dr Piotr KACPRZYK
Instytut Matematyki i Kryptologii
Wydział Cybernetyki
Wojskowa Akademia Techniczna
ul. Gen. Sylwestra Kaliskiego 2
00-908 Warszawa

Warszawa, 16.05.2012r.

A U T O R E F E R A T

Głównym przedmiotem mojej działalności naukowej są równania różniczkowe cząstkowe, którymi zainteresowałem się od momentu podjęcia pracy w Katedrze Matematyki Wojskowej Akademii Technicznej w 1987 roku.

Początkowo zajmowałem się zagadnieniami granicznymi opisującymi ośrodki sprężyste, termosprężyste oraz procesy termodyfuzji w ciałach stałych. Tej tematyki dotyczą prace [1-10,18]. Przy tym prace [2,3] zostały wykonane w ramach grantu KBN Nr 211659101 (1991-1994) pt. *"Liniowe i nieliniowe układy równań różniczkowych cząstkowych dla ośrodków sprężystych i termosprężystych"*, którym kierował prof. Jerzy Gawinecki.

W pracy [1] uzyskano rozwiązania w postaci fal płaskich w wybranych kierunkach propagacji dla układu równań izotropowej i jednorodnej teorii sprężystości, sprowadzając ten układ do układu dziewięciu równań różniczkowych cząstkowych pierwszego rzędu. Praca ta została zaprezentowana jako komunikat na konferencji Gesellschaft für Angewandte Mathematik und Mechanik (GAMM, Kraków 1-5.04.1991).

Rozwiązaniom asymptotycznym poświęcona jest praca [2]. W pracy tej rozważano liniowy układ równań opisujących ośrodek mikrosprężysty wypełniający obszar $\Omega \subset \Re^3$ z warunkami brzegowymi typu Dirichleta. Dla tego zagadnienia skonstruowano rozwiązanie asymptotyczne, stosując metodę optyki geometrycznej.

W pracy [3] udowodniono istnienie i jednoznaczność słabego rozwiązania dla pierwszego brzegowo-początkowego zagadnienia liniowej termodyfuzji w ośrodku mikropolarnym oraz udowodniono twierdzenie o regularności tego rozwiązania. W tym celu zastosowano metodę Galerkina.

W 1995 roku w Instytucie Matematyki Politechniki Warszawskiej obroniłem rozprawę doktorską pt."*Zagadnienie brzegowo-początkowe dla nieliniowych równań różniczkowych cząstkowych termodyfuzji ciał stałych",* której promotorem był prof. Jerzy Gawinecki.

W pracy doktorskiej rozważałem zagadnienie brzegowo-początkowe z warunkami brzegowymi typu Dirichleta dla nieliniowego hiperboliczno-parabolicznego układu pięciu równań różniczkowych cząstkowych. Wykazałem istnienie oraz jednoznaczność rozwiązania lokalnego w czasie tego zagadnienia w klasie funkcji gładkich. W dowodzie zastosowałem metodę półgrup oraz metodę Galerkina dla zlinaryzowanego problemu, następnie stosując twierdzenie Banacha o punkcie stałym pokazałem istnienie rozwiązania lokalnego w czasie dla problemu nieliniowego. Praca ta została zaprezentowana na konferencji The Third International Congress on Industrial and Applied Mathematics, (GAMM-ICIAM, Hamburg 3-7.07.1995, [5]).

Analogiczne metody zostały zastosowane w pracach [7, 8]. W pracy [7] udowodniono istnienie i jednoznaczność rozwiązania lokalnego w czasie dla zagadnienia brzegowo-początkowego dla parabolicznego układu występującego w teorii termodyfuzji ciał stałych. Podobny rezultat dla brzegowo-początkowego zlinaryzowanego zagadnienia mikropolarnej teorii sprężystości udowodniono w pracy [8]. Przypadek nieliniowy tego zagadnienia został zaprezentowany na konferencji Gesellschaft für Angewandte Mathematik und Mechanik (GAMM, Göttingen 2-7.04.2000, [10]).

