cycles for $n \geq 5$, so if H contains all 3-cycles, then H is either A_n or S_n. If $H = S_n$, then $[H,H] = A_n$, hence H_1 is either A_n or S_n, and either way it contains all 3-cycles. (Note that the only non-trivial normal subgroup of S_n for $n \geq 5$ is A_n.) If $H = A_n$, then we know A_n is non-abelian and simple for $n \geq 5$, therefore the commutator is non-trivial, but the commutator of H is a normal subgroup of H, so $H = [H,H] = H_1$, H_1 contains all 3-cycles as well.

(c) Suppose S_n is solvable for $n \geq 5$, then $A_n \lhd S_n$ is also solvable, but any non-abelian simple group is not solvable, contradiction.

□

Problem 3. (a) With the canonical basis, this is just

$$\begin{pmatrix}
0 & 0 & 0 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & -5 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -12\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 22\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -25\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 20\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -14\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -6
\end{pmatrix}$$

(b) (i) Under $\mathbb{C}$, we have invariant factors as $q_1 = (x-2)^2(x+i)(x-i)$ and $q_2 = (x-2)^3(x+i)^2(x-i)^2$. Therefore, the elementary divisors are $\{(x-2)^3, (x-2)^2, (x+i)^2, (x+i), (x-i)^2, (x-i)\}$.

(ii) By the invariant factors above, we know the Jordan normal form is given by

$$\begin{pmatrix}
2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & i & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & i & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & i & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -i & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -i & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -i
\end{pmatrix}$$

□

Problem 4. (a) This is obvious by Eisenstein Criterion on $p = 2$.

(b) Note that the four roots are distinct, i.e., $\{\pm 2^{\frac{1}{4}}, \pm 2^{\frac{1}{4}} i\} = i^n 2^{\frac{1}{4}}$, so f is separable. Hence, $L/\mathbb{Q}$ is Galois. We claim that $L = \mathbb{Q}(2^{\frac{1}{4}}, i)$. Indeed, all four roots are contained in $\mathbb{Q}(2^{\frac{1}{4}}, i)$, and both $2^{\frac{1}{4}}$ and i can be generated from the four roots via $\mathbb{Q}$. Now, we have the following diagram:

$$\begin{tikzcd}
 & \mathbb{Q}(2^{\frac{1}{4}}, i) \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{Q}(2^{\frac{1}{4}}) \arrow[dr, no head] & & \mathbb{Q}(i) \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Therefore, $\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}$ is a field extension of degree 4 by looking at the obvious basis. Hence $L/\mathbb{Q}$ is a field extension of degree 8 since $L/\mathbb{Q}(2^{\frac{1}{4}})$ has degree at most 2, and $i \notin \mathbb{Q}(2^{\frac{1}{4}})$. We now know that G is a group of order 8, embedded in S_4, so it is a Sylow 2-subgroup. The obvious way to do this is to note that by Sylow theorems there is a unique such Sylow 2-subgroup, namely D_8. To give an explicit description, if φ sends $2^{\frac{1}{4}} \mapsto 2^{\frac{1}{4}} i$ and $i \mapsto i$, and ψ sends $2^{\frac{1}{4}} \mapsto 2^{\frac{1}{4}}$ and $i \mapsto -i$, note that φ is of order 4 and ψ is of order 2, and note that they generate the entire Galois group G. To determine the relation, we have $\psi\varphi\psi^{-1} = \varphi^{-1} = \varphi^3$, therefore this gives a description of the dihedral group:

$$\left\langle \varphi, \psi \mid \varphi^4 = \psi^2 = e, \psi\varphi\psi^{-1} = \varphi^{-1} \right\rangle.$$

□

Problem 5. (a) We proceed by induction on integer n. Fix prime p. Note that $0^p \equiv 0 \nmid p$. Therefore, the base case is true. We will prove the inductive step for $n > 0$, and the case where $n < 0$ follows in a similar manner. Suppose we have proven this for $n \geq 0$, then $n^p \equiv n \pmod{p}$, then $(n+1)^p \equiv n^p + 1 \equiv n + 1 \pmod{p}$ by the inductive step and binomial theorem. Therefore, this proves the inductive step and that the statement holds for any $n > 0$. Similarly the statement holds for any $n < 0$, therefore this is true for all $n \in \mathbb{Z}$.

(b) (i) This is similar to August 2020, Problem 4 (Problem 4.4) part (b). Suppose g is a root of $f(x)$ in k, then we claim that the roots of f are exactly $g, g-1, g-2, \dots, g-p+1$. Indeed, for any $y \in \{0, \dots, p-1\}$, because k has characteristic p, we have

$$\begin{aligned}
f(g-y) &= (g-y)^p - (g-y) - a \\
&= g^p + (-y)^p - g + y - a \\
&= (g^p - g - a) + (-y)^p + y \\
&= 0 + (-1)^p \cdot y + y \\
&= 0
\end{aligned}$$

for any p and any y. Therefore, this gives the p distinct roots of f.

(ii) Note that $f'(x) = px^{p-1} - 1 = -1$, so $\gcd(f, f') = -1$ whenever f does not have a root, which means f is separable. Since f does not have a root in k, then $a \neq 0$. Let g be some root of f over some extension of k, then from part (a), we know that all roots are of the form above, therefore $k(g)$ should be the splitting field of f. If we admit a factorization like $f = f_1 f_2$, then the sum of roots of f_1 should be of the form $ng + r$ where $n = \deg(f_1)$ and $r \in k$. Therefore, $f_1 \in k[x]$, but by Vieta's Theorem we know $ng + r \in k$, therefore $g \in k$, contradiction.

(iii) Suppose we have the case as in (ii), and let g be any root of f, then $k(g)$ is the splitting field of f according to part (i). Note that $f'(x) = px^{p-1} - 1 = -1$, so $\gcd(f, f') = -1$ whenever f does not have a root, which means f is separable. In particular, the extension is separable and normal, therefore Galois. Moreover, we can show that f is irreducible. To see this, note that the Frobenius map $x \mapsto x^p$ sends the root g to $g - a$, and since $a \neq 0$, this automorphism generates the Galois group, i.e., any automorphism sending g to any $g - y$ can be given by this Frobenius map. Therefore, the Galois group acts transitively on the roots, therefore by the Galois correspondence we know that f is irreducible.

Hence, f becomes the minimal polynomial of g, then the size of the Galois group is just the size of the field extension (by Galois property), which is just the degree of g. Hence, the Galois group of f is a group of order p, which is a prime so must be the cyclic group of order p.

□

7 May 2019

Problems

Problem 7.1. (a) Let p be the smallest prime dividing the order of a finite group G. If H is a subgroup of G of index p, prove that H is normal in G.

(b) Show that any group of order 77 is cyclic.

Problem 7.2. Let q be a prime power and let $\mathbb{F}_q$ be a finite field with q elements. Let $\mathrm{GL}_2(\mathbb{F}_p)$ be the (finite) group of invertible 2×2 matrices with coefficients in $\mathbb{F}_p$.

(a) Show that there is a group homomorphism $\mathrm{GL}_2(\mathbb{F}_q) \to S_{q+1}$ with kernel equal to the subgroup of scalar matrices $Z = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid 0 \neq a \in \mathbb{F}_q \right\}$. (Hint: construct an action of $\mathrm{GL}_2(\mathbb{F}_q)$ on the set of one-dimensional subspaces of $\mathbb{F}_q^2$.)

(b) Use part (a) to prove that $\mathrm{GL}_2(\mathbb{F}_3)$ is solvable and that $\mathrm{GL}_2(\mathbb{F}_4)$ is not solvable. You may use without proof that $\mathrm{GL}_2(\mathbb{F}_q)$ has cardinality $(q^2-1)(q^2-q)$.

Problem 7.3. Let M be the quotient abelian group $\mathbb{Z}^4/A$, where A is the subgroup of $\mathbb{Z}^4$ generated by the elements $(1,1,1,1)$, $(0,1,1,0)$, and $(1,2,-1,0)$.

(a) Determine the structure of M.

(b) How many non-trivial homomorphisms $M \to \mathbb{Z}/5\mathbb{Z}$ are there?

Problem 7.4. Let k be a field, and consider the element $D = \det \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ in the polynomial ring $k[x,y,z,w]$.

(a) Show that D is irreducible.

(b) Show that $k[x,y,z,w]/D$ is not a UFD.

Problem 7.5. Let K be the splitting field of x^6+3 over $\mathbb{Q}$.

(a) Compute the Galois group of K over $\mathbb{Q}$.

(b) How many subfields of K are there, which have degree 3 over $\mathbb{Q}$?

Solutions

Problem 1. (a) Note that G acts on G/H by left translation, i.e., given $g \in G$ and $xH \in G/H$, we map $(g,x) \mapsto gxH$. This induces a group homomorphism $\varphi : G \to \Sigma(G/H) = S_p$ such that for any $g \in G$, it is mapped to $xH \mapsto gxH$. We claim that $H = \ker(\varphi) \lhd G$, then H has to be a normal subgroup. Let $g \in \ker(\varphi)$, then the mapping $xH \mapsto gxH$ is the identity mapping. In particular, if $x \in H$, then this forces $g \in H$. Therefore, $\ker(\varphi) \subseteq H$. Now consider $\operatorname{im}(\varphi) \subseteq S_p$, then $|\operatorname{im}(\varphi)| \mid p!$. However, $\operatorname{im}(\varphi) \cong G/\ker(\varphi)$, therefore $|\operatorname{im}(\varphi)| \mid |G|$, so $|\operatorname{im}(\varphi)|$ is either 1 or p. Therefore, $[G : \ker(\varphi)] \leq p$, and since $\ker(\varphi) \subseteq H$ and $[G : H] = p$, so this forces $[G : \ker(\varphi)] = p$, hence $H = \ker(\varphi)$.

(b) We will prove that a group of order pq with $p > q$ and $p \not\equiv 1 \pmod{q}$ is cyclic. Let P_p and P_q be a Sylow p-subgroup and a Sylow q-subgroup, respectively. We have $[G : P_p] = q$, which is the smallest prime dividing $|G|$, therefore $P_p \lhd G$ by part (a). Let $H = N_G(P_q)$, so $P_q \lhd H \subseteq G$. Now $|H|$ is either q or pq, so $[G : H]$ is either p or 1. By Sylow Theorem, $n_q \equiv 1 \pmod{q}$ and $n_q \mid p$, so n_q is either 1 or p, but $p \not\equiv 1 \pmod{q}$, therefore $n_q = 1$. In particular, P_q is the unique Sylow q-subgroup and therefore $P_q \lhd G$. Therefore, the only Sylow subgroups of G are P_p and P_q, therefore $G \cong P_p \times P_q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$ since $\gcd(p, q) = 1$.

□

Problem 2. (a) In $\mathbb{F}_q^2$ there are q^2-1 non-zero elements, and since every one-dimensional subspace is determined by $q-1$ elements, the set of one-dimensional subspaces of $\mathbb{F}_q^2$ has $\frac{q^2-1}{q-1} = q+1$ elements. Consider the left translation action of $\mathrm{GL}_2(\mathbb{F}_q)$ on this set of one-dimensional subspace, then this extends to a group homomorphism $\mathrm{GL}_2(\mathbb{F}_q) \to S_{q+1}$, where the kernel is the set Z above since the target falls in the same equivalence class.

(b) First consider $\mathrm{GL}_2(\mathbb{F}_3)$. Note that $|\mathrm{GL}_2(\mathbb{F}_3)| = 48$, $|Z| = 2$, therefore the image of the group homomorphism $\mathrm{GL}_2(\mathbb{F}_3) \to S_4$ has 24 elements, hence this is a surjection. Note that $Z \lhd \mathrm{GL}_2(\mathbb{F}_3)$ is solvable as a 2-group, and $S_4 \cong \mathrm{GL}_2(\mathbb{F}_3)/Z$ is solvable, therefore $\mathrm{GL}_2(\mathbb{F}_3)$ is solvable.

Now consider $\mathrm{GL}_2(\mathbb{F}_4)$. We have $|\mathrm{GL}_2(\mathbb{F}_4)| = 180$, $|Z| = 3$, therefore the image of the group homomorphism $\mathrm{GL}_2(\mathbb{F}_4) \to S_5$ has 60 elements, but the only such subgroup of S_5 is A_5, so the image is just A_5. Now $Z \lhd \mathrm{GL}_2(\mathbb{F}_4)$, and $A_5 \cong \mathrm{GL}_2(\mathbb{F}_4)/Z$ is not solvable, therefore $\mathrm{GL}_2(\mathbb{F}_4)$ is not solvable.

□

Problem 3. (a) By the elementary row operations, A is essentially generated by row vectors $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, and $(0, 0, 1, 0)$. Therefore, $M \cong \mathbb{Z}^4/A \cong \mathbb{Z}^4/\mathbb{Z}^3 \cong \mathbb{Z}$.

(b) The set of group homomorphisms $\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ is given by $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/5\mathbb{Z})$ as $\mathbb{Z}$-module homomorphisms, but this is just isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Moreover, exactly one of them is the trivial homomorphism, so there are four non-trivial group homomorphisms.

□

Problem 4. (a) Note that $D = xw-yz$ is linear in w, so if it is reducible, we have $xw-yz = c \cdot q(w)$ for $\deg(q(w)) = 1$ and $c \in k[x, y, z]$. Therefore, c divides x and yz, so c is a unit in $k[x, y, z]$, therefore c is a unit in $k[x, y, z, w]$, hence $xw - yz$ is irreducible.

(b) Note that $xw = yz$ in $k[x, y, z, w]/D$, therefore to show that this is not a UFD, it suffices to show that x, y, z, w are all irreducible. Indeed, the graded structure on the domain says that if $x = rs$, then the degree argument with respect to x shows either r or s has degree 0, say r has degree 0, but $r \mid x$, so that forces r to be a unit, i.e., $r = \pm 1$, therefore x is irreducible. Similarly, y, z, w are all irreducibles, so we have a factorization $xw = yz$ as two products of irreducibles, therefore this is not a UFD.

□

Problem 5. (a) By Eisenstein criterion, x^6+3 is irreducible, and since the derivative is non-zero it is separable, therefore $K/\mathbb{Q}$ is a Galois extension of polynomial $x^6 + 3$. Therefore, $K/\mathbb{Q}$ is of degree 6. The roots of $x^6 + 3$ are of the form $\sqrt[6]{-3}\zeta_6^k$ where ζ_6 is a primitive 6th root of unity, namely $\zeta_6 = e^{\frac{2\pi i}{6}} = \frac{1+\sqrt{-3}}{2}$. Therefore, $K = \mathbb{Q}(\sqrt[6]{-3}, \zeta_6) = \mathbb{Q}(\sqrt[6]{-3})$. Now this is generated by σ sending $\sqrt[6]{-3} \mapsto \sqrt[6]{-3}\zeta$ and τ sending $\sqrt[6]{-3} \mapsto -\sqrt[6]{-3}$, therefore σ has order 3 and τ has order 2, and $\sigma\tau \neq \tau\sigma$, therefore this must be S_3.

(b) Subfields L of K over $\mathbb{Q}$ such that $L/\mathbb{Q}$ has degree 3 corresponds to automorphism groups G such that $[S_3 : G]$ has index 3, therefore G is of order 2, thus this is just the 2-cycles in S_3, namely there are 3 of them.

□

8 January 2019

Problems

Problem 8.1. Let G be a p-group. Let H be a normal subgroup of G of order p. Show that H is contained in the center of G.

Problem 8.2. Find all abelian groups, up to isomorphism, of order 360 by listing in each case the elementary divisors and the corresponding invariant factors.

Problem 8.3. (a) Show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

(b) Consider the ring $R = \mathbb{Z}[\sqrt{-5}]$. Show that the ideal $I = (3, 2 + \sqrt{-5})$ is not principal.

(c) Is it possible for R, as defined in part (b), to be a Euclidean domain with respect to some norm?

Problem 8.4. (a) Find the cyclotomic polynomial $\Phi_{20}(x)$ for 20th roots of unity over any field K whose characteristic is relatively prime to 20.

(b) Let $F = \mathbb{Z}/p\mathbb{Z}$, p a prime, and let K be an extension of F such that $[K : F] = n$. Prove that the elements of K are the roots of $x^{p^n} - x = 0$.

(c) Show that every irreducible factor of $\Phi_k(x)$, $k = p^n - 1$, in $F[x]$ has degree n.

Problem 8.5. Consider $f(x) = x^5 - 4x - 2 \in \mathbb{Q}[x]$.

(a) Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(b) Let K be the splitting field of $f(x)$ in $\bar{\mathbb{Q}}$. Find the Galois group $G(K/\mathbb{Q})$ of $f(x)$ over $\mathbb{Q}$.

Solutions

Problem 1. We consider the conjugation action on G, then the fixed points of the conjugation action are just elements in $Z(G)$. Similarly, there is a conjugation action of G on normal subgroup H. By the class equation, we have

$$|H| = |Z(G) \cap H| + \sum_{i=1}^{r} |\operatorname{Orb}(h_i)|,$$

where $\operatorname{Orb}(h_i)$ is the orbit of h_i, where $h_1, \ldots, h_r$ are representatives of conjugacy classes of $H \setminus Z(G)$. Note that $Z(G) \cap H$ has size at least 1, so $\operatorname{Orb}(h_i)$ has size less than p for all i. By orbit-stabilizer theorem, we know that $\operatorname{Orb}(h_i) \mid |H|$, so this forces it to be 1. But this means $h_i \in Z(G) \cap H$, contradiction. In particular, this means there is no such orbits outside of $Z(G) \cap H$, thus $H = Z(G) \cap H$, so $H \subseteq Z(G)$. □

Problem 2. By the fundamental theorem of finitely-generated abelian groups, given a group G of order 360, it must be the product of cyclic groups. Note that $360 = 2^3 \times 3^2 \times 5$, so G must be one of the following:

- $\mathbb{Z}/2^3\mathbb{Z} \oplus \mathbb{Z}/3^2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$,
- $\mathbb{Z}/2^2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3^2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$,
- $\mathbb{Z}/2^2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$,
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3^2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$,

- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

Therefore, these correspond to the following elementary divisors:

- $\{8, 9, 5\}$,
- $\{4, 2, 9, 5\}$,
- $\{4, 2, 3, 3, 5\}$,
- $\{2, 2, 2, 9, 5\}$,
- $\{2, 2, 2, 3, 3, 5\}$.

Also, these correspond to the following invariant factors:

- $\{360\}$,
- $\{180, 2\}$,
- $\{60, 6\}$,
- $\{90, 2, 2\}$,
- $\{30, 6, 2\}$.

