Math 402 - 01 Previous Homework (Spring 2019)

$\newcommand{\aut}{\textrm{Aut}} \newcommand{\inn}{\textrm{Inn}} \newcommand{\sub}{\textrm{Sub}} \newcommand{\cl}{\textrm{cl}} \newcommand{\join}{\vee} \newcommand{\bigjoin}{\bigvee} \newcommand{\meet}{\wedge} \newcommand{\bigmeet}{\bigwedge} \newcommand{\normaleq}{\unlhd} \newcommand{\normal}{\lhd} \newcommand{\union}{\cup} \newcommand{\intersection}{\cap} \newcommand{\bigunion}{\bigcup} \newcommand{\bigintersection}{\bigcap} \newcommand{\sq}[2][\ ]{\sqrt[#1]{#2\,}} \newcommand{\pbr}[1]{\langle #1\rangle} \newcommand{\ds}{\displaystyle} \newcommand{\C}{\mathbb{C}} \newcommand{\R}{\mathbb{R}} \newcommand{\Q}{\mathbb{Q}} \newcommand{\Z}{\mathbb{Z}} \newcommand{\N}{\mathbb{N}} \newcommand{\A}{\mathbb{A}} \newcommand{\F}{\mathbb{F}} \newcommand{\T}{\mathbb{T}} \newcommand{\ol}[1]{\overline{#1}} \newcommand{\imp}{\Rightarrow} \newcommand{\rimp}{\Leftarrow} \newcommand{\pinfty}{1/p^\infty} \newcommand{\power}{\mathcal{P}} \newcommand{\calL}{\mathcal{L}} \newcommand{\calC}{\mathcal{C}} \newcommand{\calN}{\mathcal{N}} \newcommand{\calB}{\mathcal{B}} \newcommand{\calF}{\mathcal{F}} \newcommand{\calR}{\mathcal{R}} \newcommand{\calS}{\mathcal{S}} \newcommand{\calU}{\mathcal{U}} \newcommand{\calT}{\mathcal{T}} \newcommand{\gal}{\textrm{Gal}} \newcommand{\isom}{\approx} \newcommand{\idl}{\textrm{Idl}} \newcommand{\lub}{\textrm{lub}} \newcommand{\glb}{\textrm{glb}} \newcommand{\cis}{\textrm{cis}} $

Problem Set 07 (complete) Due: 04/17/2019 Board presentation: 04/26/2019

1. Let E be a field, G a finite subgroup of $\aut(E)$, $F=E_G$, and $L\in\sub_F(E)$. Show that $L^*=\aut_L(E)$, and it is a subgroup of G.
2. Let E be a field, G a subgroup of $\aut(E)$, and $F=E_G$. Prove that for any $H,H_1,H_2\in\sub(G)$, and any $L,L_1,L_2\in\sub_F(E)$
   I. If $H_1 \leq H_2$, then $H_2^* \leq H_1^*$. (i.e. $\,^*$ is order reversing)
   II. If $L_1 \leq L_2$, then $L_2^* \leq L_1^*$. (i.e. $\,^*$ is order reversing)
   III. $H\leq H^{**}$ (i.e. $1 \leq \,^{**}$)
   IV. $L\leq L^{**}$ (i.e. $1 \leq \,^{**}$)
3. Let $E/L/F$ be a field tower.
   I. Prove that if E/F is a normal extension then so is E/L.
   II. Prove that if E/F is a Galois extension then so is E/L.

Problem Set 06 (complete) Due: 04/12/2019 Board presentation: 04/17/2019

1. Let F be a field, $\alpha_1,\dots,\alpha_n$ elements from some extension E of F, and R a commutative ring with unity. If $\varphi_1,\varphi_2:F(\alpha_1,\dots,\alpha_n)\to R$ are homomorphisms such that $\varphi_1(a)=\varphi_2(a)$ for all $a\in F$ and $\varphi_1(\alpha_i)=\varphi_2(\alpha_i)$ for $i=1,\dots,n$, then $\varphi_1=\varphi_2$.
2. Let $f(x)=x^5-2\in\Q[x]$, and E the splitting field of $f(x)$. Consider the group $G=\aut_\Q(E)$.
   I. What is the order of G?
   II. Is it abelian?
   III. What are the orders of elements in G?
3. Let $F=\F_p(t)$ be the field of rational functions on t with coefficients in $\F_p$. Consider the polynomial $f(x)=x^p-t\in F[x]$.

   I. Show that $f(x)$ has no root in F.
   II. Show that the Frobeni\us endomorphism $\Phi:F\to F$ is not surjective.
   III. Show that $f(x)$ has exactly one root, and that root has multiplicity p.
   IV. Show that $f(x)$ is irreducible over F.

Problem Set 05 (complete) Due: 03/25/2019 Board presentation: 04/02/2019

1. Let F be a field and $f(x), g(x)\in F[x]$. Prove:
   I. $(f(x)+g(x))' = f'(x) + g'(x)$
   II. $(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$
2. Let F be a field, and $\varphi:F\to F$ an endomorphism of F. Prove that the set \[F_\varphi=\{a\in F\mid\varphi(a)=a\}\] is a subfield of F.
3. How many monic irreducible polynomials of degree 4 are there over $\F_5$?
4. Let E be a field extension of F. Prove that E is an algebraic closure of F iff E is minimal with the property that every polynomial $f(x)\in F[x]$ splits over E.