Ostatnia praca z tego cyklu badań [18] pokazuje istnienie eksplozji rozwiązania dla zagadnienia brzegowo-początkowego nieliniowej hipersprężystości. W pracy tej pokazano istnienie oraz jednoznaczność lokalnego w czasie gładkiego rozwiązania tego zagadnienia. Następnie korzystając z wyników A. Majdy udowodniono, że dla specjalnej postaci funkcji energii materiału hipersprężystego następuje eksplozja rozwiązania w pewnym momencie czasu. Wynik ten został zaprezentowany na konferencji Gesellschaft für Angewandte Mathematik und Mechanik (GAMM, Metz 12-16.04.1999, [9]).

W roku 2000 rozpocząłem współpracę naukową z prof. Wojciechem Zajączkowskim, profesorem w Instytucie Matematycznym PAN. Efektem tej współpracy był mój udział w realizacji kolejnych grantów kierowanych przez prof. W. Zajączkowskiego.

W ramach grantu KNB Nr 2P03A00223 (2002-2005) pt. *„Nieliniowe układy ewolucyjne - globalne własności”* zrealizowałem bardzo ważny cykl prac, który zatytułowałem „**Stabilność rozwiązań dla nieliniowych równań magnetohydrodynamiki nieściśliwej i ściśliwej cieczy ze swobodną powierzchnią”**. Najważniejsze wyniki dotyczące tych badań przedstawiłem na konferencji ”Regulartity and other aspects of the Navier-Stokes equations”(Będlewo, 10-16.09.2005).

Prace te [11-16] przedstawiam jako osiągnięcie naukowe w rozumieniu art. 16 ust. 2 ustawy o stopniach i tytule naukowym i tytule w zakresie sztuki.

Badany problem można opisać następująco.
W obszarze $\Omega_t \subset \Re^3$ ograniczonym swobodną powierzchnią S_t znajduje się ciecz. W obszarze D_t zewnętrznym do Ω_t znajduje się gaz pod stałym ciśnieniem. Dodatkowo w obszarze D_t jest pole elektromagnetyczne generowane przez pewne źródło znajdujące się na zewnętrznym stałym brzegu B obszaru D_t. Wtedy ruch cieczy w obszarze Ω_t jest opisany za pomocą równań magnetohydrodynamiki. W obszarze $D_{t,}$, który jest dielektrykiem (gazem) mamy jedynie pole elektromagnetyczne, zatem równania magnetohydrodynamiki ulegają odpowiedniej redukcji ponieważ nie ma ruchu cieczy w obszarze D_t. Na swobodnej powierzchni $S_t = \delta\Omega_t \cap \delta D_t$ zakładamy odpowiednie warunki transmisji na pole elektryczne i magnetyczne oraz warunki brzegowe.

Główne rezultaty dotyczące tej tematyki są zawarte w pracach [11-16]. Równania magnetohydrodynamiki przedstawili i opisali L. Landau i E. Lifschitz w monografii: Electrodynamics of Continous, Media, Nauka, Moskwa 1986.

Prace [11-14] dotyczą przypadku nieściśliwego, czyli zakładamy, że gęstość cieczy jest stała. Omówię teraz zawartość tych prac.

W pracy [11] udowodniłem istnienie rozwiązania lokalnego w czasie tego zagadnienia. W tym celu zapisałem równania we współrzędnych Lagrange'a związanych z prędkością cieczy. Dzięki temu można było rozważać równoważny problem w stałym obszarze $\Omega \subset \Re^3$. Następnie zlinearyzowałem badany problem, gdzie współrzędne Lagrange'a związano z daną bezdywergencyjną funkcją. Metodą Galerkina pokazałem istnienie lokalnego w czasie rozwiązania słabego tego zagadnienia. Ze względu na warunki transmisji na brzegu obszaru Ω podniesienie regularności rozwiązania słabego dla tego problemu wymagało różniczkowania równań układu. Uzyskano w ten sposób nierówność energetyczną o regularności H^3 względem zmiennych przestrzennych. W końcu stosując metodę kolejnych przybliżeń, udowodniłem istnienie regularnego lokalnego w czasie rozwiązania badanego zagadnienia.