□

Problem 3. (a) We define

$$\begin{aligned} \varphi : \mathbb{Z}[\sqrt{2}] &\to \mathbb{Z}_{\geq 0} \\ a + b\sqrt{2} &\mapsto |a^2 - 2b^2| \end{aligned}$$

and it suffices to show that φ is Euclidean. (Note that φ is the absolute norm.) Indeed, consider $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2} \neq 0$, then we have

$$\frac{x}{y} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} = \frac{(ac - 2bd) + (bc - ad)\sqrt{2}}{c^2 - 2d^2},$$

and we denote it by $\frac{x}{y} = A + B\sqrt{2}$. Suppose $C + D\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is the closest point to $A + B\sqrt{2}$, then we have $|A - C| \leq \frac{1}{2}$ and $|B - D| \leq \frac{1}{2}$. Now we have

$$\frac{x}{y} - (C + D\sqrt{2}) = (A - C) + (B - D)\sqrt{2},$$

therefore $((A - C) + (B - D)\sqrt{2})y = x - (C + D\sqrt{2})y \in \mathbb{Z}[\sqrt{2}]$, therefore

$$x = (C + D\sqrt{2})y + ((A - C) + (B - D)\sqrt{2})y.$$

Since $C + D\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and $(A - C) + (B - D)\sqrt{2}, y \in \mathbb{Z}[\sqrt{2}]$, then this is a division algorithm. It now suffices to show that the norm $N(((A - C) + (B - D)\sqrt{2})y) < N(y)$. Indeed,

$$\begin{aligned} N(((A - C) + (B - D)\sqrt{2})y) &= N((A - C) + (B - D)\sqrt{2}) \cdot N(y) \\ &= |(A - C)^2 - 2(B - D)^2| \cdot N(y) \end{aligned}$$

$$\begin{aligned}&\leq \left|\frac{1}{4}-2\times\frac{1}{4}\right|\cdot N(y)\\&< N(y).\end{aligned}$$

Therefore, $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain indeed.

(b) Suppose not, then $I=(a+b\sqrt{-5})$ for some $a+b\sqrt{-5}\in\mathbb{Z}[\sqrt{-5}]$. In particular, $a+b\sqrt{2}$ should divide both elements, and therefore its norm $N(a+b\sqrt{-5})$ divides $N(3)=3^2=9$ and $N(2+\sqrt{-5})=9$, so it is either 1, 3, or 9. There is no element $a+b\sqrt{-5}$ with norm 3, so it cannot be 3. It cannot be 9 as well because it has norm 9 and divides 3, then it has to be 3 up to multiplication of units, but that means 3 and $2+\sqrt{-5}$ are the same up to multiplication of units, contradiction. Therefore, the norm of $a+b\sqrt{-5}$ must be 1, hence $a+b\sqrt{-5}$ is a unit, therefore $I=\mathbb{Z}[\sqrt{-5}]$. We claim that this is impossible by showing $\sqrt{-5}\notin I$. Suppose we have $3(x_1+y_1\sqrt{-5})+(2+\sqrt{-5})(x_2+y_2\sqrt{-5})=1$, then $(3x_1+2x_2-5y_2)+(3y_1+x_2+2y_2)\sqrt{-5}=1$, therefore

$$\begin{cases}3x_1+2x_2-5y_2 &=1\\3y_1+x_2+2y_2 &=0\end{cases}$$

and so

$$\begin{cases}2x_2-2y_2 &\equiv 1 \pmod 3\\x_2+2y_2 &\equiv 0 \pmod 3\end{cases}$$

but when adding these two equations together we get a contradiction. Therefore, $I\neq\mathbb{Z}[\sqrt{-5}]$, hence there is no such generator $a+b\sqrt{-5}$, so $I=(3,2+\sqrt{-5})$ is not principal.

(c) No. If it is a Euclidean domain, then it must be a PID as well. However, by part (b), we have shown that it is not a PID since the ideal $I=(3,2+\sqrt{-5})$ is not principal, contradiction.

□

Problem 4. (a) First note that

$$x^{20}-1=\prod_{n\mid 20}\Phi_d=\Phi_1\Phi_2\Phi_4\Phi_5\Phi_{10}\Phi_{20}$$

and note that $\Phi_p=x^{p-1}+\cdots+1$ for prime p. We also have $\Phi_1=x-1$, therefore

$$x^{20}-1=(x^2-1)(x^4+\cdots+x+1)\Phi_4\Phi_{10}\Phi_{20}.$$

Also, if n is odd, then $\Phi_{2n}(x)=\Phi_n(-x)$; if p is prime and $p\nmid n$, then $\Phi_{np}(x)=\Phi_n(x^p)/\Phi_n(x)$; if p is prime and $p\mid n$, then $\Phi_{np}(x)=\Phi_n(x^p)$. Therefore, $\Phi_4(x)=\Phi_2(x^2)=x^2+1$, $\Phi_{10}=\Phi_5(-x)=x^4-x^3+x^2-x+1$, and $\Phi_{20}=\Phi_{10}(x^2)=x^8-x^6+x^4-x^2+1$. This checks out.

(b) See part (b) of May 2022, Problem 4 (Problem 1.4).

(c) Note that $\Phi_{p^n-1}\mid x^{p^n-1}-1\mid x^{p^n}-x$, therefore the roots of Φ_{p^n-1} are elements in K. In particular, Φ_{p^n-1} splits in K over F. Therefore, a root $\eta\in K$ if and only if $\eta^{p^n}=\eta$, if and only if $p^n\equiv 1\pmod n$. Moreover, n is the minimal exponent such that this holds, therefore the minimal polynomial of η over K must have degree n. But that means every root of Φ_{p^n-1} has minimal polynomial of degree n, therefore the polynomial must split into such irreducible factors of degree n.

□

Problem 5. (a) This is obvious by Eisenstein criterion on $p = 2$.

(b) Because f is a polynomial of degree 5, then there is a natural embedding of $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_5$. Since $f(x)$ is irreducible with non-zero derivative, then it is separable with five distinct roots. Therefore, $K/\mathbb{Q}$ is a Galois extension. Taking the derivative, we have $f'(x) = 5x^4 - 4$, with two real roots. By Rolle's Theorem, there exists a root of $f'(x)$ between any two roots of $f(x)$, therefore since f is separable we know f has three real roots and a pair of complex roots. Therefore, the complex conjugation of order 2 is part of the Galois group. Let α be a non-real root of f, then note that the size of the Galois group is $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \times [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \times 5$ since f is irreducible and separable. Therefore, $\mathrm{Gal}(K/\mathbb{Q})$ should contain a 5-cycle and a transposition. However, we know S_n is generated by an n-cycle and a transposition if and only if n is prime. Therefore, S_5 is generated by a 5-cycle and a transposition, therefore $\mathrm{Gal}(K/\mathbb{Q}) = S_5$.

□

9 August 2018

Problems

Problem 9.1. Let G be a finite group of order p^2q^2, with $p \neq q$ prime numbers. Show that there is a Sylow subgroup of G which is normal in G.

Problem 9.2. Let R be a ring with identity 1. An element $x \in R$ is called *nilpotent* if $x^n = 0$ for some positive integer n. Denote by $N \subseteq R$ the set of nilpotent elements. Show that:

(a) if x is nilpotent, then $1 - x$ is a unit;

(b) if R is commutative, then $N \subseteq R$ is an ideal;

(c) if R is commutative, then R/N has exactly one nilpotent element.

Problem 9.3. Let V denote the vector space over $\mathbb{R}$ of real polynomials of degree $\leq n$. Let $T : V \to V$ be the linear map given by $T(p(x)) = p'(x)$.

(a) Find the Jordan canonical form of T.

(b) Find the rational canonical form of T.

Problem 9.4. Let L be a Galois extension of $\mathbb{Q}$ of order 100. Show that there exists a chain of extensions $\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq K_3 \subsetneq K_4 = L$ where each K_{i+1} is a Galois extension of K_i.

Problem 9.5. Show that the polynomial $x^6 - 3 \in \mathbb{Q}[x]$ is irreducible and determine its Galois group.

Solutions

Problem 1. If $p = q$ this is just Sylow First theorem. Without loss of generality, say $p > q$, now suppose a group G of order p^2q^2 does not have a normal Sylow subgroup, by Sylow Theorem we know $n_p \equiv 1 \pmod{p}$, $n_p \mid q^2$, and since $p > q$, we must have $n_p = q^2$, therefore $p \mid (q^2 - 1)$, but since $p > q$, we must have $p \mid q + 1$, and this forces $q = 2$ and $p = 3$.

We now have the situation where G is a group of order 36, with $p = 3$ and $q = 2$, and $n_p = 4$ and $n_q = 3$ or 9. Let X be the set of Sylow 3-subgroups, then by Sylow Second theorem we know all elements of X are conjugation, and the conjugation action of G on X induces a group homomorphism $\varphi : G \to S_4$ based on a Sylow 3-subgroup P, so $G/\ker(\varphi) \hookrightarrow S_4$ is a transitive subgroup of S_4, and by cardinality argument we know $\ker(\varphi)$ has order divided by 3. Moreover, $\ker(\varphi) \subseteq P$ by the group action, so $\ker(\varphi)$ has order 3 or 9. If it has order 9, we have a normal Sylow 3-subgroup, contradiction, so suppose $\ker(\varphi)$ has order 3. In particular, we have a normal subgroup $K = \ker(\varphi)$ of G of order 3.

Since $K \lhd G$, then G acts on K by conjugation, and this induces a group homomorphism $\psi : G \to \operatorname{Aut}(K) \cong \mathbb{Z}/2\mathbb{Z}$. Suppose $\operatorname{im}(\psi)$ has order 2, then G has a normal subgroup of order 18. If such a subgroup exists, then P is a Sylow 3-subgroup of it as well, and in particular it is a normal subgroup of index 2. Therefore, it is the unique Sylow 3-subgroup in it. For any $g \in G$, we now have gPg^{-1} contained in some conjugate of this normal subgroup, which is just the subgroup of order 18 itself. In particular, $gPg^{-1} = P$ by uniqueness. Therefore, P is normal in G as well, contradiction. This shows that G does not have a subgroup of order 18, hence the image can only be trivial. Thus, the conjugation action of G on K is trivial, so $K \subseteq Z(G)$ by definition. The center $Z(G)$ now has order divisible be 3 and is normal in G, so the order can be $\{3, 6, 9, 12, 18, 36\}$.

Suppose G is abelian, then every Sylow p-subgroup should be unique, but this is not the case, so G is non-abelian, hence $Z(G)$ cannot have order 36. Moreover, we know $G/Z(G)$ is cyclic implies G to be abelian, so we must have $G/Z(G)$ to not be cyclic, thus $Z(G)$ can only have order as one of $\{3, 6, 9\}$. But $Z(G)$, as a normal subgroup, cannot have order 9 since that implies it is the unique Sylow 3-subgroup; also, if $Z(G)$ has order 6, by Sylow Second theorem we know $PZ(G)$ is a subgroup, and that there is a group isomorphism $PZ(G)/Z(G) \cong P/P \cap Z(G)$. The product group $PZ(G)$ has order dividing by 54, so it must have order dividing 18. Moreover, it contains both K and N, so it has order exactly 18, but we know such subgroup does not exist. Therefore, $Z(G)$ has order 3, but $K \subseteq Z(G)$, so $K = Z(G)$ is the center.

Since $Z(G)$ is a 3-subgroup of G, then it is contained in some Sylow 3-subgroup, and by definition, the conjugates of every element of $Z(G)$ is still in $Z(G)$, so the center is contained in every conjugate of this Sylow subgroup, namely $Z(G)$ is contained in the intersection of all Sylow 3-subgroups, and in particular this means it is exactly the intersection. Therefore, the union of all Sylow 3-subgroups gives $3 + 4 \times (9 - 3) = 27$ elements, including identity.

By Cauchy's theorem, there exists some elements of G of order 2. Let $g \in G$ be of order 2, then adjoining g onto K gives a cyclic group of order 6, therefore creating two elements of order 6 in $K\langle g\rangle$. In particular, adjoining two different elements of order 2 on K gives completely different extensions, such that they are linearly disjoint. Hence, since there are 9 elements of order divisible by 2, so there are at most 3 elements of order 2. Since this element of order 2 is not in the center, then some conjugation of this element produces a second element of order 2, therefore the number of elements of order 2 is either 2 or 3. From the proof of Cauchy's theorem, we know there are an odd number of elements in G of order 2, so there are three of them. In particular, that means we must have three elements of order 2 and six elements of order 6, with no elements of order 4, so this means each Sylow 2-subgroup is given by V_4, including three elements of order 2. But that means we can only find one Sylow 2-subgroup, contradiction. □

Problem 2. (a) Note that $(1 - x)(1 + x + x^2 + \cdots + x^{n-1}) = 1 - x^n = 1$, therefore $1 - x$ is a unit by definition.

(b) We first show that N is an additive subgroup. Note that 0 is obviously nilpotent. If x is nilpotent, then $x^n = 0$, but similarly $(-x)^n = (-1)^n x^n = 0$, so $-x$ is nilpotent as well. Also, if x and y are nilpotent, with $x^{M_1} = 0$ and $y^{M_2} = 0$ for some minimal $M_1, M_2 > 0$, then $(x + y)^{M_1+M_2} = 0$ by looking at the coefficients of the binomial theorem, hence $x + y$ is also nilpotent. Therefore, N is an additive subgroup of R. Moreover, suppose $x \in N$ with $x^M = 0$ and $y \in R$, then xy is nilpotent because $(xy)^M = x^M y^M = 0$ by commutativity. Therefore, N is an ideal of R.

(c) Suppose $a + N$ is nilpotent in R/N for some $a \in R$, then $(a + N)^M = a^M + N = 0 + N$ for some integer $M > 0$. In particular, we know $a \in N$, therefore $a + N$ is just N, thus N is the only element in R/N that is nilpotent.

□

Problem 3. (a) First note that T corresponds to a $(n + 1) \times (n + 1)$ matrix of the form

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & n \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

It is obvious that zero is the only eigenvalue of this matrix by considering the derivative. Also note that $T^{n+1} = 0$ but $T^n \neq 0$, therefore the minimal polynomial of T is $m_T(x) = x^{n+1}$. This already gives a Jordan block of size

$n+1$, therefore the Jordan canonical form is just

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

(b) By part (a), the only invariant factor of T is x^{n+1}, therefore the rational canonical form is

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

as well.

□

Problem 4. Note that $L/\mathbb{Q}$ corresponds to a Galois group of order $100 = 2^2 \times 5^2$. By Sylow Theorems, we know there exists a normal subgroup of order 25. By Galois correspondence, this gives an intermediate field K_2 such that both L/K_2 and $K_2/\mathbb{Q}$ are normal, of degree 25 and 4, respectively, so both subextensions are Galois. By the primitive element theorem, the extension $K_2/\mathbb{Q} = \mathbb{Q}(u)/\mathbb{Q}$ for some element $u \in K_2$, therefore this gives an intermediate field $K_1 = \mathbb{Q}(u^2)$ between K_2 and $\mathbb{Q}$. Finally, since L/K_2 is a Galois extension of order 25, then this corresponds to a Galois group of order 25, but now there exists a normal subgroup of order 5 by Sylow Theorem, therefore this constructs K_3. □

Problem 5. By the Eisenstein criterion, $x^6 - 3$ is irreducible over $\mathbb{Q}$. Moreover, it has non-zero derivative, so it is separable as well. Therefore, any splitting field of $x^6 - 3$ gives a Galois extension over $\mathbb{Q}$. The roots of $x^6 - 3$ are exactly $\sqrt[6]{3}\zeta^i$ where $\zeta = e^{\frac{2\pi i}{6}} = \frac{1+\sqrt{3}i}{2}$ is a primitive 6th root of unity. Therefore, $\mathbb{Q}(i, \sqrt[6]{3}) = \mathbb{Q}(\sqrt{3}i, \sqrt[6]{3}) = \mathbb{Q}(\zeta, \sqrt[6]{3})$ is the splitting field of $x^6 - 3$, since it contains the splitting field and the splitting field contains $\mathbb{Q}(i, \sqrt[6]{3})$. Therefore, $\mathbb{Q}(i, \sqrt[6]{3})/\mathbb{Q}$ is Galois extension for the polynomial $x^6 - 3$, therefore this is an extension of degree 12. Therefore, the Galois group is of order 12. Moreover, this is generated by σ (of order 6) where $\sqrt[6]{3} \mapsto \sqrt[6]{3}\zeta$ and $\zeta \mapsto \zeta$, and τ (of order 2) where $\sqrt[6]{3} \mapsto \sqrt[6]{3}$ and $\zeta \mapsto \bar{\zeta}$. We also have $\sigma\tau\sigma\tau$ to be the identity, therefore this gives a description of the Galois group as D_6. □

10 May 2018

Problems

Problem 10.1. Let P be a Sylow p-subgroup of a finite group G and let N be a normal subgroup of G, such that $P \cap N \neq \{e\}$. Prove that $P \cap N$ is a Sylow p-subgroup of N.

Problem 10.2. Let $\varphi : S_5 \to G$ be a group homomorphism. Classify the image $\varphi(S_5)$, i.e., list all the possibilities for $\varphi(S_5)$ up to isomorphism.

Problem 10.3. Let $T : \mathbb{Q}^4 \to \mathbb{Q}^4$ be the $\mathbb{Q}$-linear transformation which relative to some basis is represented by the matrix

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & -2 & 0 & 1 \\ -2 & 0 & -1 & -2 \end{pmatrix}.$$

Find the rational canonical form for T.

Problem 10.4. Let $\langle (11, 13) \rangle$ be the subgroup of $\mathbb{Z} \oplus \mathbb{Z}$ generated by the element $(11, 13)$. Show that the quotient group $(\mathbb{Z} \oplus \mathbb{Z}) / \langle (11, 13) \rangle$ is torsion-free.

Problem 10.5. (a) Find the Galois group of the polynomial $p(x) = x^3 - 10$ over the field $K = \mathbb{Q}(\sqrt{2})$.

(b) Let $q(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree $p \geq 2$. Show that if $q(x)$ has exactly two non-real roots (i.e., two complex roots) then the Galois group of $q(x)$ is isomorphic to S_p.