Problem Set 04 (complete) Due: 03/11/2019 Board presentatiion: 03/25/2019

1. Let E/F be a field extension. Prove that $[E:F]=1$ iff $E=F$.
2. Let E and K be field extensions of F and $\varphi:E\to K$ an F-extension homomorphism. Show that φ is a linear transformation of F-vector spaces.
3. Write $\sq{2}$ as a polynomial expression on $\alpha=\sq{2}+\sq{3}$.
4. Find the minimal polynomial of $u=(\sq[3]{2}+\omega)$ over $\Q$.

Problem Set 03 (complete) Due: 02/18/2019 Board presentation: 02/20/2019

1. Let V be a vector space and $B\subseteq V$. Show that the following are equivalent
   I. B is a basis for V,
   II. B is maximal linearly independent set,
   III. B is minimal spanning set.
2. Let V be a vector space and W a subspace of V.
   I. Prove that $\dim(W) \leq \dim(V)$.
   II. Prove that if V is finite dimensional and $\dim(W)=\dim(V)$ then $W=V$
   III. Show, with a counterexample, that the finite dimensional hypothesis is necessary in part b.
3. In regards to the *Universal Mapping Property* for vector spaces discussed in class today:
   I. Complete the proof of it.
   II. Prove that the set $\{\alpha(v)\mid v\in B\}$ is linearly independent in W iff $\widehat{\alpha}$ is injective.
   III. Prove that the set $\{\alpha(v)\mid v\in B\}$ is a spanning set for W iff $\widehat{\alpha}$ is surjective.
4. Let V be a vector space over F, and W a subspace of V. Let B_1 be a basis for W and B a basis for V such that $B_1\subseteq B$. Prove that the set \[\{v+W\mid v\in B-B_1\} \] is a basis for the quotient space V/W.

Problem Set 02 (complete) Due: 02/11/2019 Board presentation: 02/18/2019

1. Let D be a UFD. $a,b,c\in D$, and $f(x)\in D[x]$. a,b are said to be "*relatively prime*" if $\gcd(a,b)$ is a unit.
   I. Prove that if a,b are relatively prime and $a|bc$ then $a|c$.

   II. Prove that if $\frac{a}{b}$ is a root of $f(x)$, and a,b are relatively prime, then a divides the constant term of $f(x)$ and b divides the leading term of $f(x)$.
2. Let D be an ED, $a,b\in D$, with $b\neq 0$. Consider the sequence $r_0,r_1,r_2,\dots,r_n$ defined recursively as follows: $r_0=a,r_1=b$, and using the propery of an Euclidean Domain, until obtaining a residue 0, \[\begin{array}{rclll} r_0 &=&q_1 r_1 + r_2 &\text{ and} &\delta(r_2) < \delta(r_1), \\ r_1 &=&q_2 r_2 + r_3 &\text{ and} &\delta(r_3) < \delta(r_2), \\ &\vdots \\ r_{n-3} &=&q_{n-2} r_{n-2} + r_{n-1} &\text{ and} &\delta(r_{n-1}) < \delta(r_{n-2}), \\ r_{n-2} &=&q_{n-1} r_{n-1} + r_n &\text{ and} &r_n=0. \\ \end{array} \] Why does the sequence $r_1,r_2,\dots,r_n$ have to eventually attain the value $r_n=0$? Prove that the last non-zero entry in the residues list, i.e. $r_{n-1}\sim\gcd(a,b)$.
3. Let D be a PID, $a,b\in D$. Let d be a generator of the ideal $\pbr{a}+\pbr{b}$. Show that $d\sim\gcd(a,b)$.
4. Let D be an ID, $a,b\in D$. Prove that if a and b have a least common multiple $l\in D$, then $\frac{ab}{l}$ is a greatest common divisor of a and b in D.
5. (Optional) Let $\gamma=\ds\frac{1+\sqrt{-19}}{2}$ and consider the subring of $\C$ given by: \[R = \{a + b\gamma\mid a,b\in\Z\} \] Prove that R is a PID but not an ED. A detailed proof can be found in Mathematics Magazine, Vol. 46, No. 1 (1973), pp 34-38. If you choose to work on this problem, do not consult this reference, or any other reference. Hand-in only your own work, even it it is only parts of the solution.

Problem Set 01 (complete) Due: 02/01/2019 Board presentation: 02/08/2019

1. Let D be an integral domain. Consider the following two properties that D and a function $\delta:D-\{0\}\to\N_0$ may have:
   I. For any $a,d\in D$ with $d\neq 0$, there are $q,r\in D$ such that $a=qd+r$ and ($r=0$ or $\delta(r) < \delta(d))$
   II. For any $a,b\in D-\{0\}$, $\delta(a)\leq\delta(ab)$.
   Prove that if there is a function δ satisfying the first condition, then there is a function γ satisfying both of them. Hint: consider γ defined by: \[\gamma(a):= \min_{x\in D-\{0\}}\delta(ax)\]
2. Chapter 18, problem 22.
3. Chapter 16, problem 24. Can you weaken the assumption “infinitely many”?
4. Show that an integral domain D satisfies the ascending chain condition ACC iff every ideal of D is finitely generated. (Hint: one direction is similar to the proof that every PID satisfies the ACC).

Home