W pracy [12] udowodniłem, że jeśli prędkość cieczy w chwili początkowej, pole magnetyczne i elektryczne na brzegu B oraz siły zewnętrzne i ich pochodne w obszarze Ω są dostatecznie małe, to czas istnienia rozwiązania lokalnego uzyskanego w pracy [11] można dowolnie wydłużyć; podobnie jak w [11] pokazałem, że dobierając odpowiednio małe

omawiane dane, można zastosować metodę kolejnych przybliżeń w przypadku, gdy czas istnienia rozwiązania lokalnego tego zagadnienia może być dowolnie długi.

W pracach [13, 14] udowodniłem istnienie globalnego w czasie rozwiązania tego zagadnienia, zakładając odpowiednią postać warunków brzegowych na swobodnej powierzchni S_t. W tym celu założyłem dostateczną małość prędkości cieczy w chwili początkowej oraz pola elektrycznego i magnetycznego i ich pochodnych względem zmiennej czasowej na brzegu B. Ponadto założyłem brak działania innych sił zewnętrznych. Następnie zbudowałem odpowiednią nierówność różniczkową oraz udowodniłem specjalną nierówność typu Korna, dzięki którym pokazałem, że kształt obszaru Ω_t ulega dostatecznie małej deformacji w czasie przy założeniu o małości omawianych wcześniej danych oraz wykorzystaniu faktu, że wtedy rozwiązanie lokalne badanego zagadnienia można dowolnie wydłużyć. Otrzymane w ten sposób rezultaty i przyjęte założenia pozwoliły w końcu na wykazanie, że rozwiązanie to można przedłużać krok po kroku uzyskując rozwiązanie regularne, globalne w czasie tego zagadnienia.

Prace [15, 16] dotyczą przypadku cieczy ściśliwej, czyli przy założeniu, że gęstość cieczy jest funkcją czasu oraz zmiennych przestrzennych. W pracy [15] udowodniłem istnienie rozwiązania lokalnego w czasie dla tego zagadnienia analogiczne jak w pracy [11]. W pracy [16] udowodniłem istnienie rozwiązania globalnego w czasie tego zagadnienia podobnie jak w pracy [14], wykorzystując fakt, że analogicznie jak w przypadku nieściśliwym, przy odpowiednich założeniach o danych czas istnienia rozwiązania dla zagadnienia ściśliwego można dowolnie wydłużyć. Użyte metody były identyczne jak w przypadku nieściśliwym, ale zmienna gęstość cieczy powodowała dodatkowe trudności rachunkowe.

Ten cykl prac pokazuje, że przy przyjętych założeniach o małości niektórych danych można utrzymać ciecz znajdującą się w obszarze Ω_t ograniczonym swobodną powierzchnią S_t w dowolnie długim czasie w stanie bliskim stanu równowagowego, działając na nią polem elektromagnetycznym, którego źródło znajduje się na zewnętrznym względem obszaru Ω_t stałym brzegu B. Trzeba podkreślić, że otrzymane rezultaty wymagały przezwyciężenia dużych trudności technicznych, w szczególności ze względu na postawione warunki transmisji na swobodnym brzegu S_t oddzielającym obszar Ω_t od zewnętrznego obszaru D_t względem Ω_t, w którym znajduje się gaz. Podniesienie regularności do H^3, rozwiązania słabego dla zlinearyzowanego zagadnienia wymagało różniczkowania równań układu względem zmiennych przestrzennych i czasowych. Ponieważ S_t było swobodnym brzegiem,

prowadziło to do bardzo skomplikowanych i żmudnych obliczeń. Ponadto udowodnienie nierówności różniczkowych implikujących istnienie globalnych rozwiązań badanych problemów wymagało wykazania oszacowań rozwiązań w otoczeniu swobodnej powierzchni S_t, przy zastosowaniu techniki lokalizacji oraz odpowiednich na niej warunków zgodności.