Solutions

Problem 1. Recall by the second isomorphism theorem, we have $N \lhd PN$ and $P \cap N \lhd P$, and that $\frac{|PN|}{|N|} = \frac{|P|}{|P \cap N|}$, and therefore $\frac{|PN|}{|P|} = \frac{|N|}{|P \cap N|}$. Since $P \subseteq PN \subseteq G$, then $\frac{|PN|}{|P|}$ is not divisible by p. If the value is 1, then $|PN| = |P|$, then $N = P \cap N$, hence $N \subseteq P$. In particular, N is a p-subgroup of G since P is. Therefore, $N = P \cap N$ is a Sylow p-subgroup of N by definition. Suppose the value is not 1, $\frac{|N|}{|P \cap N|}$ is not 1 and is not divisible by p, but since $P \cap N \subseteq P$ then it is a p-subgroup of N (and is not trivial by assumption), so by definition $P \cap N$ is a Sylow p-subgroup of N. □

Problem 2. By the first isomorphism theorem, the image $\varphi(S_5) \cong S_5 / \ker(\varphi)$ where $\ker(\varphi) \lhd S_5$. Therefore to classify the image is just to classify the normal subgroups of S_5. But we know that for $n \geq 5$, the only proper normal subgroup of S_n is A_n, therefore the normal subgroups of S_5 are $\{e\}$, A_5, and S_5. Hence, $\varphi(S_5)$ are either S_5, $S_5/A_5 \cong \mathbb{Z}/2\mathbb{Z}$, or $\{e\}$. □

Problem 3. By cofactor expansion via the first row, we know

$$\begin{aligned} \det(A - \lambda I) &= (1 - \lambda) \cdot \det \begin{pmatrix} 1 - \lambda & 0 & 0 \\ -2 & -\lambda & 1 \\ 0 & -1 & -2 - \lambda \end{pmatrix} \\ &= (1 - \lambda) \cdot ((1 - \lambda)(-\lambda)(-2 - \lambda) - (\lambda - 1)) \\ &= (1 - \lambda)((\lambda - 1)(\lambda(-2 - \lambda) - 1)) \\ &= (1 - \lambda)((\lambda - 1)(-\lambda^2 - 2\lambda - 1)) \\ &= (\lambda - 1)^2(\lambda + 1)^2. \end{aligned}$$

This gives the characteristic polynomial $c_A = (x-1)^2(x+1)^2$ of A. To find the invariant factors, note that the minimal polynomial m_A, as the largest invariant factor, must satisfy $(x-1)(x+1) \mid c_A \mid m_A$. Therefore, c_A is either $(x-1)(x+1)$, $(x-1)^2(x+1)$, $(x-1)(x+1)^2$, or $(x-1)^2(x+1)^2$. We can calculate

$$A^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -4 & -2 & -1 & -2 \\ 4 & 2 & 2 & 3 \end{pmatrix}$$

so $m_A \neq (x-1)(x+1)$. Also,

$$A^3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 0 & 2 & 3 \\ -6 & -2 & -3 & -4 \end{pmatrix}.$$

By comparing elements we know A is not a root of $(x-1)^2(x+1) = x^3 - x^2 - x + 1$ is not the minimal polynomial, but A is a root of $(x-1)(x+1)^2 = x^3 + x^2 - x - 1$, so the minimal polynomial is $m_A = x^3 + x^2 - x - 1$. The invariant factors are $\{(x-1), (x-1)(x+1)^2\}$. Therefore, the rational canonical form of T is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

□

Problem 4. Let (a, b) be a torsion element of $(\mathbb{Z}\oplus\mathbb{Z})/\langle(11, 13)\rangle$, then there exist some positive integer n such that $a^n \equiv 0 \pmod{11}$ and $b^n \equiv 0 \pmod{13}$, but the first equation means $11 \mid a^n$, so $11 \mid a$, therefore $a = 0$; similarly $b = 0$, therefore $(0, 0)$ is the only torsion element in $(\mathbb{Z}\oplus\mathbb{Z})/\langle(11, 13)\rangle$, hence $(\mathbb{Z}\oplus\mathbb{Z})/\langle(11, 13)\rangle$ is torsion-free as a group. □

Problem 5. (a) Note that the roots of $p(x) = x^3 - 10$ are $\sqrt[3]{10}$, $\sqrt[3]{10}\zeta_3$, and $\sqrt[3]{10}\zeta_3^2$, where $\zeta = \frac{-1+\sqrt{3}}{2}$ is a primitive third root of unity. Therefore, we claim that the splitting field of $p(x) = x^3 - 10$ over $K = \mathbb{Q}(\sqrt{2})$ is $K(\sqrt[3]{10}, \zeta_3)$. Indeed, note that all three roots are generated in this field, and note that the splitting field should contain $K(\sqrt[3]{10}, \zeta_3)$ as well. Since $p(x)$ is irreducible over a perfect field, then it is separable, and therefore the extension is separable and normal hence Galois. Therefore, we just need to find out the degree of this extension $K(\sqrt[3]{10}, \zeta_3)/K$. First note that $K(\sqrt[3]{10})/K$ is of degree 3 since $x^3 - 10$ is irreducible in K as it does not have a root in K, and $K(\sqrt[3]{10}, \zeta_3)/K(\sqrt[3]{10})$ is of degree 2, since $K(\sqrt[3]{10}, \zeta_3) = K(\sqrt[3]{10}, \sqrt{3})$ and $\sqrt{3} \notin K(\sqrt[3]{10})$. Hence, we have $K(\sqrt[3]{10}, \zeta_3)/K$ as degree 6. In particular, the Galois group G of $p(x)$ is of order 6. This is generated by two automorphisms, namely σ with $\sqrt[3]{10} \mapsto \sqrt[3]{10}\zeta_3$ and $\zeta_3 \mapsto \zeta_3$, and τ with $\sqrt[3]{10} \mapsto \sqrt[3]{10}$ and $\zeta_3 \mapsto \zeta_3^2$. Therefore, $\sigma^{-1}\tau\sigma$ sends $\sqrt[3]{10} \mapsto \sqrt[3]{10} \mapsto \sqrt[3]{10}\zeta_3$ and $\zeta_3 \mapsto \zeta_3^2$, therefore we have $\tau\sigma = \sigma\tau$, so G is abelian since its generators commute, hence by classification we have $G \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\times\mathbb{Z}/3\mathbb{Z}$.

(b) Since $q(x)$ is of degree $p \geq 2$ over $\mathbb{Q}$, then irreducible implies separable, therefore the splitting field $K/\mathbb{Q}$ is a Galois extension. Let $\alpha \in K$ be a root of $q(x)$, then $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \times [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] \times p$ (where $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ since this is the degree of the minimal polynomial, namely $q(x)$). Hence, $\mathrm{Gal}(K : \mathbb{Q})$ has order divisible by p. By Cauchy's Theorem, the Galois group has an element of order p. Moreover, since $q(x)$ has exactly two non-real roots, then the complex conjugation acts as an automorphism of order 2, i.e., a transposition.

Finally, since S_n is generated by an n-cycle and a transposition if and only if n is prime, then the Galois group is just S_p.

□

11 January 2018

Problems

Problem 11.1. Let P be a Sylow p-subgroup of a finite group G and let $N_G(P) \subseteq H \subseteq G$ be a subgroup, where $N_G(P)$ denotes the normalizer of P. Prove that $N_G(H) = H$.

Problem 11.2. Must a group of order $3 \cdot 3 \cdot 3 \cdot 5$ be nilpotent?

Problem 11.3. Let V be a vector space over the field K. Assume that V is isomorphic to the direct sum of cyclic $K[x]$-modules

$$K[x]/(x+1)^2 \oplus K[x]/(x^2-1) \oplus K[x]/(x-1)^2.$$

(a) Determine the invariant factors and elementary divisors for V.

(b) Give the rational canonical form for the matrix that describes multiplication by x on V, i.e., for the linear map $V \to V$ that maps $v \mapsto xv$.

Problem 11.4. Let F and K be fields with $F \subseteq K$.

(a) State what it means for an element $x \in K$ to be algebraic over F.

(b) Using the definition in (a) prove that if $x \in K$ and $y \in K$ are algebraic over F then both $x+y$ and xy are algebraic over F.

Problem 11.5. Let $f(x) = x^4 + 6x^2 + 1 \in \mathbb{Q}[x]$.

(a) Compute, with proof, the Galois group of the polynomial $f(x)$. You may use that the polynomial has discriminant $\Delta = 2^{14}$ and cubic resolvent $g(x) = x^3 - 12x^2 + 32x$.

(b) Let K be the splitting field over $\mathbb{Q}$ of the polynomial $f(x)$. Use the Galois group obtained under part (a) to determine the number of subfields $F \subseteq K$ with $[F : \mathbb{Q}] = 2$.

Note: If you were not able to solve part (a) you may assume that the Galois group is $G \cong A_4 \subseteq S_4$.

Solutions

Problem 1. Recall that

Lemma 1 (Frattini Argument)**.** Suppose K is a finite group, $H \lhd K$ is normal and $P \subseteq G$ is Sylow-p, then $K \cong H \times N_K(P)$.

In particular, let $K = N_G(H)$, then $H \lhd N_G(H)$ and $P \subseteq N_G(H)$ is Sylow-p, therefore $N_G(H) \cong H \times N_G(P)$, but $N_G(P) \subseteq H$, so $N_G(H) \subseteq H$, therefore $N_G(H) = H$. □

Problem 2. By Sylow theorems we know $n_3 = 1$ and $n_5 = 1$, then every Sylow subgroup of such groups should be normal, therefore this group is the product of its Sylow subgroups, hence it must be nilpotent. □

Problem 3. (a) The elementary divisors are $\{(x-1)^2, (x-1), (x+1)^2, (x+1)\}$, and the invariant factors are $\{(x+1)^2(x-1)^2, (x+1)(x-1)\}$.

(b) Note that the companion matrix is similar to the matrix of multiplication by x, so we are just looking for the rational canonical form of cyclic modules. Therefore, if we set $V = K[x]/(x+1)^2(x-1)^2 \oplus K[x]/(x+1)(x-1)$, then the rational canonical form is

$$\begin{pmatrix} 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

□

Problem 4. (a) An element $x \in K$ is algebraic over F if there exists a non-zero polynomial $f \in F[x]$ such that $f(x) = 0$.

(b) Suppose $x, y \in K$ are both algebraic elements, then we find $f, g \in F[x]$ such that $f(x) = 0$ and $g(y) = 0$. We first show that $x + y$ is also algebraic. Without loss of generality, let f and g be minimal (polynomials), then we think of $F[x, y]/(f(x), g(y))$ as a cyclic module. Obviously there is a basis given by $x^i y^j$ for some i, j, then consider multiplication by $x + y$ on this cyclic module, then this corresponds to a matrix with respect to the basis above. In particular, by Cayley-Hamilton theorem, this matrix satisfies its own characteristic equation, but note that this means its eigenvalues also satisfy this equation, and namely $x + y$ is one of the eigenvalues. Similar results hold for xy.

□

Problem 5. (a) First note that the determinant of $f(x)$ is a square, therefore the Galois group is a subgroup of $A_4 \subseteq S_4$. Now we look at the resolvent $g(x) = x^3 - 12x^2 + 32x = x(x-4)(x-8)$, therefore g is reducible and so the Galois group is a subgroup of D_4. Moreover, since the resolvent just splits, so this is K_4, the Klein-4 group.

(b) It is easy to check that $f(x)$ is separable, so $K/\mathbb{Q}$ is Galois. By the fundamental theorem of Galois theory, the number of subfields $F/\mathbb{Q}$ in $K/\mathbb{Q}$ corresponds to the subgroups of K_4, but $K_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle$, so the subgroups are exactly $\{e\}$, $\langle a \rangle$, $\langle b \rangle$, $\langle ab \rangle$, and K_4. Therefore, there are five of them.

□

12 August 2017

Problems

Problem 12.1. (a) Let $u_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$ denote the upper triangular nilpotent matrix with 1's just above the diagonal and 0's elsewhere. Show that if c is any non-zero complex number and I_n is the $n \times n$ identity matrix, then $(cI_n + u_n)^k \neq I_n$ for all $k > 0$.

(b) Let $\mathrm{GL}_n(\mathbb{C})$ denote the group of invertible $n \times n$ matrices with complex coefficients (with matrix multiplication as the group operation). Prove that for every $k > 0$, if $\Phi : \mathbb{Z}/k\mathbb{Z} \to \mathrm{GL}_n(\mathbb{C})$ is any group homomorphism, there exists some $g \in \mathrm{GL}_n(\mathbb{C})$ such that $g\Phi(m)g^{-1}$ is a diagonal matrix for all $m \in \mathbb{Z}/k\mathbb{Z}$.

(c) Prove by example that the conclusion of part (b) can fail if $\mathrm{GL}_n(\mathbb{C})$ is replaced by $\mathrm{GL}_n(F)$ for appropriate choices of integers k and n and finite field F.

Problem 12.2. Must a group of order $3 \cdot 5 \cdot 7$ be solvable?

Problem 12.3. Let $A = \begin{pmatrix} -2 & -2 & -1 \\ 0 & -4 & -1 \\ 0 & 4 & 0 \end{pmatrix}$. Make $V = \mathbb{C}^3$ into a $\mathbb{C}[x]$-module by $f(x)v := f(A) \cdot v$ via matrix multiplication for $f(x) \in \mathbb{C}[x]$, $v \in V$. Find an elementary divisor decomposition of the module V.

Problem 12.4. Consider the ring $R = \mathbb{C}[x, y, z]/\left\langle z^2 - xy \right\rangle$. Show that R is not a UFD.

Problem 12.5. Let $K = \mathbb{Q}(\omega)$ where $\omega = e^{\frac{2\pi i}{17}}$.

(a) Prove that K contains a unique subfield L such that $[L : \mathbb{Q}] = 8$.

(b) Is L Galois over $\mathbb{Q}$?

Solutions

Problem 1. (a) Note that $cI_n + u_n$ is in Jordan canonical form with eigenvalue c's, and note that $u_n^n = 0$. Therefore, the kth power gives $(cI_n + u_n)^k = \sum\limits_{r=0}^{k} \binom{k}{r} (cI_n)^{k-r} u_n^r = \sum\limits_{r=0}^{\min(k,n-1)} \binom{k}{r} c^{k-r} u_n^r$ which is obviously not I_n.

(b) Since $1 \in \mathbb{Z}/k\mathbb{Z}$ generates the group, then it suffices to show there exists such g for $m = 1$, then $g\Phi(m)g^{-1} = g\Phi(1)g^{-1})^m$. Now m has order k, therefore $m^k = 0 \in \mathbb{Z}/k\mathbb{Z}$, and so $\Phi(m)^k = \Phi(m^k) = I_n$ is the identity matrix. Therefore, $x^k - 1$ annihilates the matrix, and so the minimal polynomial of $\Phi(m)$ divides $x^k - 1$. In particular, that means the minimal polynomial splits into distinct linear factors over $\mathbb{C}$, thus $\Phi(m)$ is diagonalizable.

(c) For instance, take $\Phi(m) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with $k = 2$, $m = 1$, and $F = \mathbb{F}_2$, then the minimal polynomial and the characteristic polynomial are both $x^2 + 1 = (x + 1)^2$, therefore the minimal polynomial does not split into distinct linear factors, hence this is not diagonalizable.

□

Problem 2. Recall that a subgroup of the smallest prime index is normal, therefore a group G of order $3 \cdot 5 \cdot 7 = 105$ has a normal subgroup N of order 7. In particular, N is solvable. Now $H = G/N$ is a group of order 15, so by Sylow theorems we find a normal subgroup M of order 5 therefore it is solvable, and since H/M is a group of order 3, then it is solvable as well, hence H is solvable, and therefore G is solvable. □

Problem 3. Note that the matrix has characteristic polynomial $-(x+2)^3$, and note that $(x+2)^2$ already gives the zero matrix, therefore the invariant factors are $\{-(x+2), (x+2)^2\}$. This is also the set of elementary divisors. □

Problem 4. Note that $z^2 = xy$ in R. We claim that x, y, z are all irreducible elements in R. Consider $x = rs$, then since R gives a graded structure, then the degree with respect to x says that either r or s has degree 0, say $\deg(r) = 0$, then $r \in \mathbb{C}$ is a unit, therefore x is irreducible. Similarly, y, z are both irreducible, so we have two distinct irreducible factorizations for an element in R, so R is not a UFD. □

Problem 5. (a) Note that ω is a root of $x^{17} - 1$, which factors into $(x-1)(x^{16} + \cdots + x + 1)$, and therefore the minimal polynomial m_ω has degree 16. In particular, the minimal polynomial splits and therefore any splitting field of m_ω is Galois. In particular, $K = \mathbb{Q}(\omega)$ generates all roots of m_ω since ω is primitive, so $K/\mathbb{Q}$ is Galois extension as the splitting field of ω and m_ω. By the Galois correspondence, this gives a Galois group of order 16, namely $(\mathbb{Z}/17\mathbb{Z})^\times \cong \mathbb{Z}/16\mathbb{Z}$. By the Galois correspondence, if we want a subfield with degree 8, we just need a subgroup of index 8, namely a group of order 2, hence we just need to prove there exists a unique element of order 2 in the group. This is obvious given by $8 + 8 \equiv 0 \pmod{16}$.

(b) Having $L/\mathbb{Q}$ to be Galois is equivalent to having it to be normal, which is equivalent to having $\langle 8 \rangle \subseteq \mathbb{Z}/16\mathbb{Z}$ as a normal subgroup. This is true since given any $n \neq 0$, we have $n + 8 + (-n) \equiv 8 \pmod{16}$.

□

13 May 2017

Problems

Problem 13.1. (a) Let G be a group of order $2n$ ($n > 0$). Show that G has at least one element of order 2.

(b) Consider the action of $\mathbb{Z}_2 \cong (\{1, -1\}, \times)$ on S_4 by automorphisms, where -1 acts by conjugation by the transposition $(1\ 2)$. Is the semi-direct product $\mathbb{Z}_2 \ltimes S_4$ a nilpotent group? Solvable?

Problem 13.2. (a) Give an example of a finite field of order 27.

(b) Suppose a commutative ring R with identity has order 27. List all possible values of the characteristic of R, and give examples to show that all the values you list are attained.

Problem 13.3. Let $\mathbb{R}^\infty = \bigoplus\limits_{k=1}^{+\infty} \mathbb{R}$ (direct sum of $\mathbb{R}$-modules) and let $R = \operatorname{End}(\mathbb{R}^\infty)$ be the ring of all $\mathbb{R}$-linear transformations from $\mathbb{R}^\infty$ to itself. Show that R is isomorphic to $R \oplus R$ as a left R-module (so R, viewed as a left R-module, has a basis with 2 elements!).

Problem 13.4. Given an example of an integral domain D, where every irreducible element is prime, and which admits an infinite chain of ascending principal ideals:

$$\langle d_1 \rangle \subsetneq \langle d_2 \rangle \subsetneq \langle d_3 \rangle \subsetneq \cdots \subsetneq \langle d_n \rangle \subsetneq \cdots$$

What can you say about prime factorizations in this domain?

Problem 13.5. Consider the extension $L = \mathbb{Q}(\sqrt[3]{5}, i)$ of $\mathbb{Q}$. Find all subfields $\mathbb{Q} \subsetneq M \subsetneq L$ which are normal extensions of $\mathbb{Q}$.

Solutions

Problem 1. (a) We will prove Cauchy's Theorem directly.

Theorem 13.6. Let G be a group of order n with some prime $p \mid n$, then G has an element of order p.

Let X be the set of elements $(g_1, \ldots, g_p)$ for $g_i \in G$ such that $g_1 g_2 \cdots g_p = e$. In particular, g_p is determined by the previous $p-1$ elements, so $|X| = |G|^{p-1}$ and is divisible by p. Note that given such p elements, any $g_i \cdots g_p g_1 \cdots g_{i-1} = e$ as well. Therefore, by shifting p times we are back to the original ordering. Hence, $H = \mathbb{Z}/p\mathbb{Z}$ acts on X by this permutation of elements, and since H is a p-group, then $|X^H| \equiv |X| \pmod{p}$. Note that X^H is the set of elements that is fixed by every element in H, which means this is the set of elements of the form $(g, \ldots, g)$, hence $X^H \neq \varnothing$ because $(e, \ldots, e) \in X^H$. In particular, X^H has at least p elements, so we can find some non-trivial element $g \in G$ such that $(g, \ldots, g) \in X^H$, and by definition this means $g^p = e$.

(b) Let $G = K \times H := \mathbb{Z}_2 \ltimes S_4$ with $H \lhd G$. Suppose G is nilpotent, then $H = S_4 \lhd G$ must also be nilpotent, but this is not true. Note that H is nilpotent if and only if it is the direct product of its Sylow subgroups, which happens if and only if all Sylow subgroups are normal, i.e., unique, but S_4 has $\binom{4}{3} \times 2 = 8$ elements $(a\ b\ c)$ of order 3, so it cannot have only one Sylow-3 subgroup, contradiction.

However, G is solvable. Indeed, $G/H \cong \mathbb{Z}/2\mathbb{Z}$ and $H \lhd G$ are both solvable.

□

Problem 2. (a) Let $p(x) = x^3 + 2x + 1$, then $p(x)$ is irreducible over $\mathbb{F}_3$. In particular, the quotient ring $F_3/p(x)$ gives a field extension of degree 3, and since $p(x)$ is irreducible hence prime in the field, we know $F_3/p(x)$ is a field of order 27.

(b) Note that if a ring has characteristic 0 then it is infinite, so the characteristic of R must be finite. Since the ring has 27 elements, then every element in the additive group has order dividing 27. In particular, the order of 1 divides 27, so the characteristic should be either 3, 9, or 27.

A ring of characteristic 27 is just $\mathbb{Z}/27\mathbb{Z}$. An example of a ring of characteristic 3 is given in part (a), namely a field of order 27. A ring of characteristic 9 can be given by $\mathbb{Z}_9[x, y]/(x^2, y^2)$.

□

Problem 3. In particular, R is the matrix ring of dimension $\infty \times \infty$ with entries in $\mathbb{R}$. Given an R-module structure on $R \oplus R$, we define a module homomorphism by

$$\begin{aligned} \varphi : R \oplus R &\to R \\ (A, B) &\mapsto C \end{aligned}$$

where the matrix C has odd columns given by columns of A and even columns given by columns of B. This is a homomorphism of abelian groups that respects the (left) action of R. This homomorphism respects the action of R because we send it by columns instead of rows. The bijection is obvious. Also, this bijection is well-defined as a direct sum since C is finitely-generated (i.e., has finitely many non-zero entries) if and only if A and B are both finitely-generated. Therefore, this is a well-defined module isomorphism. □

Problem 4. Note that

- if D admits factorization then D is a UFD if and only if irreducible elements are prime;
- if D admits an infinite chain of ascending principal ideals, then D is not Noetherian, hence D is not a PID.

Therefore, we want a UFD that is not a PID. For instance, we can take $D = F[x, y]$ where F is a field. Since F is a field hence UFD, then so is $F[x]$ and $F[x, y]$. But $F[x, y]$ is not a PID since (x, y) is not principal in $F[x, y]$. In particular, this is a UFD and therefore admits a unique factorization. □

Problem 5. Note that $L/\mathbb{Q}$ is not the splitting field of $x^3 - 5$. We look at the diagram

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[3]{5}, i) = \mathbb{Q}(\sqrt[3]{5}i) \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
\mathbb{Q}(\sqrt[3]{5}) \arrow[dr, dash, "3"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\mathbb{Q}(i)/\mathbb{Q}$ is obviously normal since $x^2 + 1$ splits in this extension. $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ is not normal since the minimal polynomial of $\sqrt[3]{5}$ is $x^3 - 5$, which does not split in this extension. □

14 January 2017

Problems

Problem 14.1. (a) Suppose G is a group with an abelian normal subgroup N and abelian quotient group G/N. Is G an abelian group?

(b) Suppose G has order p^3 for a prime p. Is G a nilpotent group?

Problem 14.2. (a) Prove that every finite field has order a power of a prime p.

(b) Given an example of a commutative ring R of prime power order p^n which is not a field.

Problem 14.3. Consider the action of the group $G = \mathrm{GL}_2(\mathbb{C})$ (2×2 invertible matrices with complex coefficients) on the set $M_2(\mathbb{C})$ (*all* 2×2 matrices with complex coefficients) defined by $g \cdot M = gMg^{-1}$. For the matrix

$$M_{ab} = \begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix}$$

describe (in terms of $a, b \in \mathbb{C}$) its stabilizer subgroup

$$G_{M_{ab}} = \{g \in \mathrm{GL}_2(\mathbb{C}) \mid gM_{ab}g^{-1} = M_{ab}\}.$$

Problem 14.4. Let D be a unique factorization domain. If $D' \subseteq D$ is a subring containing 1, is it true that D' is itself a unique factorization domain?

Problem 14.5. Let $p(x) \in \mathbb{Q}[x]$ be a polynomial of degree 5, with splitting field E and Galois group isomorphic to the alternating group A_5.

(a) Is $p(x)$ irreducible over $\mathbb{Q}$?

(b) Find $[E : \mathbb{Q}]$.

(c) How many subfields of E have degree 12 over $\mathbb{Q}$?

(d) Which subfields of E are normal over $\mathbb{Q}$?

Solutions

Problem 1. (a) No, this is not necessarily true. Take $G = Q_8$, then by Sylow Theorem we know there exists a subgroup N of order 4, in particular N has index 2 in G, so this is a normal subgroup of order 4, hence abelian. Moreover, we have $G/N \cong \mathbb{Z}/2\mathbb{Z}$ to be another abelian subgroup. But $G = Q_8$ is known to be non-abelian, since $ij = k \neq -k = ji$.

(b) Yes, every group of order p^n for some prime p is nilpotent. Fix some prime p, and we proceed by induction on n. This is obvious for $n = 1$, as we have $G \cong \mathbb{Z}/p\mathbb{Z}$, which is abelian and therefore nilpotent. For $n > 1$, suppose the statement is true for order $p, \dots, p^{n-1}$, then recall that a p-group must have non-trivial center, therefore $Z(G) \neq \{e\}$ is a p-group, so $G/Z(G)$ is also a p-group with order less than p^n, then by the inductive hypothesis we know $G/Z(G)$ is nilpotent, therefore so is G.

In particular, a group of order p^3 is nilpotent.

□

Problem 2. (a) Since the field is finite, then it has non-zero characteristic. Let $p \geq 2$ be the characteristic of the finite field F, therefore $p \mid |F|$. Suppose there exists some other prime q such that $q \mid |F|$, then by Cauchy theorem there exists some element x in F with order q, so $qx = 0$. Note that by definition $px = 0$ as well. Since $\gcd(p, q) = 1$, then there exists some integers a, b such that $ap + bq = 1$, therefore $(ap + bq)x = x$, hence $x = 0$. In particular, this says that F is the trivial field, which cannot have characteristic $p \geq 2$.

(b) The ring $\mathbb{Z}/p^2\mathbb{Z}$ is obviously not a field. By construction, it must have characteristic p, therefore $p \cdot [1] = 0$, which is not true.

□

Problem 3. Suppose there is a matrix A that satisfies this, then the normalized matrix $\bar{A}$ with determinant 1 should also satisfy the relation, so without loss of generality we ask A to have determinant 1. A calculation shows that we want M_{ab} equals to

$$\begin{pmatrix} aa_{11}a_{22} - a_{11}a_{21} - ba_{12}a_{21} & -aa_{11}a_{12} + a_{11}^2 + ba_{11}a_{12} \\ aa_{21}a_{22} - a_{21}^2 - ba_{21}a_{22} & -aa_{12}a_{21} + a_{11}a_{21} + ba_{11}a_{22} \end{pmatrix}$$

In particular, this gives

$$\begin{cases} a_{11}(a_{11} + (b-a)a_{12}) & = 1 \\ a_{21}((a-b)a_{22} - a_{21}) & = 0 \end{cases}.$$

If $a = b$, then $a_{21} = 0$ and $a_{11} = \pm 1$, therefore $a_{22} = \pm 1$, so we have matrices of the form

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} -1 & c \\ 0 & -1 \end{pmatrix}$$

for $c \in \mathbb{C}$. From now on we suppose $a \neq b$. The second equation gives $a_{21} = 0$ or $a_{21} = (a-b)a_{22}$.

- If $a_{21} = 0$, then $a_{11}a_{22} = 1$, so $a_{22} = \frac{1}{a_{11} + (b-a)a_{12}}$, hence $a_{11}a_{22} + (b-a)a_{11}a_{12} = 1$, therefore $(b-a)a_{11}a_{12} = 0$, but $a_{aa} \neq 0$ and $a \neq b$, then $a_{12} = 0$. We now have matrices of the form

$$\begin{pmatrix} d & 0 \\ 0 & \frac{1}{d} \end{pmatrix}$$

for $d \in \mathbb{C}^\times$.

- If $a_{21} = (a-b)a_{22}$, then we have

$$\begin{aligned} b &= -aa_{12}a_{21} + a_{11}a_{21} + ba_{11}a_{22} \\ &= -aa_{12}a_{21} + aa_{11}a_{22} \\ &= a, \end{aligned}$$

which is a contradiction from the assumption that $a \neq b$.

Therefore, the stabilizer is given by $\mathbb{C}$-multiples of the following matrices:

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} -1 & c \\ 0 & -1 \end{pmatrix}$$

for $c \in \mathbb{C}$, and

$$\begin{pmatrix} d & 0 \\ 0 & \frac{1}{d} \end{pmatrix}$$

for $d \in \mathbb{C}^{\times}$. □

Problem 4. No. Since $\mathbb{C}$ is a field, then it is a UFD. But $\mathbb{Z}[\sqrt{-5}]$ as a subring of $\mathbb{C}$ is not a UFD: in particular we have $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. □

Problem 5. (a) Since the Galois group is A_5, then this does not embed into S_4 and therefore all roots have to be distinct, so the extension is separable hence $p(x)$ is irreducible. Alternatively, we know A_5 is simple, then the Galois group acts on roots transitively, which implies that the polynomial is separable. (This requires some more work.)

(b) Note that the extension is separable and normal, so this is Galois. By the Galois correspondence, we have $[E : \mathbb{Q}] = |A_5| = 60$.

(c) By the Galois correspondence, we want to know the number of subgroups of A_5 with order 5, but this is just the number of 5-cycles: the only possible construction is $\mathbb{Z}/5\mathbb{Z}$. Note that every 5-cycle generates a group of order 5 (since it is maximal), and every group of order 5 has four 5-cycle, then there are $\frac{4!}{4} = 6$ of them. Hence, there are 6 corresponding subfields.

(d) By the Galois correspondence, we just want to know the number of normal subgroups in A_5. But A_5 is simple already, so the answer is 2, namely the two obvious ones.

□

15 August 2016

Problems

Problem 15.1. A *short exact sequence* of groups is given by group homomorphisms:

$$K \xrightarrow{i} G \xrightarrow{j} H$$

where i is injective, j is surjective and $\ker(j) = \operatorname{im}(i)$. The short exact sequence is called *split* if there exists a group homomorphism $s : H \to G$ such that $j \circ s = \mathrm{id}$.

(a) Show that there is a split short exact sequence

$$A_n \xrightarrow{\ \ i\ \ } S_n \xrightarrow{\ \ j\ \ } \mathbb{Z}_2.$$

(b) Show that if a short exact sequence is split then G is isomorphic to a semi-direct product $G \cong H \ltimes K$.

Problem 15.2. Let D be a PID and let R be an integral domain containing D as subring. Show that if d is a greatest common divisor in D of elements $a, b \in D$ then d is also a greatest common divisor of a and b in R.

Problem 15.3. Determine the structure of the abelian group $\mathbb{Z}^3/K$ where K is the subgroup generated by $(2, 1, -3)$ and $(1, -1, 2)$.

Problem 15.4. (a) Let $u = e^{\frac{2\pi i}{12}}$, a primitive 12th root of unity. Show that $[\mathbb{Q}(u) : \mathbb{Q}] = 4$ and determine the minimal polynomial of u over $\mathbb{Q}$.

(b) Let F be a subfield of E and assume that $E = F(u)$ where u is algebraic of odd degree. Show that $E = F(u^2)$.

Problem 15.5. Compute the Galois group of $g(x) = x^3 - 4x + 1 \in \mathbb{Q}[x]$.

Solutions

Problem 1. (a) Let $i : A_n \to S_n$ be the obvious inclusion map and $j : S_n \to \mathbb{Z}/2\mathbb{Z}$ be given by the parity of the permutation. Therefore, i is injective and j is surjective, and $\ker(j)$ is exactly the set of even maps, which is isomorphic to $\operatorname{im}(i) \cong A_n$. To see that this sequence splits, let $s : \mathbb{Z}/2\mathbb{Z} \to S_n$ be the map $[0] \mapsto (\ )$ and $[1] \mapsto (1\ 2)$, then obviously $js = \mathrm{id}$ on $\mathbb{Z}/2\mathbb{Z}$. Therefore, the short exact sequence splits.

(b) By the first isomorphism theorem, we know that $H \cong G/K$, and K has to be a normal subgroup of G to maintain the group structure. We need to show that $G = HK$ and $H \cap K = \{e\}$. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r, "i"] & G \arrow[r, "j"] & G/K \arrow[r] & 0 \\
 & & H \arrow[u, hook] \arrow[ur, "j'"'] & &
\end{tikzcd}$$

where j' is the restriction of j onto H. Let $x \in H \cap K$, then $j(x) = e$ by exactness, so $j'(x) = e$ by restriction. But the restriction map j' is an isomorphism, so $x = e$. Hence, $H \cap K = \{e\}$. Now suppose $g \in G$, then let $g' = j(g) \in G/K$, so there exists $h \in H$ such that $j(h) = g'$, hence $j(h^{-1}g) = e$, but that means $h^{-1}g \in \ker(j)$, therefore $h^{-1}g \in \operatorname{im}(i)$, so $h^{-1}g \in K$. In particular, we have $g = h \cdot h^{-1}g \in H \cdot K$. Collecting these properties, we know $G \cong H \ltimes K$.

□

Problem 2. Since d is a greatest common divisor of a and b in D, then $\gcd(a,b) \in D$ is unique up to multiplication of units. Since D is a PID, then the ideal $\langle a,b\rangle_D \subseteq D$ can be generated by one element, and we obviously have $\langle d\rangle_D = \langle a,b\rangle_D$, so the ideal $\langle a,b\rangle$ with elements $xa+yb$ is generated by the greatest common divisor. Now we have $\langle a,b\rangle_R = \langle a,b\rangle_D \cdot R = dD \cdot R = dR$, so the ideal of R generated by both a and b is still generated by $d \in E$. In particular, the R-linear combination of a and b is principal. Therefore, this is generated by the greatest common divisor of a and b in E, hence this would be d since the greatest common divisor is unique up to multiplication of units. □

Problem 3. By the elementary row/column operations we have row vectors $(1,0,0)$ and $(0,1,0)$, therefore the quotient is isomorphic to $\mathbb{Z}$. □

Problem 4. (a) Note that $u = \frac{\sqrt{3}}{2} + \frac{1}{2}i$. We know u is a primitive 12th root of unity, so we know u is some root of $x^{12}-1$. We have

$$x^{12}-1 = (x^6-1)(x^6+1),$$

and note that u is not a 6th root of unity, so u is a root of x^6+1, and now we have $(x^2+1)(x^4-x^2+1)$, and u is not a root of x^2+1, so u is a root of x^4-x^2+1. We claim that x^4-x^2+1 is irreducible. Indeed, by rational root theorem we know it has no rational roots, and suppose we have a factorization $x^4-x^2+1 = (x^2+ax+b)(x^2+cx+d)$, then $a+c=0$, hence $b-a^2+d=-1$, $ad-ab=0$, and $bd=1$, therefore either $a=0$ or $b=d$. If $a=0$, then $b+d=-1$ and $bd=1$, which is not possible. Therefore we must have $b=d$, and since $bd=1$, then $b=d=\pm 1$, but either way we have a contradiction. Therefore, x^4-x^2+1 is irreducible with u as a root, therefore this is the minimal polynomial of u, so $\mathbb{Q}(u)/\mathbb{Q}$ is a field extension of degree 4.

(b) Since u is algebraic over F, then $[F(u):F]$ is of odd degree. We have an intermediate field extension $F(u)/F(u^2)/F$, but that means

$$[F(u):F] = [F(u):F(u^2)] \times [F(u^2) \times F]$$

is odd. Suppose $F(u) \neq F(u^2)$, then $u \notin F(u^2)$, so we know $[F(u):F(u^2)] = 2$ since u is a root of x^2-u^2 over $F(u^2)$, but this is impossible since the degree should be odd. Hence, we have $F(u) = F(u^2)$, and in particular $E = F(u^2)$.

□

Problem 5. By the rational root theorem, this polynomial has no roots over $\mathbb{Q}$, so this is an irreducible polynomial. Now the derivative is non-zero, so the polynomial is separable. Hence, any splitting field gives a Galois extension. The discriminant of a polynomial x^3+ax+b is $-4a^3-27b^2$, so the discriminant of $g(x)$ is $256-27=229$, which is not a square. Since the discriminant is not a square, then the Galois group, which is already embedded in S_3, is not contained in A_3, therefore it must be S_3. □

16 May 2016

Problems

Problem 16.1. Classify (up to isomorphism) the finite groups G that are both solvable and simple.

Problem 16.2. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear transformation which is represented relative to the canonical basis by the matrix:

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & -1 \\ 1 & 0 & -2 \end{pmatrix}$$

Consider on $\mathbb{R}^3$ the $\mathbb{R}[x]$-module structure defined by T. Show that there exists $p_0(x) \in \mathbb{R}[x]$ and an isomorphism of $\mathbb{R}[x]$-modules $\mathbb{R}^3 \cong \mathbb{R}[x]/\left\langle p_0(x) \right\rangle$.

Problem 16.3. Recall that a real number is *algebraic*, if it is the root of some polynomial $p(x) \in \mathbb{Q}[x]$. Show that the set $A \subseteq \mathbb{R}$ of real algebraic numbers is an algebraic extension of $\mathbb{Q}$. What is $\dim_{\mathbb{Q}}(A)$?

Problem 16.4. Given examples of:

(a) a commutative ring with 1 that is not an integral domain,

(b) an integral domain that is not a UFD,

(c) a UFD that is not a PID,

(d) a prime ideal that is not maximal,

(e) an ideal that is not prime.

Justify, for each of your examples, that it has the properties claimed.

Problem 16.5. Compute the Galois group of $g(x) = x^3 - 4x + 1 \in \mathbb{Q}[x]$.

Solutions

Problem 1. Since G is simple, then the only normal subgroups are G and $\{e\}$. In particular, $[G, G]$ is a normal subgroup, hence it is either G or $\{e\}$. Suppose $[G, G] = G$, then the corresponding derived series never terminates at $\{e\}$, hence G is never solvable, contradiction. Therefore, we must have $[G, G] = \{e\}$, therefore G is abelian, which implies nilpotence and therefore solvable. Therefore, we just need to classify all finite abelian groups, but by the structure theorem this is just

$$\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{k_n}\mathbb{Z}$$

for some positive integer n, distinct primes p_i's, and positive integers k_i's. □

Problem 2. The characteristic polynomial is $f(x) = -x^3 - 2x^2 + x - 1$, and this is not irreducible over $\mathbb{R}$ since complex roots occur in pairs. (Using calculus knowledge, there is some real root. If we use enough techniques, we will probably see that there is a real root and a pair of complex conjugates.) Therefore, the polynomial $f(x)$ either

- factors into a linear term and a quadratic term, i.e., with a pair of complex roots, or
- splits in $\mathbb{R}$, i.e., has three real roots.

It suffices to show that $f(x)$ is separable, i.e., has no repeated roots, then we know the set of invariant factors of $f(x)$ has one element regardless. If we have a real root and a pair of complex conjugates, then the claim is obvious. If we have three real roots, then the polynomial splits in $\mathbb{R}$, so having repeated roots means $\gcd(f(x), f'(x)) \neq 1$. We calculate that the roots of $f'(x)$ are $\frac{-2\pm\sqrt{7}}{3}$, so for $\gcd(f(x), f'(x)) \neq 1$ we must have one of the roots to be a root of $f(x)$, which is not the case. Therefore, the polynomial has no repeated roots, and we are done. In particular, the set of invariant factors has one element, so by the factorization we know $\mathbb{R}^3 \cong \mathbb{R}[x]/f(x)$ as desired. □

Problem 3. In general, we have the following setting: let L/F be a field extension and let K be the set of algebraic elements of L over F, then K/F is a field extension and is algebraic. There is a constructive proof in January 2018, Problem 4 (Problem 11.4), part (b). Alternatively, let $a, b \in K$ be algebraic elements of L over F, then $a+b$ and ab are elements in $F(a,b)$. By construction, b is a root of some polynomial in $F[x]$, so it is still a root of some polynomial in $F(a)[x]$, therefore b is algebraic over $F(a)$, hence $[F(a,b) : F(a)]$ is finite. But $[F(a) : F]$ is also finite since a is algebraic over F, so $[F(a,b) : F]$ is also finite, hence indicating $F(a,b)/F$ is a finite field extension, therefore this is algebraic. In particular, both $a+b$ and ab are algebraic elements. Since this is true for arbitrary $a, b \in K$, then this is true for all elements of K, hence K/F is a field extension by closure, and is algebraic by construction.