Teraz opiszę kolejny bardzo ważny kierunek moich badań, który zatytułowałem **„Przepływy przez obszary cylindryczne".**

Prace [17, 19, 20, 21] z tego cyklu zostały zrealizowane w ramach grantu KBN Nr 1 P03A02130 (2006-2009) pt. *„Równania ośrodków ciągłych: własności i struktura rozwiązań*", a prace [22-25] w ramach grantu MNiSW Nr NN 201396937 (2009-2012) pt. *„Własności rozwiązań równań mechaniki ośrodka ciągłego i struktur geometrycznych"*. Najważniejsze rezultaty tych badań przedstawiłem na konferencji "Regularity Aspects of PDE" (Będlewo 5-11.09.2010).

W pracach [17,19] rozważałem przepływ cieczy nieściśliwej przez obszar cylindryczny $\Omega \subset \Re^3$ nie osiowo symetryczny i równoległy do osi x_3. Przepływ jest opisany równaniami Naviera-Stokesa, dla których postawiłem warunki brzegowe typu poślizgu na brzegu obszaru Ω oraz wpływ i wypływ cieczy z tego obszaru przez część brzegu obszaru Ω prostopadłego do osi x_3.

W pracy [17] pokazałem istnienie rozwiązania o regularności $\boldsymbol{W_2^{2,1}}(\Omega \text{ x } (0,T))$ dla tego problemu, gdzie czas istnienia rozwiązania T jest dowolnie długi. Dowód wymagał założenia małości pochodnych strumienia wpływu i wypływu cieczy, trzeciej składowej sił zewnętrznych oraz pochodnej względem x_3 sił zewnętrznych i prędkości początkowej cieczy. Strumień wpływu i wypływu cieczy, dwie pierwsze składowe sił zewnętrznych prędkość początkowa cieczy mogą być dowolne. W dowodzie rozważałem szereg pomocniczych problemów, które powstały z omawianego zagadnienia poprzez zróżniczkowanie równań Naviera-Stokesa względem zmiennej x_3. Dzięki temu podniosłem regularność słabego rozwiązania i zbudowałem nierówność energetyczną o regularności $\boldsymbol{W_2^{2,1}}(\Omega \text{ x } (0,T))$. Następnie rozważałem problem zlinearyzowany, gdzie dla danych dobrałem takie przestrzenie aby zostały spełnione założenia twierdzenia Leray-Schaudera o punkcie stałym.

Praca [19] dotyczy dowodu istnienia rozwiązania globalnego w czasie dla tego zagadnienia. Dowód przebiegał podobnie jak w pracy [17] oraz przyjęto analogiczne założenia o małości danych. Najpierw przemnożyłem równania Naviera-Stokesa przez

odpowiednią funkcję wycinającą zmiennej czasowej. Dzięki temu uzyskałem pomocnicze zagadnienie z jednorodnymi warunkami początkowymi, do którego zastosowałem podobne metody jak w pracy [17] oraz fakt, że czas istnienia rozwiązania lokalnego jest dowolnie długi. W końcu wykazałem, że prędkość przepływu cieczy można kontrolować w dowolnym przedziale czasowym (kT, (k + 1)T), co pozwoliło przedłużać rozwiązanie krok po kroku i uzyskać rozwiązanie globalne w czasie dla problemu pomocniczego i tym samym dla zagadnienia wyjściowego.

Prace [20, 21] dotyczą istnienia i regularności atraktora dla rozwiązania omawianego problemu. Użyte w tych pracach metody pochodzą z monografii V. Chepyzhov, M. Vishik: Attractors for Equations of Mathematical Physics, Amer. Math. Soc. RI, 2001. Dowody przeprowadzone w pracy [20] wykorzystują istnienie globalnego w czasie rozwiązania zagadnienia przepływu, które zostało wykazane w pracy [19]. Najpierw pokazałem, że rozwiązanie tego zagadnienia dla czasu większego od pewnego t_0 należy do pewnej kuli w przestrzeni funkcji bezdywergencyjnych z normą $L_2(\Omega)$, które spełniają warunki brzegowe analogiczne jak prędkość cieczy oraz dla których pochodna względem x_3 jest dostatecznie mała. Następnie, wykorzystując specjalną postać nierówności Gronwalla, pokazałem analogiczny fakt dla przestrzeni z normą $H^1(\Omega)$, co pozwoliło zastosować odpowiednie twierdzenie z cytowanej monografii i wykazać istnienie globalnego zwartego atraktora dla omawianego zagadnienia. W dalszej części udowodniłem twierdzenie o zbieganiu rozwiązania tego problem do rozwiązania stacjonarnego gdy $t\to\infty$, przy założeniu, że siły zewnętrzne oraz strumień wpływu i wypływu dążą odpowiednio do przypadków stacjonarnych tych danych.