Note that every $n+1$ elements in $\mathbb{Q}$ gives a polynomial of degree n in $\mathbb{Q}[x]$, and since a countable union of countable sets is countable, then we know $\mathbb{Q}[x]$ is countable, and since each polynomial of degree n in $\mathbb{Q}[x]$ gives at most n distinct roots in $\mathbb{Q}$, then the set of algebraic real numbers is also countable. To see that the dimension over $\mathbb{Q}$ is not finite, note that we have an infinite family of independent algebraic elements given by $\sqrt{2}$, $\sqrt{\sqrt{2}}$, $\sqrt{\sqrt{\sqrt{2}}}$, and so on. This gives a $\mathbb{Q}$-vector space of infinite dimension. □

Problem 4. (a) $\mathbb{Z}/4\mathbb{Z}$ is obviously a ring with the usual operations, but note that $[2]+[2]=[0]$ in $\mathbb{Z}/4\mathbb{Z}$, so $[2]$ is a non-zero zero divisor, hence this is not an integral domain.

(b) $\mathbb{Z}[\sqrt{-5}]$ is an integral domain: if $(x_1+y_1\sqrt{-5})(x_2+y_2\sqrt{-5})=0$, then taking the norm on both sides shows that this forces one of them to be zero. To see this is not a UFD, we have $(2+\sqrt{-5})(2-\sqrt{-5}) = 9 = 3\times 3$, where all of them are irreducible elements.

(c) $\mathbb{Z}[x]$ is a UFD: since $\mathbb{Z}$ is a UFD, then so is $\mathbb{Z}[x]$. But $\mathbb{Z}[x]$ is not a PID: the ideal $\langle 2, x\rangle$ is not principal in $\mathbb{Z}[x]$.

(d) The ideal (0) is prime in $\mathbb{Z}$: if $xy \in (0)$, then $xy = 0$, so either $x = 0$ or $y = 0$. However, (0) is not maximal: every other prime ideal of $\mathbb{Z}$ contains (0).

(e) The ideal (4) is not prime in $\mathbb{Z}$: $2\times 2 = 4 \in (4)$, but $2 \notin (4)$.

□

Problem 5. This is August 2016, Problem 5 (Problem 15.5). □

17 January 2016

Problems

Problem 17.1. Prove that a group of order $25 \cdot 7 \cdot 17$ must be solvable.

Problem 17.2. Let $n \geq 3$ and let T denote the set of 2-element subsets of $\{1, 2, \ldots, n\}$. For $\sigma \in A_n$ and $\{i, j\} \in T$, let $\sigma(\{i, j\}) = \{\sigma(i), \sigma(j)\}$.

(a) Show that this defines an action of A_n on T.

(b) Is this action of A_n on T transitive?

Problem 17.3. Make $\mathbb{C}^3$ into a $\mathbb{C}[x]$-module by $f(x)v = f(M)v$ where $v \in \mathbb{C}^3$ and

$$M = \begin{pmatrix} 3 & 2 & 0 \\ 0 & 3 & 0 \\ 0 & 1 & 7 \end{pmatrix}.$$

Find polynomials $p_i(x)$ and exponents e_i such that $\mathbb{C}^3 \cong \bigoplus_i \mathbb{C}[x]/(p_i^{e_i})$ as $\mathbb{C}[x]$-modules. Justify your answer.

Problem 17.4. Compute the Galois group of $g(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$.

Problem 17.5. Let k be a field of characteristic $p > 0$ and let $f = x^p - x + a \in k[x]$. Suppose that $f(x)$ has no roots in k. Prove that then f is irreducible over k.

Solutions

Problem 1. Let G be a group order $5^2 \cdot 7 \cdot 17 = 25 \cdot 7 \cdot 17$. Let n_5 be the number of Sylow 5-subgroup, then $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 119$, so we see $n_5 = 1$, hence G has a normal subgroup N of order 25. This is a p-group, so this is solvable. Also, G/N is a group of order $119 = 7 \cdot 17$, so this is solvable as well. Therefore, G is solvable. □

Problem 2. (a) First note that this defines a map $A_n \times T \to T$. We now show the two properties. Take $e \in A_n$, then we have $e = (\,)$, so for any $\{i, j\} \in T$, we have $e \cdot \{i, j\} = \{i, j\}$ by definition. Moreover, let $g_1, g_2 \in A_n$ be two even permutations, and let $\{i, j\} \in T$. We have

$$\begin{aligned} g_1 g_2 \cdot \{i, j\} &= \{g_1 g_2(i), g_1 g_2(j)\} \\ &= g_1 \cdot \{g_2(i), g_2(j)\} \\ &= g_1 \cdot (g_2 \cdot \{i, j\}) \end{aligned}$$

by definition. Therefore, this defines a group action indeed.

(b) Suppose we have $i_1 \neq i_2$ and $j_1 \neq j_2$, and we want to find some $\sigma \in A_n$ such that $\sigma(i_1) = i_1$ and $\sigma(i_2) = j_2$. If the two sets are identical, then we just take $\sigma = (\,)$; if there is one overlapping element, say $i_1 = j_1$, then we take $\sigma = (i_1\ j_2)(i_2\ j_1)$; if there is no overlapping element, then we just give any product of two transpositions. Any way, we have an even permutation. Hence, this action is transitive.

□

Problem 3. Note that the characteristic polynomial of M is $c(x) = (3-x)^2(7-x)$. The minimal polynomial is the largest invariant factor and should contain all roots, so it is either $c(x)$ or $(3-x)(7-x)$. We note that M is not a root of $(3-x)(7-x)$, but is a root of $c(x)$, so the minimal polynomial is just the characteristic polynomial, hence it is the only invariant factor. Therefore, the module structure is given by

$$\mathbb{C}^3 \cong \mathbb{C}[x]/(3-x)^2(7-x).$$

□

Problem 4. By rational root theorem, $g(x)$ has no root over $\mathbb{Q}$, so this is irreducible. It has non-zero derivative, so this is separable, and so any splitting field gives a Galois extension. Because the polynomial is separable and irreducible, the Galois group is transitive as a subgroup of S_3. Moreover, the discriminant of the polynomial is $81 = 9^2$, so the Galois group is contained in A_3, and since the Galois group would not be trivial, this forces the Galois group to be A_3. □

Problem 5. This is similar to August 2020, Problem 4 (Problem 4.4) part (b) and August 2019, Problem 5 (Problem 6.5) part (b). □

18 August 2015

Problems

Problem 18.1. Let G be a group of order $5 \cdot 13 \cdot 43 \cdot 73$. Determine the number of elements of order 5.

Problem 18.2. Let G be a finite group and N a normal subgroup of G. Prove or disprove:

(a) G is nilpotent if and only if both N and G/N are nilpotent.

(b) G is solvable if and only if N and G/N are solvable.

Problem 18.3. Let R be an integral domain. Let $f \in R[x]$ be a non-zero polynomial such that there exist a non-zero $d \in R$ and polynomials $g, h \in R[x]$ of degree less than f such that $df = gh$.

(a) Show that if R is a unique factorization domain then f is the product of two polynomials in $R[x]$ of degree less than f.

(b) Use part (a) with $f = x^2 - 5$ to show that $\mathbb{Z}[\sqrt{20}]$ is not a unique factorization domain.

Problem 18.4. Let G be a finite group. Show that there exist fields L and K such that L is an extension of K with Galois group G.

Solutions

Problem 1. By Sylow Theorem, the number of Sylow 5-subgroup n_5 satisfies $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 13 \cdot 43 \cdot 73$, so n_5 is a number that ends with digit 1 or 6, which is only possible if $n_5 = 1$. Hence, we have a unique Sylow 5-subgroup. Each element of order 5 generates a subgroup of order 5, but there is only one of them, so every element of order 5 is contained in this subgroup, hence there are 4 of them. □

Problem 2. (a) This is false. We know that if G is nilpotent, then any subgroup and quotient group should be nilpotent as well, hence N and G/N are both nilpotent. However, given a group G and $N \lhd G$, if N and G/N are nilpotent, we may not have G to be nilpotent. Indeed, let $G = S_3$, and let N be generated by a 2-cycle, so N is nilpotent; G/N has order 3 and is nilpotent as well. However, S_3 is not nilpotent, since it is not a direct product of p-groups: that would mean we have $S_3 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$.

Alternatively, if such thing exists, then we have a normal series, so $G_{n-1}/G_n \subseteq Z(G/G_n)$ for some $G_n = \{e\}$, but now $G = S_3$ has trivial center, so $G_{n-1} = G_n = \{e\}$, then proceeding inductively, we have $G = \{e\}$, contradiction.

(b) This is true. Suppose G is solvable, then we have a normal series of $G_i = [G_{i-1}, G_{i-1}]$ that terminates at $\{e\}$. Now define $N_i = N \cap G_i$, then this gives a normal series of $N_i \lhd N_{i-1}$ by the second isomorphism theorem, and $[N_i, N_i] \subseteq [G_i, G_i] \cap N \subseteq G_{i+1} \cap N \subseteq N_{i+1}$, therefore N_i/N_{i+1} is abelian, and terminates in the trivial group, so N is solvable. We now show that G/N is also solvable. Indeed, we have $G/N = GN/N = G_0N/N \rhd G_1N/N \rhd \cdots \rhd N/N = \{e\}$ which terminate at the trivial group, and each time we have $G_{i+1}N/N \supseteq [G_iN/N, G_iN/N]$ by construction. Therefore, G/N is solvable as well.

Now suppose $N \lhd G$ is such that N and G/N are both solvable. Let $N_0 \rhd N_1 \rhd \cdots \rhd N_m$ be the normal series of N, and let $F_0 \rhd F_1 \rhd \cdots \rhd F_n$ be the normal series of G/N. Given the canonical map $\pi : G \to G/N$, we have a series of preimages $G_i = \pi^{-1}(F_i)$, then by the correspondence theorem we know this gives another normal series. In particular, $G_n = \pi^{-1}(F_n) = \pi^{-1}(\{e\}) = N$. We also note that $G_i \to F_i$ has kernel N for all i, so we have $F_i \cong G_i/N$, and we know $F_i/F_{i+1} \cong (G_i/N)/(G_{i+1}/N)$, so by the third isomorphism theorem this is G_i/G_{i+1}. Hence, we have a normal series with abelian quotient:

$$G_0 \rhd G_1 \rhd \cdots \rhd G_n = N = N_0 \rhd N_1 \rhd \cdots \rhd N_m.$$

Therefore, G is solvable.

□

Problem 3. (a) Since R is a UFD, then let $h = d'h'$ for $d' \in R$ and $\deg(h') = \deg(h)$ such that h' is primitive. We have $h' \mid df$ over the field of fractions F of R. In this case, $d \in R$ is a unit over F, so we have $h' \mid f$. But since h' is primitive, R is a UFD, and $h' \mid f$ in $F[x]$, then $h' \mid f$ in $R[x]$. Therefore, we have $f = g'h'$ for some $g' \in R[x]$. Since $0 < \deg(h') = \deg(h) < \deg(f)$, then so is $\deg(g)$, and therefore this is a proper factorization.

(b) Let $d = 20 \in \mathbb{Z}[\sqrt{20}]$, then $df = 20(x^2-5) = 20x^2 - 100 = (\sqrt{20}x+10)(\sqrt{20}x-10)$, which is a proper factorization in $\mathbb{Z}[\sqrt{20}]$. Suppose $\mathbb{Z}[\sqrt{20}]$ is a UFD, then by part (a) we know that $f(x) = x^2 - 5$ should have a proper factorization as well, namely $x^2 - 5 = (x-a)(x+b)$ for some $a, b \in R$, so that means the two roots of $f(x)$ should be in $\mathbb{Z}[\sqrt{20}]$. By calculation have the two roots to be $\pm\sqrt{5} \notin \mathbb{Z}[\sqrt{20}]$, contradiction.

□

Problem 4. Since G is a finite group, then for some large enough prime p we have an embedding $G \hookrightarrow S_p$, so we regard every element of G as a permutation.

We claim that there exists an irreducible polynomial f of degree n such that it has $n-2$ real roots and a pair of complex conjugates. If such polynomial f exists, then say $n = p$, its splitting field $\mathbb{Q}_f$ contains $\mathbb{Q}(a)$ where a is a root of f. Since $n = p \geq 2$, then f' is non-zero, and since f is irreducible, then f is separable and $\mathbb{Q}_f/\mathbb{Q}$ is a Galois extension. Now p divides $[\mathbb{Q}_f : \mathbb{Q}]$, so the Galois group G_f must contain a p-cycle, and since f only has a pair of complex conjugates as roots, then G_f contains a 2-cycle, now since $\gcd(p, 2) = 1$, therefore $G_f = S_p$. (Alternatively, this is proven in May 2018, Problem 5 (Problem 10.5), part (b).)

To prove this claim, we note that by algebraic number theory, if $\varphi(x) \in \mathbb{R}[x]$ has n distinct roots, then there exists $\varepsilon > 0$ such that $\varphi(x) + a$ has exactly n real roots for any real number $|a| < \varepsilon$. Therefore, we look at $\varphi(x) = (x^2 + m)(x-k_1)\cdots(x-k_{n-2})$ for even integers $m, k_1, \ldots, k_{n-2}$, then for a good choice of $\frac{a}{b}$ by above we know $\varphi(x) + \frac{a}{b}$ has exactly $n-2$ real roots. Therefore, $b\varphi(x) + a$ has $n-2$ real roots and a pair of complex roots. In particular, let $\varphi(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, then by the construction above we note that all a_i's are even integers. Let b be odd, $a = 2$, and prime $q = 2$, then $bf(x) + a$ satisfies $q \mid ba_0 + a$, $q \mid ba_i$ for $i = 1, \ldots, n-1$, $q \nmid a_n$, and $q^2 \nmid ba_0 + a$. Therefore, by Eisenstein criterion with respect to $q = 2$, we know $bf(x) + a$ is an irreducible polynomial of degree n over $\mathbb{Q}$, with exactly $n-2$ real roots.

Let $\mathbb{Q}_G$ be the fixed field of $G \subseteq S_p$ over $\mathbb{Q}$, then by the Galois correspondence, we know $\mathbb{Q}_f/\mathbb{Q}_G$ is Galois, therefore G is the Galois group of this field extension. In particular, let $L = \mathbb{Q}_f$ and $K = \mathbb{Q}_G$, then G is the Galois group of this extension L/K. □

19 May 2015

Problems

Problem 19.1. (a) Give the definition of a nilpotent group in terms of its upper central series.

(b) Show that every p-group is nilpotent.

Problem 19.2. Show that A_5 does not contain a group of order 15.

Problem 19.3. (a) Show that any finite integral domain must be a field.

(b) Is the polynomial $p(x) = x^6 + x^3 + 1$ irreducible in $\mathbb{Z}[x]$?

Problem 19.4. Find the Galois group of the polynomial $p(x) = x^3 + 6x^2 - 9x + 3 \in \mathbb{Q}[x]$.

Solutions

Problem 1. (a) A nilpotent group is in fact one with a central series, i.e., a normal series $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$ where each $G_i \lhd G$, and $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$.

A lower central series is a normal series given by $G_0 = G$ and $G_i = [G_{i-1}, G] \lhd G$ (that does not necessarily terminates at $G_n = \{e\}$).

An upper central series is a normal series given by $G_0 = \{e\}$, $G_1 = Z(G)$, and for $n \geq 1$, G_n is the unique normal subgroup of G such that $G_n/G_{n-1} \cong Z(G/G_{n-1})$, i.e., we have $G_i \lhd G$ such that $G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots$ (that does not necessarily reaches $G_n = G$ at some point).

Under these definitions, a nilpotent group is, equivalently:

- a group with a central series,
- a group with an upper central series that terminates at $G_n = G$,
- a group with a lower central series that terminates at $G_n = \{e\}$,
- a group that is the internal direct product of its Sylow subgroups.

(b) Following the definition above, we will find an upper central series that terminates at a p-group G. Let $G_0 = \{e\}$ and $G_1 = Z(G)$, and construct G_i inductively. Note that $Z(G)$ is non-trivial since G is a p-group. Suppose we have $G_i \neq G$, then G/G_i has to be a p-group, therefore it has non-trivial center $Z(G/G_i)$, so there exists a unique subgroup G_{i+1} that strictly contains G_i. Therefore, we have $G_{i+1} \supsetneq G_i$ unless $G_i = G$ already. Since G is a p-group, with order p^n, then the process above shows that it terminates at most at G_n, therefore this is an upper central series that terminates at G, therefore G is nilpotent, and so all p-groups are nilpotent.

□

Problem 2. Suppose, towards contradiction, that A_5 contains a subgroup G of order 15. By Sylow Theorem, G has a unique Sylow 3-subgroup and a unique Sylow 5-subgroup, so G is the internal product of these two subgroups, hence $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$. In particular, let the elements of G be denoted at $1, x, \ldots, x^{14}$. By Cauchy's Theorem, there exists some element y of order 2 in A_5, and obviously $y \notin G$. Therefore, we claim that there is now a subgroup of A_5 with order 30, namely $\langle x, y\rangle \subseteq A_5$, with elements $1, x, \ldots, x^{14}, y, xy, \ldots, x^{14}y$. To show that the group has order 30, it suffices to show that all elements are distinct. Indeed, if $x^a y^b = x^c y^d$, then we have $x^m y^n = 1$ for some integers

m, n. If $n = 0$, we must have $m = 0$; if $n = 1$, we must have $x^m = y$, but this is not possible. Therefore, we have a subgroup of order 30, which is normal in A_5 since it has index 2. But this is a contradiction since A_5 is simple.

Alternatively, the action of A_5 on A_5/G gives a homomorphism $A_5 \to S(A_5/G) = S_4$, but A_5 is simple, and since the action is non-trivial, we note that the kernel of this map is zero, so the image of this homomorphism is isomorphic to A_5, contradiction. □

Problem 3. (a) Let R be a finite integral domain and consider arbitrary $0 \neq x \in R$. Since R is finite, then there must exist some positive integers $n > m > 0$ such that $x^n = x^m$, so this forces $x^{n-m} = 1$ by the cancellation law on the domain R, therefore x^{n-m-1} is an inverse of x, which means every non-zero element in R is invertible, hence R is a domain by definition.

(b) By taking $x = y + 1$, we know the polynomial is equivalent to $y^6 + 6y^5 + 15y^4 + 21y^3 + 18y^2 + 9y + 3$, so by Eisenstein criterion we know the polynomial is irreducible over $\mathbb{Q}$. Since the polynomial is primitive, then this implies the polynomial is irreducible over $\mathbb{Z}$ as well.

□

Problem 4. By the Eisenstein criterion, $f(x)$ is irreducible over $\mathbb{Q}$. Therefore, the splitting field gives a Galois extension. Moreover, this is separable since it has non-zero derivative, and so the Galois group must be transitive so it is either A_3 or S_3. We need to calculate the discriminant by some change of variables. We take $y = x + 2$, so $y^3 = x^3 + 6x^2 + 12x + 8$, therefore $f(x)$, when expressed in terms of y, is the polynomial $y^3 - 21x - 5 = y^3 - 21y + 37$. Therefore, the discriminant is $-4(-21)^3 - 27(37^2) = 81$, which is a square, therefore the Galois group has to be contained in A_3, therefore the Galois group is just A_3. □

20 January 2015

Problems

Problem 20.1. Let G be a finite group with center $C(G)$. Show that G is nilpotent if and only if there exists a subgroup $A \subseteq C(G)$ such that G/A is nilpotent.

Problem 20.2. Let $p \leq q$ be odd primes. Show that a group of order $2pq$ is solvable.

Problem 20.3. (a) Show that $\mathbb{Z}[\sqrt{10}]$ is not a unique factorization domain.

(b) Is the polynomial $p(x) = x^3 - 4ix^2 + 16x - (1+3i)$ irreducible in $\mathbb{Z}[i][x]$?

Problem 20.4. Show that an irreducible quartic polynomial $f(x) \in \mathbb{Q}[x]$ with exactly two real roots has Galois group $G \cong S_4$ or $G \cong D_8$.

Solutions

Problem 1. Suppose G is nilpotent, then any quotient group of G is nilpotent, and since $C(G) \lhd G$, then the quotient group $G/C(G)$ is nilpotent. Now suppose $G/C(G)$ is nilpotent, we claim that G is also nilpotent. By the correspondence theorem, we have a central series $G/C(G) = G_0/C(G) \supseteq G_1/C(G) \supseteq \cdots G_n/C(G) = \{e\}$ of groups that terminates, where $C(G) \lhd G_i$ for all i, so $G_i/C(G) \lhd G/C(G)$ is a normal subgroup, and $(G_i/C(G))/(G_{i+1}/C(G)) \subseteq C((G/C(G))/(G_{i+1}/C(G)))$. By the third isomorphism theorem, we have $G_i/G_{i+1} \subseteq C(G/G_{i+1})$ for all i, and this gives $G = G_0 \supseteq G_1 \supseteq \cdots G_n = C(G)$ as a series where $G_i \lhd G$ for all i. Now take $G_{n+1} = \{e\}$, then $G_n/G_{n+1} = C(G) = C(G) = C(G/G_{n+1})$, so by definition we have a central series, so G is nilpotent. □

Problem 2. If $p = q$, we have a group of order $2p^2$. Therefore, a Sylow p-subgroup of order p^2 has index 2, therefore it is normal. In particular, we know this subgroup is solvable since it is a p-group, with a quotient group of order 2, which is also solvable, so the group itself is solvable.

It suffices to show that a group G of order $2pq$ is not simple. That is, we want to show that there is a unique Sylow a-subgroup N for some prime a. Therefore, this Sylow subgroup N is normal, and so G/N is a group of order bc for some primes b and c, which is also solvable, so G is solvable.

Suppose that none of the Sylow subgroups are normal. Note that the number of Sylow q-subgroups n_q satisfies $n_q \equiv 1 \pmod{q}$ and $n_q \mid 2p$, so $n_q = 1, 2, p, 2p$, but $q > p > 2$, so $n_q = 2p$. We have $2p(q-1) = 2pq - 2p$ elements of order q[1]. We now look at Sylow p-subgroups, then by the same reasoning we know $n_p \geq q$. Suppose it is q, then we have at least $q(p-1) = pq - q$ elements of order p; similarly, there are $n_2 \geq p$ Sylow 2-subgroups, so there are at least p elements of order 2. In total, we have accounted for $2pq - 2p + pq - q + p = 3pq - p - q$ distinct non-trivial elements, but $pq = (p-1)q + q > p + q$, so $3pq - p - q > 2pq$, contradiction. Therefore, we have some normal Sylow subgroup here. □

Remark 20.1. In fact, one can show that for a group G of order pqr where $p < q < r$ are primes, there is a unique Sylow r-subgroup. Indeed, we know there exists some normal Sylow subgroup already, so it should be of order q or p.

Suppose we have a normal Sylow q-subgroup N, then G/N has order pr, so it has a normal Sylow q-subgroup. In particular, there is a normal Sylow r-subgroup of G/N, so by the correspondence theorem we know there exists a normal subgroup $N \subseteq H \subseteq G$ such that H/N has order r. Hence H has order qr, and therefore it contains a normal subgroup

[1] Note that Sylow subgroups are not necessarily intersecting trivially, but since they are all groups of order q, then if there is a non-zero element in the intersection, then it generates both subgroups, so they should be the same group.

P of order r. We now show that $P \lhd G$. Indeed, for any $g \in G$, we have $|gPg^{-1}| = r$ and $gPg^{-1} \subseteq H \lhd G$, then note that P is the unique Sylow r-subgroup of H, so $gPg^{-1} = P$, hence by definition $P \lhd G$.

Analogously, we can construct a normal Sylow r-subgroup if the normal subgroup has order p.

Problem 3. (a) Note that $\sqrt{10} \cdot \sqrt{10} = 10 = 2 \cdot 5$. We claim that $2, 5$ are both irreducible elements. Since the norm of every element $a + b\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$ is $a^2 - 10b^2$ which is an integer, and that the norm of an element is ± 1 if and only if it is a unit. Therefore, a non-unit factorization of 2 with norm 4 must have norm ± 2 and ± 2, but an element of norm ± 2 gives $a^2 - 10b^2 = \pm 2$, so $a^2 \equiv \pm 2 \pmod{10}$, but there is no square that ends with digit 2 or 8, contradiction. Hence, 2 has to be irreducible. Similarly, 5 has to be irreducible: a non-unit factorization has norm ± 5 and ± 5, so $a^2 - 10b^2 = \pm 5$, so $5 \mid a$, and if $a = 5k$ we must have $25k^2 - 10b^2 = \pm 5$, and so $5k^2 - 2b^2 = \pm 1$, therefore $b^2 \equiv 2, 3 \pmod{5}$, which means it ends with digit $2, 3, 7, 8$, and none of them is possible. Hence, we see that $2 \cdot 5$ is an irreducible factorization already. Now we just have to show that $2 \nmid \sqrt{10}$. Say $2u = \sqrt{10}$ for some $u = a + b\sqrt{10}$, then $a = 0$ and $2b = 1$, so $b \notin \mathbb{Z}$, contradiction. Therefore, $2 \nmid \sqrt{10}$. Therefore, the factorization of $\sqrt{10} \cdot \sqrt{10}$ do not contain 2 up to multiplication of unit, so we have two different factorizations.

(b) Note that $1 + 3i = (1 + i)(2 + i)$. We claim that $1 + i$ is a prime element in $\mathbb{Z}[i]$, but every prime is irreducible in the UFD $\mathbb{Z}[i]$, so it suffices to show $1 + i$ is irreducible. Suppose $(a + bi)(c + di) = 1 + i$, then taking the norm on both sides give $(a^2 + b^2)(c^2 + d^2) = 2$, and since an element is a unit if and only if norm is 1, and a norm must be an integer, so this forces one of the elements to have norm ± 1, therefore hence we know $1 + i$ is irreducible and therefore prime. By the generalized Eisenstein criterion, since $1 + i$ is irreducible and not a unit, so $1 + i \nmid 1$, and since $1 + i \mid 1 + 3i$, $1 + i \mid 2 \mid 4 \mid 4i$, and $4i \mid 16$, then we know $1 + i$ divides all coefficients except the leading one. Finally, we claim that $(1 + i)^2 = 2i \nmid 1 + 3i$ in $\mathbb{Z}[i]$. Indeed, if $2i(a + bi) = 1 + 3i$, then $2a = 3$, so $a \notin \mathbb{Z}$, contradiction. Therefore, by Eisenstein criterion, we know the polynomial is irreducible over $\mathbb{Q}[i]$, the field of fractions of the UFD $\mathbb{Z}[i]$. Also note that the polynomial is primitive with leading coefficient 1, so being irreducible in the field of fractions $\mathbb{Q}[i]$ implies being irreducible in the field of fractions $\mathbb{Z}[i]$. Therefore, the polynomial is irreducible indeed.

□

Problem 4. Since $f(x)$ is an irreducible quartic, then it must be separable, and its Galois group must be a transitive subgroup of S_4, which is either $\mathbb{Z}_4$, V_4 (this needs to be the subgroup generated by $(1\ 2)$ and $(3\ 4)$, NOT generated by three pairs of disjoint 2-cycles), D_4, A_4, or S_4. Since f has exactly two real roots, then it has exactly two complex roots, therefore complex conjugation must be part of the Galois group. In particular, that means the Galois group has a transposition. Therefore, it must be either D_4 or S_4 since a transposition is an odd permutation. □

21 August 2014

Problems

Problem 21.1. Let G be the unique simple group of order 168. Determine the number of elements of order 7.

Problem 21.2. Let G be a finite group, let P be a Sylow p-subgroup of G and let $H = N_G(P)$ be the normalizer of P in G. Show that, for all $g \in G$, $gHg^{-1} = H$ if and only if $g \in H$.

Problem 21.3. (a) Prove that in a unique factorization domain R, an element x is irreducible if and only if it is prime.

(b) Give an example of a commutative ring R and an element $x \in R$ such that x is irreducible but not prime.

Problem 21.4. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible quartic polynomial with splitting field extension $L/\mathbb{Q}$.

(a) List the possible degrees for the extension $L/\mathbb{Q}$ and for each degree the possible Galois groups of the extension.

(b) Let $f(x)$ have the property that $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$, for any two distinct roots α and β of $f(x)$. Determine the Galois group of $L/\mathbb{Q}$.

Solutions

Problem 1. Note that every element of order 7 must be contained in a Sylow 7-subgroup, namely a group of order 7. By Sylow Theorem, we know the number of Sylow 7-subgroup n_7 satisfies $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 24$, so $n_7 = 1, 8$. Since the group is simple, then $n_7 \neq 1$, so $n_7 = 8$. Since a Sylow 7-subgroup has order 7, then each Sylow group contains 6 elements of order 7, so in total there are $6 \times 8 = 48$ elements of order 7. Note that all Sylow subgroups here are intersecting trivially: if x is a non-trivial element contained in two Sylow subgroups, then since the group has order 7, every non-trivial element generates the group, hence both Sylow subgroups are equivalent to $\langle x \rangle$, namely they are the same group. □

Problem 2. By definition of normalizer, we have $N_G(P) = \{g \in G : gPg^{-1} = P\}$. Therefore, we want to show that $N_G(N_G(P)) = N_G(H)$ is just H. Obviously $H \subseteq N_G(H)$, so we show that $N_G(H) \subseteq H$. Suppose $g \in N_G(H)$ is an element such that $gHg^{-1} \subseteq H$. Recall that $H = N_G(P) \rhd P$, so P is the unique Sylow p-subgroup of H, therefore any automorphism in H, sending a Sylow p-group to another Sylow p-group, must fixes P. In particular, the conjugation action is an inner automorphism and therefore an automorphism, hence g normalizes P, therefore $N_G(H) \subseteq N_G(P) = H$ by definition. Hence, $H = N_G(H)$, as desired. □

Problem 3. (a) In any domain, a prime element is irreducible: let p be a prime element and suppose $p = ab$ is a decomposition, then $p \mid ab$, therefore either $p \mid a$ or $p \mid b$; say $p \mid a$, then $a = pc$ for some c, therefore $p = ab = pcb$. In particular, $cb = 1$; similarly, $bc = 1$, so b is a unit, hence p is irreducible.

We now show that in a UFD every irreducible element is prime. Suppose c is irreducible, and suppose $c \mid ab$ for some elements a, b, then we have $ab = cd$ for some element d. Taking the unique factorization, we have $a = a_1 \cdots a_m$, $b = b_1 \cdots b_n$, and $d = d_1 \cdots d_l$, so we must have $c \sim a_i$ or $c \sim b_j$ for some i or j. In particular, either $c \mid a$ or $c \mid b$, so c is prime.

(b) In $\mathbb{Z}[\sqrt{-5}]$, we claim that 2 is irreducible but not prime. Suppose $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$, then taking the norm on both sides we see $(a^2 + 5b^2)(c^2 + 5d^2) = 4$. Suppose we have a non-unit factorization, we must have $a^2 + 5b^2$ and $c^2 + 5d^2$ as 2. This is impossible. Therefore, 2 must be irreducible. However, 2 is not prime; we have $2 \times 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, so $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, but we claim that 2 does not divide either of the elements. If $1+\sqrt{-5}=2(a+b\sqrt{-5})$, then this forces $a=b=\frac{1}{2}$, but now this element is not in $\mathbb{Z}[\sqrt{-5}]$; similar contradiction happens for $1-\sqrt{-5}$. Therefore, 2 is not prime.

□

Problem 4. (a) Since $f(x)$ is a quartic irreducible polynomial, then it is separable over $\mathbb{Q}$, so $L/\mathbb{Q}$ is Galois. Therefore, by the Galois correspondence we know the Galois group G is a transitive subgroup of S_4, so there are five possible candidates, namely S_4, A_4, D_4, V_4, C_4. Since the Galois group has order equals to the degree of the extension, we know the possible degrees of $L/\mathbb{Q}$ are $24, 12, 8, 4$.

(b) Note that the property shows that f has no complex roots: if it does, then we must have at least a pair of complex conjugate, then they should generate the same field extension. By the Galois correspondence, for any root α of f, $\mathbb{Q}(\alpha)/\mathbb{Q}$ should have degree 4 as the minimal polynomial, but $\mathbb{Q}(\alpha)\subsetneq L$, therefore the group has order greater than 4, so the Galois group G is S_4, A_4, or D_4. Since $\mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)=\mathbb{Q}$, then the smallest supergroup of any two subgroups of index 4 is G. If $G=D_4$, then groups of index 4 are either given by transpositions of the form $(1\ 2)$ or product of transpositions of the form $(1\ 2)(3\ 4)$. Either way, there exists two groups among the four of them that is contained in V_4; therefore, $G\ncong D_4$. So G is either S_4 or A_4. If $G=S_4$, then the groups $\mathbb{Q}(\alpha)$'s are S_3's, but S_3's are not contained in A_4 because it is not full of even permutations, so the smallest supergroup containing them is S_4 itself, therefore satisfying the trivial intersection. If $G=A_4$, then the groups $\mathbb{Q}(\alpha)$'s are $A_3\cong\mathbb{Z}/3\mathbb{Z}$'s, namely they are 3-cycles. If the smallest supergroup is not A_4, then it has to be a group of order 6, namely C_6 or S_3; obviously S_4 contains no C_6, so say it is S_3, but again S_3 is not contained in A_4, so the smallest supergroup has to be A_4. This validates both possibilities, so we have Galois group as S_4 or A_4.

□

22 January 2014

Problems

Problem 22.1. Let X be a regular hexagon, that is, a polygon with 6 equal sides and equal angles.

(a) Describe the set of *rigid* symmetries of X. ("Flipping", that is, orientation-reversing symmetries of X, *are* allowed. Hexagon is assumed to be rigid, so we do not allow symmetries that "twist or bend" the hexagon.)

(b) Denote $G = S(X)$ be set of rigid symmetries of X. Prove that $S(X)$ is a group. What is the order of this group? Describe the action of G on X.

(c) Let g be the rotation by $180°$. What is the centralizer of g in G.

(d) Explicitly describe one 2-Sylow subgroup of G.

(e) How many 3-Sylow subgroups does G have? Prove that each of them is normal in G.

(f) List all the Sylow subgroups of G that are normal in G.

(g) Is G solvable?

(h) Is G nilpotent?

(i) Suppose that each side of X can be colored in one color. In how many ways can the sides of the hexagon be colored if one is allowed to use 5 colors arbitrarily? (Possibly with repetitions.) Let $C(X)$ be then set of all possible such colorings of X. Describe the action of G on $C(X)$ induced by the action of G on X.

(j) What is the maximal number of colorings of X (using 5 colors) such that, for any two of them, one cannot be obtained from the other by acting by any element of G?

Problem 22.2. (a) For a unique factorization domain R prove that $p \in R$ is irreducible if and only if (p) is a prime ideal.

(b) Show that the ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Problem 22.3. (a) Let E/F be a Galois extension of degree p^k. Prove that there exists an intermediate field K with $[E : K] = p$ and K/F Galois of degree p^{k-1}.

(b) Determine the splitting field extension $E/\mathbb{Q}$ of the polynomial $x^4 - 2 \in \mathbb{Q}[x]$.

(c) Give an intermediate field K with $[E : K] = 2$ and $K/\mathbb{Q}$ Galois.

Solutions

Problem 1. (a) A rigid symmetry would be a transformation such that the hexagon end up with the same shape, that is, if we label the vertices as $1, \dots, 6$, then the resultant hexagon would be the same with a relabeling of vertices. Such transformations needs 1) to fix a starting point, i.e., where to send 1, and 2) orientation of the transformation, i.e., same as before, or of opposite direction. Therefore, this categorizes all such symmetries as rotations and reflections. Rotations are operations that rotate the hexagon via the center at some angle, such that the label 1 ends up somewhere; reflections are operations that reflects via, either a line through two opposite vertices, or a line through two opposite sides. Therefore, there are 6 rotations, and 6 reflections. This gives a total of 12 rigid symmetries.

(b) Note that after a composition of certain actions above, we know the six vertices are still labelled one after another either clockwise or counterclockwise, and overlapping with the original hexagon entirely, therefore the composition itself is also a rigid symmetry. The identity of the group is obviously the symmetry that does nothing, namely sending 1 to 1, 2 to 2, and so on, without changing the orientation. In particular, all compositions with this rigid symmetry does nothing for obvious reasons, so this is the identity. Finally, for every rigid symmetry, we can undone it by transforming everything backwards, which is also a rigid symmetry because it overlaps with the original hexagon entirely and the vertices are still labelled with well-ordering. Moreover, the composition of these two symmetries is the identity since it does nothing, so every rigid symmetry has an inverse. Therefore, we see that $G = S(X)$ is a group indeed. As we just saw, the group has 12 elements. The action of $G = S(X)$ on X sends the tuple $(1\,2\,3\,4\,5\,6)$, say we order this clockwise, to a reordering of the tuple, given by some rigid symmetry, that describes the order of the vertices in clockwise order again.

By observation, the group $G = D_6 = \langle r, s \mid r^6 = s^2 = 1, rs = sr^{-1}\rangle$. Here we define the hexagon to be labelled by $1, \dots, 6$ clockwise, and r is the clockwise rotation by 60 degrees, s flips the hexagon via the horizontal axis. Every element is now of the form $s^n r^m$.

(c) The centralizer of g is exactly the elements $h \in G$ such that $hg = gh$. Let $h = s^n r^m$, then we want $s^n r^{m+3} = r^3 s^n r^m$. Obviously this works if $n = 0$. If $n = 1$, we have $sr^{m+3} = r^3 sr^m = sr^{m+3}$, therefore this works as well. Hence, the centralizer of g is the entire group $G = D_6$.

(d) A Sylow 2-subgroup would have order 4, so we have $\langle r^3, s\rangle$. Obviously the elements are $e, r^3, s, r^3 s$, where $(r^3 s)^2 = e$ is the trivial symmetry by illustration.

(e) We have the number n_3 of Sylow 3-subgroup of G to satisfy $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 4$, so either $n_3 = 1$ or $n_3 = 4$. Similarly $n_2 = 1$ or 3. We note that there are more than one Sylow 2-subgroup, i.e., of order 4, for instance we saw $\langle r^3, s\rangle$, and we also have $\langle r^3, rs\rangle$, where $r^4 s$ is of order 2. Therefore, we see that the two groups, although both are of order 4, are not the same, so we have 3 subgroups of order 4, therefore there can only be one subgroup of order 3, namely the Sylow 3-subgroup, therefore it has to be normal.