W pracy [21] podwyższyłem regularność otrzymanego atraktora dla klasy $H^2(\Omega)$, wykorzystując rezultaty z pracy [20] oraz rozważając zagadnienia pomocnicze o jednorodnych warunkach brzegowych.

Następnym problemem, którym się zajmowałem w tym cyklu prac jest zagadnienie przepływu cieczy prze obszary cylindryczne, w którym równanie przepływu jest sprzężone z nieliniowym równaniem na temperaturę. Założyłem, że obszar Ω oraz warunki brzegowe na prędkość cieczy są analogiczne jak z pracy [17], przyjąłem także te same założenia o małości danych. W pracy [22] rozważałem przypadek $\Omega \subset \Re^2$, który jest szczególnie prosty ze względu na istnienie globalnego w czasie regularnego rozwiązania dla równania Naviera-Stokesa. Najpierw wykazałem ograniczoność temperatury dla dowolnego czasu, co pozwoliło oszacować nieliniowe wyrażenie na temperaturę występujące w równaniu przepływu.

Następnie rozważyłem pomocnicze zagadnienia z jednorodnymi warunkami brzegowymi. Dzięki temu zbudowałem nierówność energetyczną na prędkość cieczy o regularności $\boldsymbol{W_q^{2,1}}(\Omega \text{ x } (0,T))$, $q \in (1,6)$, gdzie T jest dowolnie duże. W końcu do zlinearyzowanego zagadnienia zastosowałem twierdzenie Leray-Schaudera o punkcie stałym.

Praca [23] dotyczy przypadku trójwymiarowego tego zagadnienia. Rozwiązania równania na temperaturę poszukiwałem w przestrzeniach Höldera, aby można było wykorzystać zasadę maksimum dla równań parabolicznych i w ten sposób pokazać ograniczoność temperatury dla dowolnego czasu. Następnie rozważyłem kilka problemów pomocniczych, które powstały z omawianego zagadnienia poprzez zróżniczkowanie równań układu względem zmiennej x_3. Pozwoliło to zbudować nierówność energetyczną o odpowiedniej regularności, a następnie zastosować twierdzenie Leray-Schaudera o punkcie stałym dla problemu zlinearyzowanego.

W pracy [24] rozpatrzyłem omawiany problem z jednorodnymi warunkami brzegowymi, czyli założyłem brak wpływu i wypływu cieczy z obszaru $\Omega \subset \Re^3$. Wtedy przy przyjętych wcześniej założeniach o małości danych pokazałem istnienie globalnego w czasie rozwiązania tego zagadnienia. Najpierw pokazałem ograniczoność temperatury dla dowolnego czasu. Następnie udowodniłem istnienie rozwiązania tego zagadnienia w każdym przedziale czasowym (kT, (k + 1)T), gdzie T jest dowolnie duże, stosując metody analogiczne jak w pracy [23]. Następnie, zakładając odpowiedni warunek na siły zewnętrzne, pokazano że prędkość cieczy oraz temperaturę można kontrolować na każdym odcinku (kT, (k + 1)T). To pozwoliło dowieść istnienia rozwiązania globalnego tego zagadnienia przez przedłużanie rozwiązania lokalnego krok po kroku.

Ostatnia praca w tym cyklu [25] dotyczy istnienia i regularności atraktora dla rozwiązania zagadnienia omawianego w pracy [24]. Zastosowane tutaj metody są identyczne jak w pracy [20,21], czyli najpierw w oparciu o prace [24] wykazałem istnienie globalnego atraktora dla omawianego zagadnienia, a następnie pokazałem zbieżność rozwiązania tego zagadnienia do rozwiązania stacjonarnego oraz w końcu podniosłem regularność atraktora do klasy $H^2(\Omega)$.