(f) Since Sylow 3-subgroup is unique, then it is normal; since Sylow 2-subgroup is not unique, then it is not normal. Therefore the only Sylow subgroup that is normal is the Sylow 3-subgroup.

(g) Yes. Take a subgroup of order 6, then the subgroup is either C_6 or S_3, either way it is solvable. Therefore, the quotient of G over this subgroup is C_2, which is also solvable, and so G itself must be solvable.

(h) Recall that the center of direct product of groups is the direct product of centers of groups. (Also note that D_n is nilpotent if and only if $n = 2^k$ for $k \geq 0$.) Suppose D_n is nilpotent, then it is the direct product of its Sylow p-subgroups, then since each p-group has non-trivial center, we note that for every prime p dividing $|D_n|$, p divides $|Z(D_n)|$. In our case, we note that this means the center of the group has some element of order 3. This is not possible: we know the Sylow 3-subgroup is unique, therefore either r^2 or r^4 is in the center. But $r^2 s \neq sr^2$ already, contradiction.

(i) Note that $C(X)$ is the set of functions $f : \{1, \dots, 6\} \to \{1, \dots, 5\}$, therefore there are 5^6 total ways. We know the action of D_n on $C(X)$ is given by permutation of elements, representing the rigid motions on the hexagon and sending a function to another function. The number of distinct coloring is now just the orbit of this induced group action.

Let $C = \{1, ..., X\}^n$ represent the set of colorings of n labeled vertices. The dihedral group D_n acts on C by permuting elements, representing the rigid motions of an n-polygon.

Remark 22.1. Note that this is just the number of distinct colorings up to rigid symmetries. Therefore, the distinct colorings we are looking for are the orbits of this group action. Burnside's Lemma tells us that the number of orbits is equal to the average number of fixed points of a group element. So for each element $g \in D_n$, we should calculate $|C^g|$, the number of colorings in C that are unchanged by g. D_n consists of n rotations (including the identity element, which we can think of as a rotation by n steps) and n reflections.

If g is a rotation by k steps, then choosing a fixed point of g corresponds to freely choosing the colors of $\gcd(n,k)$ adjacent vertices; the constraint that our coloring is unchanged by g forces us to repeat this color sequence around the polygon, determining the remaining vertices' colors. So $|C^g| = X^{\gcd(n,k)}$.

If g is a reflection, then to build a fixed point we can freely choose the colors of any vertices that lie on the axis of reflection, and the remaining vertices must be colored in pairs so that they match their reflections. If n is odd, each reflection has one vertex on its axis, so $|C^g| = X^{(n+1)/2}$. If n is even, half of the reflections have two vertices on their axis (yielding $|C^g| = X^{n/2+1}$) and the other half have none (yielding $|C^g| = X^{n/2}$).

Putting these things together and taking the average, we find that the number of orbits is

$$\frac{1}{2n}\left(\sum_{k=1}^{n} X^{\gcd(n,k)} + \begin{cases} nX^{(n+1)/2} & n \text{ odd} \\ \frac{n}{2}X^{n/2+1} + \frac{n}{2}X^{n/2} & n \text{ even} \end{cases}\right).$$

(j) In particular, for $n = 6$, we see that the maximum number is given by having the maximal possible number of colorings, therefore we take $X = 5$. Therefore,

- if g is a rotation by k steps, then a fixed point of g should be d-periodic where $d \mid k$, and note that we need $d \mid 6$ as well, so we need to take $d = \gcd(k, 6)$. In particular, in the period of d points, each point can be colored in 5 ways, so we have $5^{\gcd(k,6)}$ number of colorings for each k.
- if g is a reflection, then we just need to build half of the edges and reflect it. Since D_6 has an even number of edges, then 3 of the reflections require us to build 4 edges, the other 3 requiring us to build 3 edges; thus, we now have $3 \times 5^4 + 3 \times 5^3$ in this case.

Taking everything into account, we have a total number of $5^1+5^2+5^3+5^2+5^1+5^6+3\times 5^4+3\times 5^3 = 18060$ fixed points. Taking the average, we know there are $\frac{18060}{12} = 1504$ orbits.

□

Problem 2. (a) Let (p) be a prime ideal of R, then p is a prime element: suppose $p \mid ab$, then $ab \in (p)$, so by definition either $a \in (p)$ or $b \in (p)$, hence either $p \mid a$ or $p \mid b$ by definition. This implies $p \in R$ is irreducible by Fall 2014, Problem 3 (Problem 21.3) part (a).

Suppose $p \in R$ is irreducible, then by Fall 2014, Problem 3 (Problem 21.3) part (a), we know $p \in R$ is prime. To show (p) is a prime ideal, suppose $ab \in (p)$, then $p \mid ab$ by definition, therefore $p \mid a$ or $p \mid b$ since p is prime, so $a \in (p)$ or $b \in (p)$, hence (p) is a prime ideal.

(b) We have $2\times 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$. We claim that 2 and 3 are both irreducible. Let $2 = (a+b\sqrt{-5})(c+d\sqrt{-5})$, then by the norm argument we see that $(a^2+5b^2)(c^2+5d^2) = 4$; for 2 to not be irreducible, we need the factorization to not contain units, which are elements with norm 1, so we must have $a^2+5b^2 = \pm 2$, which is impossible in $\mathbb{Z}$. Therefore, 2 is irreducible. A similar proof shows that 3 is also irreducible, so $6 = 2\times 3$ is an irreducible factorization. We now show that 2 does not divide $1+\sqrt{-5}$: if it does, we have $2(a+b\sqrt{-5}) = 1+\sqrt{-5}$, then $a, b \notin \mathbb{Z}$, contradiction; similarly, 2 does not divide $1-\sqrt{-5}$, so 2 is not an irreducible factor in the irreducible factorization of $6 = (1+\sqrt{-5})(1-\sqrt{-5})$, hence $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Alternatively, $\mathbb{Z}[\sqrt{-5}]$ admits a factorization, but irreducible element 2 is not prime by above, so this is not a UFD.

□

Problem 3. (a) To show that existence of K such that $[L : K] = p$, note that the Galois group G is a p-group and therefore it has non-trivial center, so the center is a p-subgroup of G, therefore it contains a group of order p by Cauchy's theorem, which is normal in particular (as a subgroup of the center). By the Galois correspondence, let K be the field corresponding to this group of order p, then $[L : K] = p$, and we know K/F is Galois since K corresponds to a normal subgroup.

(b) This is similar to August 2019, Problem 4 (Problem 6.4). We showed that the Galois group G is D_4.

(c) We want $E/K/\mathbb{Q}$ such that $[E : K] = 2$ and $K/\mathbb{Q}$ is Galois, so we need the corresponding group H to be a normal subgroup of $G = D_4$ with order 2. Note that $rs \neq sr$ and $r^2 s = sr^2$ in $D_4 = \langle r, s \mid r^4 = s^2 = 1, rs = sr^{-1} \rangle$, so both $r, s \notin Z(G)$ and $r^2 \in Z(G)$. Therefore, $\langle r^2 \rangle \subseteq Z(G)$ is a subgroup of order 2, and it is normal in G. By the Galois correspondence, we want the field extension to stabilize $\sqrt{3}$ and i, therefore the field extension is $\mathbb{Q}(\sqrt{3}, i)$.

□

23 August 2013

Problems

Problem 23.1. Let G be a finite group acting on a finite set X. Let $X^G = \{x \in X \mid gx = x \, \forall g \in G\}$, and for any $x \in X$ let $G \cdot x = \{gx \mid g \in G\}$ and $G_x = \{g \in G \mid gx = x\}$.

(a) Prove that

(i) $X = X^G \cup \Big(\bigcup\limits_{\substack{x \in X \\ \mathrm{Card}(G \cdot x) \neq 1}} G \cdot x \Big)$,

(ii) $\mathrm{Card}(G \cdot x) = [G : G_x]$.

(b) Suppose that G is a p-group. Prove that $\mathrm{Card}(X) \equiv \mathrm{Card}(X^G) \pmod{p}$.

(c) Prove that the center of a non-trivial p-group is non-trivial. (Hint: take $X = G$ with a suitable action and use part (b).)

(d) Deduce that any p-group is nilpotent.

Problem 23.2. (a) Let G be a finite group, and let $H \lhd G$ be a normal subgroup. Suppose that p is a prime dividing the order of G, but p does not divide $[G : H]$. Show that all Sylow p-subgroups of G are contained in H.

(b) Suppose G has order $p^2 q$, where p and q are distinct primes. Show that G is not simple.

Problem 23.3. Determine a complete list of all non-isomorphic abelian groups of order 1800.

Problem 23.4. Let R be an integral domain with quotient field F. Let $f(x) \in R[x]$ be a monic polynomial, and assume $f(x) = g(x)h(x)$ where g, h are monic polynomials in $F[x]$ of smaller degree than $f(x)$. Prove that if $g(x) \notin R[x]$, then R is not a UFD. Deduce that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD.

Problem 23.5. (a) Let k be a field, and let $f(x) \in k[x]$ of degree n. Let L denote the splitting field of $f(x)$ over k and let G be the Galois group of L/k. Show how to identify G with a subgroup of S_n.

(b) With hypotheses as in part (a), let $f(x) = x^3 + ax + b$, and assume that $f(x)$ is irreducible in $k[x]$. Discuss the possibilities for G and its corresponding orders, and how these depend on a and b. If α is a root of $f(x)$, is $k(\alpha)$ normal over k?

(c) Determine the Galois group of $x^3 - x + 1$ over $\mathbb{Q}$.

Problem 23.6. Let F be a field, and let G be a finite group of automorphisms of F of order n. Let $k = F^G$ be the fixed field of G.

(a) Let $\alpha \in F$ and let $\sigma_1, \ldots, \sigma_r$ be a maximal set of elements of G such that $\sigma_1\alpha, \ldots, \sigma_r\alpha$ are distinct. Show that every $\tau \in G$ induces a bijection on $\{\sigma_1\alpha, \ldots, \sigma_r\alpha\}$ via multiplication on the left.

(b) Prove that every $\alpha \in F$ is the root of a polynomial $f(x) \in k[x]$, where all roots are distinct and contained in F, and $\deg(f(x)) \leq n$. (Hint: use part (a).)

(c) Deduce that F is a finite Galois extension of k of degree n with Galois group G.

SOLUTIONS

Problem 1. (a) (i) Note that the orbits $G \cdot x$ gives an equivalence relation on X, therefore the corresponding equivalence classes partitions X into a disjoint union of the orbits $G \cdot x$'s. Indeed, $G \cdot x_1 = G \cdot x_2$ if and only if $gx_1 = x_2$ for some $g \in G$.

Therefore, consider the set of orbits, then an orbit either has size 1 or has size at least 2. An orbit $\{x\}$ of size 1, by definition, is just a fixed point $\{x\}^G$, therefore the union of all fixed points, given as a set, is just the set of fixed points X^G. Therefore, we partition $X = X^G \cup (\bigcup_{\substack{x \in X \\ \mathrm{Card}(G \cdot x) \neq 1}} G \cdot x)$ as desired.

(ii) Fix $x \in X$ and consider the stabilizer G_x, then this induces a function

$$\begin{aligned} f : G/G_x &\to G \cdot x \\ g \cdot G_x &\mapsto gx \end{aligned}$$

To see that the function is well-defined, we first show that $g \cdot G_x = g' \cdot G_x$ implies $gx = g'x$. Indeed, having such $g, g' \in G$ implies $g^{-1}g' \in G_x$, so $(g^{-1}g')x = x$, namely $gx = g'x$ by group action.

Obviously this function is a surjection, so we are done if we can show that this is an injection. Indeed, if $gx = g'x$, then $g^{-1}g' \in G_x$, therefore $g \cdot G_x = g' \cdot G_x$.

(b) Let G be a group of order p^l. Since X is finite, then let the set of fixed points be denoted as $X^G = \{x_1, \dots, x_n\}$. By definition, $G \cdot x_i = \{x_i\}$. By part (a), we extend these n singletons to a partition of X via G, given by the disjoint union $\bigcup_{i=1}^{n+m} G \cdot x_i$, where $x_{n+1}, \dots, x_{n+m}$ are the representatives of the m orbits with size at least 2. By the orbit-stabilizer theorem, we know $\mathrm{Card}(G \cdot x_i) = [G : G_{x_i}] = \frac{p^l}{\mathrm{Card}(G_{x_i})}$ for $i = n+1, \dots, n+m$. Since the orbits $G \cdot x_i$'s are at least 2 for $i = n+1, \dots, n+m$, then $\mathrm{Card}(G \cdot x_i)$ is divisible by p. Therefore, the cardinality of X is equivalent to the number of fixed points modulo p since each one has size 1, and the rest of the orbits has size divisible by p, so by definition this gives $\mathrm{Card}(X) \equiv \mathrm{Card}(X^G) \pmod{p}$.

(c) Let $X = G$, and we think of the action of G on X by G-conjugation. In particular, the fixed points are $X^G = \{x \in X \mid gxg^{-1} = x \, \forall g \in G\}$, namely this is the center $Z(G)$ of $G = X$. By part (b), we know $|G| \equiv |Z(G)| \pmod{p}$, and since G is a p-group, we have $|Z(G)|$ divisible by p. Since $Z(G)$ is never empty, then $Z(G)$ has size at least p, and in particular is non-trivial.

(d) This is May 2015, Problem 1 (Problem 19.1), part (b).

□

Problem 2. (a) Since $p \mid |G|$ and $p \nmid [G : H]$, then by Lagrange's Theorem we know $p \mid |H|$. In particular, there exists some Sylow p-group N of G that is contained in H. By the Second Sylow Theorem, we know all Sylow p-groups are conjugates. In particular, since $N \subseteq H$, then for all $g \in G$, the conjugate $gNg^{-1} \subseteq gHg^{-1} = H$ since $H \lhd G$ is a normal subgroup. Therefore, all conjugates of N are contained in H. Since all Sylow p-subgroups of G are conjugates, then all Sylow p-subgroups of G are contained in H.

(b) Since $p \neq q$, we either have $p > q$ or $p < q$. If $p > q$, then by Sylow Theorem we know the number of Sylow p-subgroups satisfies $n_p \equiv 1 \pmod{p}$ and $n_p \mid q$, therefore since $p > q$ we have $n_p = 1$, therefore G has a unique Sylow p-subgroup, therefore this Sylow p-subgroup must be a normal subgroup of G, so G is not simple. If $p < q$, then by Sylow Theorem we know the number of Sylow q-subgroups satisfies $n_q \equiv 1 \pmod{q}$ and $n_q \mid p^2$. Note that $n_q \neq p$ since $p < q$, then supposing G is simple, it cannot have a unique Sylow subgroup, therefore $n_p, n_q \neq 1$, therefore $n_p = q$ and $n_q = p^2$, so $p^2 \equiv 1 \pmod{q}$ and $q \equiv 1 \pmod{p}$. In particular, $q \mid p^2 - 1$, so $q \mid (p-1)$ or $q \mid (p+1)$ since q is prime. Since $p < q$, then $q \nmid p - 1 \neq 0$, so $q \mid (p+1)$. In particular, this forces $q = p + 1$, and the only way to do this is having $p = 2$ and $q = 3$. Therefore, this means if G is simple, then G has order 12. We know $n_p = 3$ and $n_q = 4$. In particular, since Sylow q-subgroups have prime order in this case, then there are $4 \times (3-1) = 8$ elements of order 3 in G, so this means there are only three elements of order 2; every Sylow 2-subgroup has order 4, so there is a unique Sylow p-subgroup, contradiction.

□

Problem 3. By the structure theorem, a group of $1800 = 2^3 \times 3^2 \times 5^2$ must be the direct product of cyclic groups. Therefore, the group is one of the following structures:

- $\mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z})^2$,
- $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$,
- $\mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/25\mathbb{Z}$,
- $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z})^2$,
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$,
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/25\mathbb{Z}$,
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
- $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z})^2$,
- $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/9\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$,
- $(\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/25\mathbb{Z}$,
- $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$.

Note that these can be simplified since $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z}$ whenever $\gcd(n,m) = 1$, according to the Chinese Remainder Theorem. □

Problem 4. We prove the contrapositive. Suppose that R is a UFD. Since $h(x) \in F[x]$, then coefficients of $h(x)$ are fractions of elements in R. In particular, there exists some element $0 \neq a \in R$ such that $a \cdot h(x)$ is in $R[x]$. Moreover, by Gauss Lemma, one can assume $a \cdot h(x)$ to be primitive since R is a UFD (as greatest common divisors exist). Therefore, we see $a \cdot h(x)$ divides $a \cdot f(x)$ in $F[x]$, and since $a \cdot h(x)$ is primitive, then $a \cdot h(x)$ divides $a \cdot f(x)$ in $R[x]$. In particular, we have $g'(x) \in R[x]$ such that $(a \cdot h(x))g'(x) = a \cdot f(x)$ over $R[x]$. If we think of this factorization as over $F[x]$, we note that $F[x]$ is a UFD, therefore by cancellation law we have $g'(x)h(x) = f(x)$, but by unique factorization we have $g'(x) = g(x)$, so $g(x) \in R[x]$. □

Problem 5. (a) Since f has degree n, then it has $m \leq n$ roots counted with multiplicities. Recall that the Galois group is generated by automorphisms that permute the roots, then there is an embedding $G \hookrightarrow S_m$ by the permutation of roots. Because there is a natural embedding $S_m \hookrightarrow S_n$ for $m \leq n$, then this gives the embedding $G \hookrightarrow S_n$, therefore allows us to view G as a subgroup of S_n.

(b) Since this is Galois and f is irreducible, then $G \subseteq S_3$ must be a transitive subgroup. In particular, G is either A_3 of order 3 or S_3 of order 6. To see how they depend on a and b, let the discriminant be $\Delta = -4a^3 - 27b^2$, then if Δ is a square, we know it is A_3, and if it is not a square, then it is S_3. Since f is irreducible over $k[x]$, f has no roots over k, so the minimal polynomial of $\alpha \in k$ is just f itself. Therefore, $[k(\alpha) : k] = 3$. If $G = A_3$, then we must have $k(\alpha) = L$ so it is trivially Galois. If $G = S_3$, then by the Galois correspondence we must have H as order 2, so it is a transposition, and therefore generates a non-normal subgroup. By the Galois correspondence, this shows that $k(\alpha)/k$ is not normal in this case.

(c) The discriminant is not a square in $\mathbb{Q}$, so it has Galois group S_3.

□

Problem 6. (a) Take $\tau \in G$ to be an automorphism, then the image $\tau\sigma_i\alpha$ is still contained in this set for every i by the maximality of automorphism, since the the composition of two automorphisms is still an automorphism. Therefore, τ defines a function on this set of elements. In particular, the automorphism gives a bijection when restricted onto this set.

(b) Let $\alpha \in F$ be an element, and pick a maximal set $\sigma_1, \dots, \sigma_r \in G$ of F-automorphisms as said in part (a), then every $\tau \in G$ defines a bijection on $\{\sigma_1\alpha, \dots, \sigma_r\alpha\}$. Note that every $\sigma_i\alpha$ is still in F, so we define $f(x) = \prod_{i=1}^{r}(x - \sigma_i\alpha)$, therefore $\deg(f(x)) = r \leq n$ by construction. Now $\tau f = \prod_{i=1}^{r}(x - \tau\sigma_i\alpha) = f$, therefore every $\tau \in G$ fixes f, so that means $f \in k[x]$ by the definition of the fixed field. In particular, the trivial automorphism is contained in the set of automorphisms, then $\alpha = \sigma_i\alpha$ for some σ_i, therefore $\alpha \in F$ is a root of $f(x)$. Moreover, f is separable, so $\alpha \in F$ is separable and algebraic over k. Hence, every $\alpha \in F$ is the root of some $f(x) \in k[x]$ with the desired property. In particular, the degree of this extension if $[k(\alpha) : k] = \deg(m_\alpha) \leq \deg(f) \leq |G|$.