W pracach tego cyklu po raz pierwszy pokazałem istnienie rozwiązań prawie globalnych i globalnych w czasie dla zagadnień przepływu przez obszary cylindryczne nie osiowo symetryczne z wpływem i wypływem bez założeń o małości danych początkowych strumienia wpływu, wypływu oraz sił zewnętrznych. Założyłem jedynie małość pochodnych

tych danych oraz trzeciej składowej sił zewnętrznych. W dowodach istnienia rozwiązań dla tych problemów wykorzystałem twierdzenie o punkcie stałym Leray-Schaudera, które wymagało zbudowania nierówności różniczkowych o odpowiedniej regularności. Następnie, dobierając odpowiednie przestrzenie dla danych w problemach zlinearyzowanych, pokazałem że spełnione są założenia tego twierdzenia. Stanowiło to dużą trudność ze względu na odpowiednie zależności między przestrzeniami, do których należą dane oraz rozwiązania tych zagadnień. Prace te mogą stanowić punkt wyjścia do badania przepływów przez obszary cylindryczne o zmiennym przekroju.

Najnowszym obszarem moich zainteresowań są teoretyczne podstawy kryptologii. W związku z tym byłem wykonawcą w projekcie rozwojowym Nr O R00 0043 07, pt. *„Demonstrator technologii generatora koprocesora kryptograficznego operującego na elementach z ciała GF*(2^n)*”,* który został zrealizowany przez Instytut Matematyki i Kryptologii WCY WAT i firmę WASKO S.A., (2009-2011) pod kierunkiem prof. Jerzego Gawineckiego. Mój udział dotyczył opisu metod matematycznych użytych w tym projekcie.

Wybrane fragmenty tego opisu stanowią podstawę obszernego podręcznika algebry abstrakcyjnej „Algebra dla kryptologów” [26], którego jestem autorem. W założeniu książka ta miała być podręcznikiem dla studentów specjalności „Kryptologia”, która została uruchomiona na Wydziale Cybernetyki Wojskowej Akademii Technicznej. Opiszę teraz jej zawartość.

Pierwszy rozdział zawiera pojęcia wstępne. W rozdziale drugim przedstawiono teorię grup dochodząc do twierdzeń Sylowa, grup rozwiązalnych i działania grup w zbiorach. Rozdział trzeci dotyczy pierścieni i ciał. Przedstawiono w nim podstawowe twierdzenia dotyczące pierścieni i ciał, teorię podzielności w pierścieniach całkowitych oraz konstrukcje ciał, korzystając z twierdzeń o pierścieniach ilorazowych. Rozszerzenie ciał opisano szczegółowo w rozdziale czwartym. Szczególny nacisk położono na ciała Galois, które są rozszerzeniami ciał Z_p i są szczególnie ważne we współczesnej kryptologii. Następnie szczegółowo omówiono własności wielomianów cyklotomicznych i pierwiastków z jedności, które są bardzo użyteczne przy konstrukcji ciał Galois. Rozdział piąty dotyczy baz normalnych w ciałach Galois, które ze względu na swoja postać umożliwiają przyspieszenie obliczeń w tych ciałach. Wykazano szereg twierdzeń dotyczących generatorów baz normalnych oraz wielomianów których pierwiastki są generatorami tych baz. Na końcu podano twierdzenia dotyczące ciał Galois, w których istnieją optymalne bazy normalne, szczególnie ważne we współczesnej kryptologii. Twierdzenia te w zasadzie obejmują aktualny stan wiedzy na ten

temat. W rozdziale szóstym przedstawiono teorię Galois. Omawiane w tej książce zagadnienia są ilustrowane wieloma oryginalnymi przykładami. Część twierdzeń zawiera także zaproponowane przeze mnie dowody. W zamierzeniu, po rozszerzeniu omawianych treści i dodaniu rozdziałów dotyczących krzywych eliptycznych nad ciałami skończonymi, podręcznik ten ma stać się monografią obejmującą większość metod matematycznych stosowanych we współczesnej kryptologii.