(c) We now know $[F : k] \geq |\operatorname{Aut}(F/k)| \geq |G|$ since $G \subseteq \operatorname{Aut}(F/k)$. It suffices to show that $|G| \geq [F : k]$, then this forces $[F : k] = |\operatorname{Aut}(F/k)|$, then by definition F/k is a finite Galois extension. Moreover, since G is a subgroup of the Galois group with equal cardinality, then $\operatorname{Gal}(F/l) = G$ in particular.

We will now show that $|G| \geq [F : k]$. By part (b), we know every element of F is algebraic and separable over F. Suppose, towards contradiction, that $|G| < [F : k]$, then we can find linearly independent $\alpha_1, \dots, \alpha_s \in F$ over k where $s = [F : k] > |G|$. Therefore, $k(\alpha_1, \dots, \alpha_s)/k$ is a field extension of degree at least $s = [F : k] > G$, and this extension is separable as a subextension of F/k. By the primitive element theorem, there exists some $\beta \in F$ such that $k(\beta)/k$ has degree $s > |G|$, but by part (b) we should have $[k(\beta) : k] \leq |G|$, contradiction.

□

24 May 2013

Problems

Problem 24.1. (a) Let $n \geq 3$. Show that the alternating group A_n is generated by 3-cycles.

(b) Let $n \geq 5$. Let $H \subseteq S_n$ be a subgroup, and let $H_1 \lhd H$ be a normal subgroup such that H/H_1 is abelian. If H contains all 3-cycles, then show that H_1 also contains all 3-cycles.

(c) Deduce that S_n is not solvable for $n \geq 5$. Also show that the commutator subgroup of S_n is A_n.

Problem 24.2. (a) Let $f : G \to G'$ be an epimorphism of groups. Let H be a Sylow p-subgroup of G. Then $f(H)$ is either the trivial group or a Sylow p-subgroup of G'.

(b) Let G be a finite group and let p be a prime dividing $|G|$, the order of G. Suppose $H \lhd G$ is a normal subgroup such that p does not divide $[G : H]$. Show that all Sylow p-subgroups of G are contained in H.

Problem 24.3. (a) Deduce from the structure theorems for modules over a PID the following:

Given any finite-dimensional vector space $E \neq 0$ over the field k and $A \in \mathrm{End}_k(E)$, there exists a direct sum decomposition $E = E_1 \oplus \cdots \oplus E_r$, where each E_i is a principal $k[A]$-submodule with invariant $q_i \neq 0$ such that $q_1 \mid q_2 \cdots \mid q_r$. The sequence $(q_1, \ldots, q_r)$ is uniquely determined by E and A, and q_r is the minimal polynomial of A. (Note: the *invariant* of a principal $k[A]$-module M is the monic polynomial $q(t)$ of minimal degree such that $q(A)M = 0$.)

(b) Let k' be an extension field of k and A be an $n \times n$ matrix with entries in k. Show that the invariants of A over k are the same as its invariants over k'.

Problem 24.4. Prove that $f(x) = x^p - x - 1$ is irreducible in $\mathbb{Z}[x]$. (Hint: use the following problem Problem 24.5.)

Problem 24.5. Let k be a field of characteristic $p > 0$, and let $a \in k$. Show that the polynomial $f(x) = x^p - x - a$ either (i) splits into linear factors over k, or (ii) is irreducible over k.

Problem 24.6. Let k be a field of some characteristic p (which could be 0) and let n be a positive integer; in the case that $p > 0$, assume also that n is prime to p. Let ζ be a primitive nth root of unity in $\bar{k}$, the algebraic closure of k.

(a) Show that $k(\zeta)$ is a normal extension of k.

(b) Let $G = \mathrm{Aut}_k(k(\zeta))$. Prove that G can be identified as a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Deduce that G is abelian.

(c) Let $k = \mathbb{Q}$. Assume in this case $G = (\mathbb{Z}/n\mathbb{Z})^\times$ and deduce that $\mathbb{Q}(\zeta_5) \cap \mathbb{Q}(\zeta_8) = \mathbb{Q}$. (Hint: may use $\varphi(mn) = \varphi(m)\varphi(n)$ when m, n relatively prime.)

Solutions

Problem 1. This problem is very similar to August 2019, Problem 2 (Problem 6.2).

(a) Since A_n is the set of even permutations, then each element of A_n can be expressed as a product of an even number of transpositions. Therefore, A_n is generated by products of two transpositions. Now each product of two transpositions gives either 1) the trivial element, 2) a 3-cycle, or 3) a product of two 3-cycles. Therefore, either way A_n is generated by 3-cycles.

(b) Since H contains all 3-cycles, then $H \supseteq A_n$, therefore either $H = A_n$ or $H = S_n$. If $H = A_n$, then since A_n is simple for $n \geq 5$, either $H_1 = \{e\}$ or $H_1 = A_n$. But A_n itself is non-abelian for obvious reasons, so $H_1 \neq \{e\}$, thus $H_1 = A_n$ in this case, so H_1 contains all 3-cycles. If $H = S_n$, then note that H_1 is either $\{e\}$, A_n, or S_n since A_n is the only proper normal subgroup of S_n for $n \geq 5$. Since H/H_1 is abelian, then $H_1 \neq \{e\}$, since that would imply $H = S_n$ is abelian, contradiction. Therefore, either $H_1 = A_n$ or S_n, and either way it contains all 3-cycles.

(c) Suppose S_n is solvable for some $n \geq 5$, then $A_n \subseteq S_n$ is also solvable. But A_n is a non-abelian simple group for $n \geq 5$, then A_n is not solvable, contradiction. To find the commutator subgroup $[S_n, S_n]$, first note that S_n/A_n is already abelian, so $[S_n, S_n] \subseteq A_n$, but A_n is simple for $n \geq 5$, therefore either $[S_n, S_n]$ is either trivial or is A_n. But having $[S_n, S_n]$ trivial implies S_n is abelian, contradiction. Therefore, $[S_n, S_n] = A_n$. (Alternatively, every 3-cycle is a commutator, therefore A_n is contained in the commutator already.)

□

Problem 2. (a) Recall that an epimorphism in the category of groups is just a surjective group homomorphism. Let H be the Sylow p-subgroup of order p^n. Let g be the restriction of f on H, then by the first isomorphism theorem, we know $\operatorname{im}(g)$ is either a p-group or is trivial. Suppose $\operatorname{im}(g)$ is non-trivial, and we want to show that $\operatorname{im}(g)$ is a Sylow p-subgroup of $\operatorname{im}(f) = G'$. Suppose not, then $p \mid \frac{G'}{\operatorname{im}(g)}$, then taking the preimage, we have $H \subseteq f^{-1}(\operatorname{im}(g)) \subseteq G$, then by the correspondence theorem, the surjective group homomorphism induces a bijection $G/f^{-1}(\operatorname{im}(g)) \simeq G'/\operatorname{im}(g)$. In particular, this means the index of $f^{-1}(\operatorname{im}(g))$ in G is also divisible by p, but this group contains H, which already has index relatively prime to p, contradiction. Therefore, if $\operatorname{im}(g)$ is non-trivial, it would be a p-group.

(b) This is August 2013, Problem 2 (Problem 23.2), part (a).

□

Problem 3. (a) Take this to the torsion module structure, then we obtain a direct sum of cyclic modules, where we obtain the elementary divisors. By Chinese Remainder Theorem, we obtain the invariant factors with the desired property. Since the minimal polynomial annihilates everything and the invariant factors having one factoring another in order, where each invariant factor is just the quotient in the decomposition of the cyclic modules, then the minimal polynomial is just the last invariant factor.

(b) By the structure theorem, we know the invariant factors are given by the decomposition of module over PID into cyclic modules, then for each cyclic module we know the generator is given by the $k[x]$-module structure of matrix A is the companion matrix $x \cdot I - C(A)$ by the factorization. Therefore, finding the invariant factors descends to finding the Smith normal form, which does not depend on the base field.

□

Problem 4. This is similar to August 2020, Problem 4 (Problem 4.4) part (b), August 2019, Problem 5 (Problem 6.5) part (b), and January 2016, Problem 5 (Problem 17.5). It suffices to show that $f(x)$ is irreducible in $\mathbb{F}_p[x]$. Suppose not, then by the following problem (Problem 24.5), it splits into linear factors over $\mathbb{F}_p$. Note that if α is a root of $f(x)$, then the roots are $r, r+1 \ldots, r+(p-1)$, which means every element of $\mathbb{F}_p$ is a root. In particular, 0 is not a root of $f(x)$, contradiction. Therefore, this is irreducible in $\mathbb{F}_p$ hence irreducible in $\mathbb{Z}$. □

Problem 5. This is similar to August 2020, Problem 4 (Problem 4.4) part (b), August 2019, Problem 5 (Problem 6.5) part (b), and January 2016, Problem 5 (Problem 17.5). In particular, given a root α of $f(x)$, we know the roots of $f(x)$ are $\alpha, \alpha - 1, \ldots, \alpha - (p-1)$ in $k(\alpha)$, and they are obviously distinct. Therefore, either k contains all the roots of $f(x)$, or k contains none of the roots of $f(x)$. Suppose $g \mid f$ is the minimal polynomial of α, then note that by a change of variables g is the minimal polynomial of every root. Therefore, if we think of an irreducible factorization of f over $k(\alpha)$, then every factor must be the minimal polynomial of a particular root since f is separable. In particular, the degree of each factor equals to $\deg(g)$, but the sum of degrees of the factors is just $\deg(f) = p$, so $\deg(g) \mid p$, hence either $\deg(g) = p$, meaning there is only one irreducible factor, so $f = g$ is irreducible, or $\deg(g) = 1$, meaning $k(\alpha)/k$ has degree 1, therefore f splits over k. □

Problem 6. (a) Since ζ is a primitive nth root of unity, then every root of $x^n - 1$ has the form ζ^l for some l. Therefore, the field extension $k(\zeta)/k$ contains all roots of $x^n - 1$. Moreover, since all roots of $x^n - 1$ are of the said form, then $k(\zeta)$ is the splitting field of $x^n - 1$, therefore $k(\zeta)/k$ is normal.

(b) Note that $x^n - 1$ is always separable in this setting, so the extension is Galois. An automorphism σ in G now sends a root of $x^n - 1$ to some other root, i.e., of the form $\zeta \mapsto \zeta^l$ for some l such that $\gcd(l, n) = 1$ since it is an automorphism. This induces a map $G \to (\mathbb{Z}/n\mathbb{Z})^\times$ via $\sigma \mapsto [l]_n$, then this is a well-defined homomorphism. Moreover, this is an injective, and therefore this induces a subgroup structure $G \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$. We identify G as a subgroup of the cyclic group above, therefore, G is a subgroup of an abelian group and is therefore abelian.

(c) We have a larger field extension $\mathbb{Q}(\zeta_5, \zeta_8)/\mathbb{Q}$ of degree 16 by basis argument. We note that this is contained in $\mathbb{Q}(\zeta_{40})$. Taking the Galois correspondence, we note that both extensions have degree 16, since $\varphi(40) = \varphi(5)\varphi(8) = 4 \times 4 = 16$. Therefore, they are the same. By the Galois correspondence, the intersection $\mathbb{Q}(\zeta_5) \cap \mathbb{Q}(\zeta_8)$ corresponds to $\langle H, K \rangle$, where $H \cong K \cong \mathbb{Z}/4\mathbb{Z}$. We need to look at how H and K intersects. If σ generates $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$ and τ generates $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$, then we note that the two generators interact freely, therefore the product $\langle H, K \rangle$ is the direct product of the two groups, given by order 16. In particular, that means the product group equals to $(\mathbb{Z}/40\mathbb{Z})^\times$, and by the Galois correspondence we know the two fields intersect trivially.

□

25 January 2013

Problems

Problem 25.1. Let G be a finite group of order $|G|$, and let $Z(G)$ denote the center of G.

(a) If $G/Z(G)$ is cyclic, then G is abelian.

(b) If $|G| = pq$, where p and q are primes, then either $Z(G) = \{1\}$ or G is abelian.

Problem 25.2. Show that a group of order $20 \cdot 23^r$, where r is a positive integer, is solvable.

Problem 25.3. Let R be a commutative ring and let M be an R-module. M is called *projective* if there exists an R-module N such that the R-module $M \oplus N$ is free. Let $\mathbb{Q}$ be the field of rational numbers viewed as a $\mathbb{Z}$-module. Is $\mathbb{Q}$ a projective $\mathbb{Z}$-module?

Problem 25.4. (a) Let k be a field and let U be a finite multiplicative subgroup of k. Prove that U is cyclic.

(b) Let k^* be the set of units in k. Assume that k is a finite field. Show that k^* is a cyclic group.

Problem 25.5. (a) Let k be a field and let $f(x) \in k[x]$ be such that its derivative $f'(x)$ is not the null polynomial. Prove that the following are equivalent.

(i) $f(x)$ has a multiple root in the algebraic closure of k.

(ii) $f(x)$ and $f'(x)$ have a common root in the algebraic closure of k.

(iii) The greatest common divisor of $f(x)$ and $f'(x)$ in $k[x]$ is of degree ≥ 1.

(b) A polynomial over k is called separable if its roots in the algebraic closure of k are distinct. Prove the following statements.

(i) An irreducible polynomial over a field k of characteristic 0 is separable.

(ii) Let k be a field of characteristic $p > 0$ and $f(x)$ be an irreducible polynomial in $k[x]$. Suppose that $f(x)$ cannot be expressed as a polynomial in x^p with coefficients in k, then $f(x)$ is separable.

(c) Let p be a prime number. Show that the polynomial $f(x) = x^{p-1} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$.

Problem 25.6. Consider the polynomial $x^4 - 2$ over $\mathbb{Q}$.

(a) Find the splitting field K of $f(x)$ and its degree over $\mathbb{Q}$.

(b) Let G be the Galois group of the field extension $\mathbb{Q} \subseteq K$. Find the generators and relators for G. Is it isomorphic to the dihedral group D_8?

Solutions

Problem 1. (a) Take arbitrary $a, b \in G$, then this descends to $a = c^k \cdot n_1$ and $b = c^l \cdot n_2$ for generator $c \cdot Z(G)$ of $G/Z(G)$ (and $c \in G$) and some $n_1, n_2 \in Z(G)$. Therefore, $ab = c^k \cdot n_1 \cdot c^l \cdot n_2 = c^l \cdot n_2 \cdot c^k \cdot n_1 = ba$, so G is abelian.

(b) The subgroups of G are either trivial, of order p, of order q, or of order pq. If $Z(G)$ has order p, q, or pq, then $G/Z(G)$ is cyclic, hence G is abelian. If $Z(G)$ has order 1, then the center is trivial.

□

Problem 2. By Sylow Theorem, we know there exists a unique Sylow 23-subgroup N of G, so this is normal. Moreover, we know N is a solvable group. It now suffices to show that G/N of order 20 is solvable. This group of order 20 has a unique Sylow 5-subgroup, and therefore it is normal again, and it is solvable. The quotient is a group of order 4 which is a 2-group and therefore must be solvable, so the group of order 20 is solvable, hence G is solvable. □

Problem 3. Suppose it is projective, then over a PID $\mathbb{Z}$, a module is projective if and only if it is free, so $\mathbb{Q}$ should be a free $\mathbb{Z}$-module. Note that $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) = 0$: suppose $f(q) = x$ for some q and some x, for some large enough $y > x$, we have $f\left(\frac{q}{y}\right) = \frac{x}{y}$, which is well-defined if and only if $x = 0$. Therefore, $f(q) = 0$ for all $q \in \mathbb{Q}$. Since $\mathbb{Q}$ is a projective $\mathbb{Z}$-module, then there is an injective homomorphism $\mathbb{Q} \hookrightarrow \mathbb{Z}^n$, but the homomorphism on each slot is the trivial homomorphism since the hom set is zero, therefore teh injective homomorphism is the zero map, contradiction. □

Problem 4. This is similar to May 2022, Problem 4 (Problem 1.4), part (a). □

Problem 5. (a)

- $(i) \Rightarrow (ii)$: Suppose $f(x)$ has a multiple root in $\bar{k}$, then $f(x) = (x-a)^n g(x)$ for some $a \in \bar{k}$, $n \geq 2$, and $g(a) \neq 0$. Since the derivative is multiplicative, we have $f'(x) = n(x-a)^{n-1}g(x) + (x-a)^n g'(x)$, and since $n-1 \geq 1$, we have $f'(a) = 0$, so a is a root of f' and f.
- $(ii) \Rightarrow (iii)$: We prove the contrapositive. Suppose $\gcd(f(x), f'(x)) = 1$ over k, then this is still true over $\bar{k}$, so every root a of f satisfies $x - a \mid f$, but that also means $x - a \nmid f'$, so $f'(a) \neq 0$. In particular, this is true for all roots a of f, so f and f' do not share a root.
- $(iii) \Rightarrow (i)$: Suppose the greatest common divisor of f and f' has degree at least 1, then there exists some polynomial $g(x)$ that divides both. In particular, all roots of g in $\bar{k}$ are both roots of f and roots of f'. We will now work over $\bar{k}$. Let α be a root of g, then we can write $f(x) = (x-\alpha)^n \cdot f_1(x)$ for some $x-\alpha \nmid f_1(x) \in \bar{k}[x]$. Take the derivative, we have $f'(x) = n(x-\alpha)^{n-1}f_1(x) + (x-\alpha)^n f_1'(x)$. Since α is also a root of $f'(X)$, then this forces $n(x-\alpha)^{n-1}f_1(\alpha) = 0$, but $f_1(\alpha) \neq 0$, therefore $n-1 \geq 1$, hence $n \geq 2$, therefore f has a multiple root in $\bar{k}$ by definition.

(b) (i) Suppose $f(x)$ is an irreducible polynomial over a field k of characteristic 0, then the greatest common divisor of $f(x)$ and $f'(x)$ obviously has degree 0. In particular, by part (a) we know all roots of $f(x)$ in $\bar{k}$ are distinct. By definition, $f(x)$ is separable by definition.

(ii) Suppose $f(x)$ cannot be expressed as a polynomial in x^p, then the derivative is non-zero in this case. Since the polynomial is irreducible, then the greatest common divisor of $f(x)$ and $f'(x)$ in $k[x]$ must have degree 0. Therefore, by part (a), we know $f(x)$ has no multiple roots in $\bar{k}$, so by definition $f(x)$ is separable.

(c) Note that $f(x) = x^{p-1} + \cdots + x + 1 = \frac{x^p-1}{x-1}$, and by a change of variables with $x = y+1$, we have $f(y) = \frac{(y+1)^p-1}{y} = \frac{y^p+\binom{p}{1}y^{p-1}+\cdots+\binom{p}{p-1}y+1-1}{y} = y^{p-1} + \binom{p}{1}y^{p-2} + \cdots + \binom{p}{p-1}$. In particular, by Eisenstein criterion on the prime p, we know $f(y)$ is irreducible over $\mathbb{Q}$. Therefore, $f(x) = x^{p-1} + \cdots + x + 1 = \frac{x^p-1}{x-1}$ is irreducible over $\mathbb{Q}$.

□

Problem 6. This is similar to August 2019, Problem 4 (Problem 6.4) and January 2014, Problem 3 (Problem 22.3), part (b). □